Veritas NetBackup™ for Microsoft Azure Stack 管理者ガイド

リリース 9.0

VERITAS™

Veritas Microsoft Azure Stack ガイド

最終更新日: 2021-02-01

法的通知と登録商標

Veritas、Veritas ロゴ、NetBackup は、Veritas Technologies LLC または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、Veritas 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Veritas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。Veritas Technologies LLC 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。Veritas Technologies LLC 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、Veritas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。

Veritas Technologies LLC
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 Veritas 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、Veritasの Web サイトで入手できます。

https://sort.veritas.com/documents

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

NB.docs@veritas.com

次の Veritas コミュニティサイトでマニュアルの情報を参照したり、質問したりすることもできます。

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas 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。

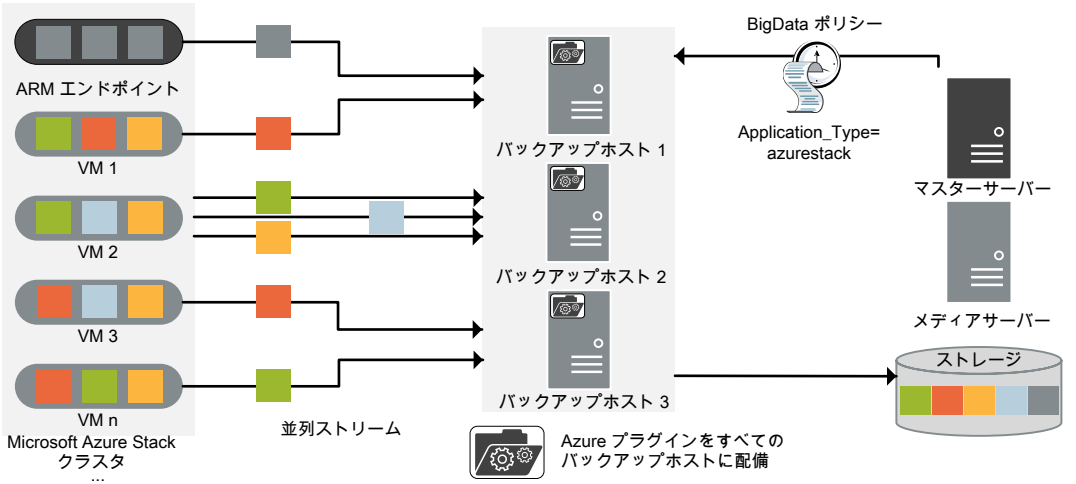
NetBackup を使用した Microsoft Azure Stack VM の保護

NetBackup と NetBackup 並列ストリームフレームワーク (PSF) を使用して、Azure Stack VM を保護できます。

次の図は、NetBackup によって Microsoft Azure Stack VM を保護する方法の概要を示しています。

用語の定義も確認してください。p.11 の「NetBackup for Microsoft Azure Stack の用語」を参照してください。

図 1-1 アーキテクチャの概要



図では次の内容を説明しています。

- VM は並列ストリームでバックアップされ、バックアップ時に NetBackup は VHD のブロブストレージデータをフェッチします。各バックアップホストは、1 つまたは複数の VM に関連付けられたデータをフェッチします。バックアップホストが複数の場合は、VM のセットが各バックアップホストに分散されます。ジョブの処理速度が、複数のバックアップホストと並列ストリームによって向上します。

  メモ: 1 つの VHD のデータは、複数のバックアップホストで並行してフェッチされません。

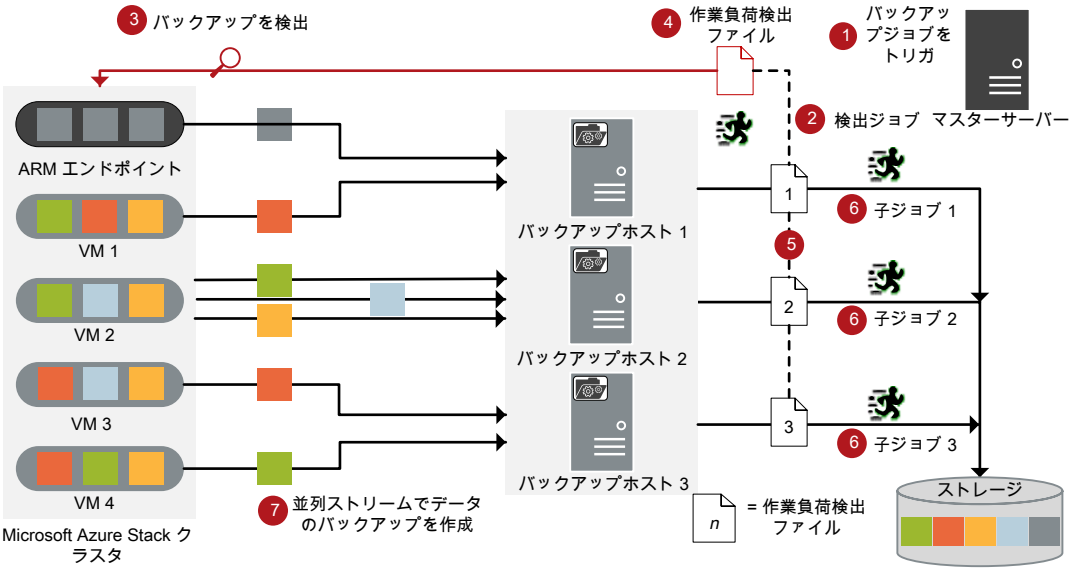
- Microsoft Azure Stack と NetBackup 間の通信は、Microsoft Azure Stack の NetBackup プラグインを使用して有効になります。
  このリリースで、プラグインは個別に利用でき、すべてのバックアップホストにインストールする必要があります。
- NetBackup の通信のために、BigData ポリシーを構成する必要があります。ここで、Application_Type=azurestack を使用し、関連するバックアップホストを追加する必要があります。
- NetBackup のメディアサーバー、クライアント、またはマスターサーバーをバックアップホストとして構成することができます。また、VM の数によっては、バックアップホストを追加または削除できます。バックアップホストをさらに追加することで使用環境の規模を簡単に拡大できます。
  NetBackup のメディアサーバーまたはクライアントをバックアップホストとして使用することをお勧めします。

- NetBackup 並列ストリームフレームワークにより、エージェントレスのバックアップが可能で、バックアップとリストア操作はバックアップホストで実行します。Microsoft Azure Stack VM には、エージェントの占有域がありません。また、NetBackup は Microsoft Azure Stack のアップグレードやメンテナンスの影響を受けません。

Microsoft Azure Stack VM のバックアップ

次の図は、バックアップフローの概要を示しています。

図 1-2 バックアップフロー



図では次の内容を説明しています。

1. スケジュールされたバックアップジョブはマスターサーバーからトリガされます。
2. Microsoft Azure Stack のバックアップジョブは複合ジョブです。バックアップジョブがトリガされると、最初に検出ジョブが実行されます。
3. 検出中に、最初のバックアップホストが ARM (Azure Resource Manager) エンドポイントと接続し、検出を実行して、バックアップする必要がある VM と関連するメタデータの詳細を取得します。
4. 作業負荷検出ファイルは、バックアップホストに作成されます。作業負荷検出ファイルには、さまざまな VM からバックアップする必要があるデータの詳細が含まれています。

5. バックアップホストは、作業負荷検出ファイルを使用して、バックアップするデータの詳細を取得します。個別の作業負荷検出ファイルは、バックアップホストごとに作成されます。
6. バックアップホストごとに個別のバックアップジョブが実行されます。作業負荷分散ファイルで指定されたデータがバックアップされます。
7. データブロックは、異なる VM から複数のバックアップホストに同時にストリームします。並列ストリーム数は、バックアップホストの数と同じです。

   ストリーム数を増やすには、`NO_OF_BACKUP_STREAMS_PER_NODE` 構成パラメータを設定します。詳しくは、`azurestack.conf` 構成ファイルを使用した Microsoft Azure プラグインの設定に関する説明を参照してください。

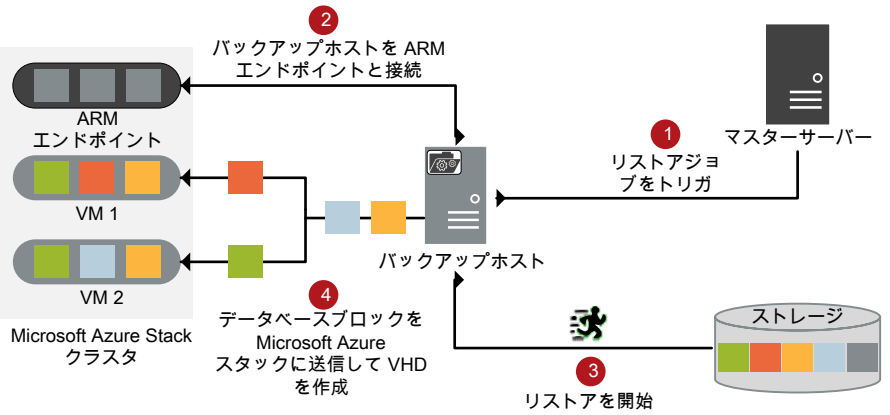
すべての子ジョブが完了するまで、複合バックアップジョブは完了しません。

Microsoft Azure Stack VM のリストア

リストアに使用されるのは、1 つのバックアップホストのみです。

次の図は、リストアフローの概要を示しています。

図 1-3 リストアフロー



図では次の内容を説明しています。

1. マスターサーバーからのリストアジョブがトリガされます。
2. バックアップホストは、ARM (Azure Resource Manager) エンドポイント (ソースクライアント) に接続します。バックアップホストは宛先クライアントです。
3. ストレージメディアからの実際のデータリストアが開始されます。

4. データブロックは、VHD を作成するために Microsoft Azure Stack に送信されます。VHD が作成された後、VM が作成されてインスタンス化されます。

管理対象ディスク VM

- 管理対象ディスクは、ARM によって管理されているブロックレベルのストレージボリュームです。管理対象ディスクを使用して、ディスクのサイズ、ディスクの種類、およびディスクのプロビジョニングを指定する必要があります。それ以外は自動的に処理されます。
- 管理対象ディスクの管理 API は、計算プロバイダで利用可能です。Azure Stack プラグインは REST API を使用して次のことを行います。
  - 管理対象ディスクのスナップショットの作成
  - スナップショットのエクスポート (アクセス権の付与)
  - エクスポート解除 (アクセス権の削除)
  - スナップショットの削除
- 単一の BigData ポリシーは管理対象と管理対象外のディスク VM の両方を保護できます。
- リストア時に、管理対象外ディスク VM を管理対象ディスクに変換できます。
- ストレージアカウントが、VM またはディスクのリストア先のターゲットサブスクリプションに一時 vhd ファイルを作成するために、管理対象ディスクのリストア時に必要になります。これは、リストア時に管理対象ディスクを直接作成するために必要な API が存在しないためです。

NetBackup for Microsoft Azure Stack の用語

次の表では、Microsoft Azure Stack の保護に NetBackup を使用するときに使われる用語を定義しています。

表 1-1 NetBackup の用語

用語	定義
複合ジョブ	Microsoft Azure Stack のバックアップジョブは複合ジョブです。 ■ バックアップジョブは、バックアップするデータの情報を取得するための検出ジョブを実行します。 ■ 子ジョブは、実際のデータ転送を実行する各バックアップホストに対して作成されます。 ■ バックアップが完了すると、ジョブは Microsoft Azure Stack 上のスナップショットをクリーンアップし、その後ジョブ自体に完了したというマークが付けられます。
検出ジョブ	バックアップジョブを実行すると、最初に検出ジョブが作成されます。検出ジョブは ARM エンドポイントと通信し、VM と、関連付けられている VHD に関する情報を収集します。検出の最後に、ジョブは作業負荷検出ファイルにデータを入力します。ファイルはその後 NetBackup によってバックアップホスト間で作業負荷を分散させるために使用されます。
子ジョブ	バックアップの場合、ストレージメディアにデータを転送するバックアップホストごとに個別の子ジョブが作成されます。
作業負荷検出ファイル	検出時のバックアップホストが ARM エンドポイントと通信するときに、作業負荷検出ファイルが作成されます。ファイルには、VM と、関連付けられている VHD に関する情報が含まれています。
並列ストリーム	NetBackup 並列ストリームフレームワークにより、複数の VM を、複数のバックアップホストを同時に使用してバックアップできます。
バックアップホスト	バックアップホストは、プロキシクライアントとして機能します。すべてのバックアップとリストア操作は、バックアップホストで実行されます。 メディアサーバー、クライアント、またはマスターサーバーを、バックアップホストとして構成できます。 バックアップホストは、リストア中に宛先クライアントとしても使用されます。
BigData ポリシー	BigData ポリシーは以下を実行するために導入されました。 ■ アプリケーションの種類を指定します。 ■ 分散マルチノード環境のバックアップを可能にします。 ■ バックアップホストを関連付けます。 ■ 作業負荷分散を実行します。

2

NetBackup 用 Microsoft Azure Stack プラグイン構成の前提条件

この章では以下の項目について説明しています。

オペレーティングシステムとプラットフォームの互換性

必要に応じたバックアップホストの場合 (メディアサーバーまたは NetBackup Appliance):

- RHEL (Red Hat Enterprise Linux) 7.4 以降がサポート対象
- Red Hat Enterprise Linux (RHEL) 8.0 以降のバージョンでは、追加の「compat-openssl10」パッケージをインストールする必要があります。

詳しくは、次の場所で NetBackup の互換性リストを参照してください。

https://www.veritas.com/support/en_US/article.100040093

NetBackup 用の Microsoft Azure Stack プラグインのライセンス

NetBackup 用 Microsoft Azure スタックプラグインを使用してバックアップおよびリストア操作を実行するためのライセンス要件については、次のページを参照してください。

How to use NetBackup plug-ins and agents: download, install, and availability information

ライセンスを追加する方法に関する詳細情報を参照できます。

『NetBackup 管理者ガイド Vol. 1』を参照してください。

IPV6 設定でのバックアップホストの設定

Azure Stack プラグインがインストールされているバックアップホストは、デュアルスタックである必要があります。

Azure Stack ARM エンドポイントが、ポリシーから構成されたバックアップホストからアクセス可能であることを確認します。

バックアップホストは、IPV4 と IPV6 のアドレスで構成する必要があります。

Azure Stack との時間同期

バックアップとリストアの失敗を回避するには、NetBackup マスターサーバー、メディアサーバー、バックアップホストの日時を Azure Stack と同期する必要があります。

時刻の同期が完了したら、バックアップホストで NetBackup サービスを再起動します。

Microsoft Azure Stack を保護するための NetBackup の配備について

- マルチノードの Microsoft Azure Stack クラスタを配備した場合は、NetBackup サーバーとバックアップホストをクラスタの外部に配備し、その上で接続を構成します。p.15 の「NetBackup と Microsoft Azure Stack の構成の概要」を参照してください。

3

NetBackup と Microsoft Azure Stack の構成

この章では以下の項目について説明しています。

- NetBackup と Microsoft Azure Stack の構成の概要
- バックアップホストの管理
- NetBackup 管理者にアクセス権を付与するための Microsoft Azure Stack カスタムロールの追加
- azurestack.conf 構成ファイルを使用した Microsoft Azure プラグインの構成
- Microsoft Azure Stack クレデンシャルを含むファイルの作成
- NetBackup での Microsoft Azure Stack クレデンシャルの追加
- NetBackup ポリシーユーティリティを使用した Microsoft Azure Stack 用 BigData ポリシーの作成
- 古いスナップショットのクリーンアップ

NetBackup と Microsoft Azure Stack の構成の概要

次の表は、認証に必要な Microsoft Azure Stack 用 NetBackup の構成手順をリストしたものです。

表 3-1 Microsoft Azure Stack 用 NetBackup の構成手順

手順	コンポーネント	詳細
1	バックアップホスト	バックアップホストを作成して、NetBackup クライアントをバックアップホストとして使用する場合はホワイトリストに追加します。 詳しくは、次を参照してください。 ■ p.17 の「バックアップホストの管理」を参照してください。 ■ p.17 の「NetBackup マスターサーバー上のバックアップホストのホワイトリスト」を参照してください。
2	Microsoft Azure Stack の NetBackup のカスタムロール	NetBackup 用 Microsoft Azure Stack で、VM をバックアップおよびリストアするためのカスタムロールを作成します。 詳しくは、次を参照してください。 p.18 の「NetBackup 管理者にアクセス権を付与するための Microsoft Azure Stack カスタムロールの追加」を参照してください。
3	■ Microsoft Azure Stack のクレデンシャルファイル ■ Microsoft Azure Stack のプラグインの構成ファイル	■ マスターサーバー上に、Azure Stack クレデンシャルを含んでいるファイルを作成します。 p.25 の「Microsoft Azure Stack クレデンシャルを含むファイルの作成」を参照してください。 ■ 構成ファイルを使用して Microsoft Azure Stack プラグインを構成し、構成ファイルのパスをホワイトリストに追加します。 詳しくは、次を参照してください。 ■ p.22 の「azurestack.conf 構成ファイルを使用した Microsoft Azure プラグインの構成」を参照してください。 ■ p.24 の「NetBackup マスターサーバー上の構成ファイルパスのホワイトリスト」を参照してください。 ■ Microsoft Azure Stack クレデンシャルを NetBackup に追加して、通信を確立してデータを保護します。 詳しくは、次を参照してください。 p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。
4	BigData ポリシー	Microsoft Azure Stack 向けの BigData ポリシーを作成します。 詳しくは、次を参照してください。 p.31 の「NetBackup ポリシーユーティリティを使用した Microsoft Azure Stack 用 BigData ポリシーの作成」を参照してください。

バックアップホストの管理

バックアップホストは、Microsoft Azure Stack のすべてのバックアップとリストア操作をホストするプロキシクライアントとして機能します。NetBackup 用 Microsoft Azure Stack プラグインの場合、バックアップホストは、Microsoft Azure Stack にインストールされている独立したエージェントなしですべてのバックアップとリストア操作を実行します。

バックアップホストは、RHEL 7.4 以降のコンピュータ上にある必要があります。NetBackup は、バックアップホストとして RHEL プラットフォームのみをサポートします。

バックアップホストを追加する前に、次の点を考慮します。

- バックアップ操作用に、1 つ以上のバックアップホストを追加できます。
- リストア操作用に、バックアップホストを 1 つだけ使用できます。
- マスターサーバー、メディアサーバー、またはクライアントが、バックアップホストの役割を実行できます。

  メモ: NetBackup のメディアサーバーまたはクライアントをバックアップホストとして使用することをお勧めします。

- 複数のバックアップホストを使用する場合は、すべてのバックアップホストがメディアサーバーと通信していることを確認します。
- Azure Stack の ID プロバイダ
  - AAD (Azure Active Directory) ID プロバイダの場合、すべてのバックアップホストで https://login.microsoftonline.com、Azure Resource Manager エンドポイント、または Azure ブロブストレージエンドポイントへの接続が必要です。ここでは、通信のためにポート 80 と 443 が必要になります。
  - Active Directory フェデレーションサービス (ADFS) ID プロバイダの場合、すべてのバックアップホストで Azure Resource Manager エンドポイント、Azure ブロブストレージエンドポイント、または ADFS エンドポイントへの接続が必要です。ここでは、通信ポート 80 と 443 が必要になります。

NetBackup 管理コンソールを使用して BigData ポリシーを構成している間に、バックアップホストを追加できます。

p.31 の「NetBackup ポリシーユーティリティを使用した Microsoft Azure Stack 用 BigData ポリシーの作成」を参照してください。

NetBackup マスターサーバー上のバックアップホストのホワイトリスト

NetBackup クライアントをバックアップホストとして使用するには、それをホワイトリストに載せる必要があります。NetBackup マスターサーバー上でホワイトリストへの追加手順を実行します。

ホワイトリストは、ソフトウェアまたはアプリケーションが安全な実行を承認されていない限り、それらを実行しないようにシステムを制限するセキュリティ手法です。

NetBackup マスターサーバー上のバックアップホストをホワイトリストに追加するには

- NetBackup マスターサーバー上で次のコマンドを実行します。
  - UNIX の場合

    ```
    bpsetconfig -h masterserver
    bpsetconfig> APP_PROXY_SERVER = clientname1.domain.org
    bpsetconfig> APP_PROXY_SERVER = clientname2.domain.org
    bpsetconfig>
    UNIX システムの場合： <ctl-D>
    ```

  - Windows の場合

    ```
    bpsetconfig -h masterserver
    bpsetconfig> APP_PROXY_SERVER = clientname1.domain.org
    bpsetconfig> APP_PROXY_SERVER = clientname2.domain.org
    bpsetconfig>
    Windows システムの場合： <Ctrl-Z>
    ```

このコマンドは *APP_PROXY_SERVER = clientname* エントリをバックアップ構成 (bp.conf) ファイルに設定します。

APP_PROXY_SERVER = clientname について詳しくは、*『NetBackup 管理者ガイド Vol. 1』*の *NetBackup クライアントの構成オプション*のセクションを参照してください。

Veritas NetBackup のドキュメント

NetBackup 管理者にアクセス権を付与するための Microsoft Azure Stack カスタムロールの追加

NetBackup では、Azure Stack サブスクリプションを保護するために、これらのサブスクリプションへのアクセス権が必要です。NetBackup 向けの Active Directory にカスタムユーザーを作成し、そのユーザーにサブスクリプションにアクセスするためのロールを付与する必要があります。ユーザーに共同所有者のロールを付与するか、バックアップやリカバリのために必要なアクセス権を持つカスタムロールを作成できます。サブスクリプションの所有者としての Azure Stack 管理者は、サブスクリプション用にカスタムロールを作成できます。

NetBackup が必要とする最低限のアクセス権は次のとおりです。

- Microsoft.Compute/virtualMachines/*
- Microsoft.Network/networkInterfaces/*
- Microsoft.Network/networkSecurityGroups/join/action

- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/publicIPAddresses/join/action
- Microsoft.Network/publicIPAddresses/read
- Microsoft.Network/publicIPAddresses/write
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Network/virtualNetworks/subnets/join/action
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listKeys/action

カスタムロールを作成するには、次の手順を完了します。

1

Active Directory フェデレーションサービス (ADFS) 向け	Microsoft 管理コンソールの[Active Directory ユーザーとコンピュータ]ダイアログボックスから、Active Directory に nbu_azst という名前のユーザーまたはサービスプリンシパルを作成します。
Microsoft Azure Active Directory (Azure AD) 向け	[Microsoft Azure Active Directory ユーザー]ダイアログボックスから、サービスプリンシパルを作成します。

Azure Stack 用 PowerShell が配備された Windows コンピュータで、次の手順を完了します。

詳しくは、
https://docs.microsoft.com/ja-jp/azure/azure-stack/azure-stack-powershell-install
を参照してください。

2 新しいテキストファイル rbac_NBU_role.json を作成し、このファイルに次のスクリプトを追加します。

```
{
"Name": "NBU BnR Role",
"IsCustom": true,
"Description": "Let's you perform backup and recovery of VMs",
"Actions": [
"Microsoft.Compute/virtualMachines/*",
"Microsoft.Compute/Disks/read",
"Microsoft.Compute/Disks/write",
"Microsoft.Compute/Disks/beginGetAccess/action",
"Microsoft.Compute/Disks/endGetAccess/action",
"Microsoft.Compute/Snapshots/*",
"Microsoft.Network/networkInterfaces/*",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/Resources/read",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action"
],
"NotActions": [],
"AssignableScopes": [
"/subscriptions/subscription_ID_1",
"/subscriptions/subscription_ID_2"
.
.
.
]
}
```

メモ: 必要なサブスクリプションを AssignableScopes フィールドに追加して、それらのサブスクリプションにカスタムロールが作成されるようにします。

たとえば、ファイルスニペットで *subscription_ID_1* と *subscription_ID_2* を持っている実際のサブスクリプション ID で置き換えます。

---

3 次のコマンドを実行します。

- `Add-AzureRMEnvironment -Name AzureStackAdmin -ArmEndpoint "ArmEndpointValue"`
  例: `Add-AzureRMEnvironment -Name AzureStackAdmin -ArmEndpoint "https://management.local.azurestack.external"`
- `Add-AzureRmAccount -EnvironmentName "AzureStackAdmin"`
- `New-AzureRmRoleDefinition -InputFile "<directory_path>¥rbac_NBU_role.json"`

次の ARM エンドポイントを使用できます。

- プロバイダサブスクリプション
- テナントサブスクリプション

4 Microsoft Azure Stack のコンソールを開いて、次の手順を完了します。

1. [メニュー]をクリックして、NetBackup で保護するサブスクリプションを開きます。[アクセス制御 (IAM)]、[役割]の順にクリックして、新しく作成したロールを表示します。

2. [サブスクリプション]、[アクセス制御 (IAM)]、[追加]の順にクリックします。[名前の選択]フィールドで `nbu_azst` ユーザー (ADFS) またはサービスプリンシパル (AAD) の表示名を追加し、[種類]フィールドで[ユーザー]を選択し、[役割]フィールドに新たに追加したロールを選択します。

5 `nbu_azst` ユーザーまたはサービスプリンシパルを `tpconfig` コマンドに追加してバックアップを取得します。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。

azurestack.conf 構成ファイルを使用した Microsoft Azure プラグインの構成

NetBackup マスターサーバーは、Microsoft Azure Stack との通信向けの構成を保存するために、`azurestack.conf` ファイルを使用します。

`azurestack.conf` ファイルは `/usr/openv/var/global` ディレクトリ内に作成する必要があります。

設定の定義は「属性 = 値」の形式にし、「=」の前後にスペースを 1 つずつ入れる必要があります。

オプションと値では大文字と小文字が区別されます。

メモ: どのパラメータにも空白値は指定できません。指定するとバックアップジョブは失敗します。

azurestack.conf ファイルの例を次に示します。

```
VM_STATE = Running
FETCH_STORAGE_KEYS = false
CA_FILE_PATH =
//directory_path_system_CA_certificate/certificate_name.crt
VM_SNAPSHOT_IN_DISCOVERY = true
NO_OF_BACKUP_STREAMS_PER_NODE = 1
ENABLE_SNAPSHOT_CLEANUP = 0
SNAPSHOT_CLEANUP_MIN = 1440
SNAPSHOT_FETCH_RETRY_COUNT = 60
ASYNC_SNAPSHOT_SUPPORT = true
SET_PUBLIC_IP_DURING_RESTORE = false
STAGING_STORAGE_ACCOUNTS = headsuptsta, restorestadisks,
stafordiskstorages
```

- VM_STATE の指定可能な値は Running、Deallocated、Stopped です。
- SNAPSHOT_FETCH_RETRY_COUNT の値は、VM のスナップショットプロセスが失敗した場合の再試行の最大回数を指定します。値は 3 を超えて指定できません。
- FETCH_STORAGE_KEYS の値は、Azure Stack のクレデンシャルファイルにアクセスキーを使用したストレージアカウントが必要かどうかを指定します。値には、true または false を指定できます。値が true の場合は、クレデンシャルファイルにアクセスキーを使用したストレージアカウントは指定しないようにします。デフォルト値は true です。
- CA_FILE_PATH の値は、システム CA 証明書のディレクトリパスと証明書の名前です。たとえば、/etc/pki/tls/certs/ca-bundle.crt のようになります。このディレクトリパスは、すべてのシステム CA 証明書のデフォルトパスです。
- VM_SNAPSHOT_IN_DISCOVERY の値は、バックアップポリシーのバックアップ対象に指定されている VM に接続されているすべてのディスクについて、VM ディスクスナップショットが作成されるかどうかを定義します。デフォルト値は false であり、単一の VM に接続されているすべてのディスクのスナップショットが、バックアップジョブの実行中に作成されることを指定します。
- NO_OF_BACKUP_STREAMS_PER_NODE の値は、バックアップホストごとのバックアップストリームの最大数を指定します。デフォルト値は 1 です。値は最大 8 まで定義できます。
- ENABLE_SNAPSHOT_CLEANUP の値は、古いスナップショットをクリーンアップするタイミングを指定します。次の値を使用できます。

- 0
  古いスナップショットを削除しません。これはデフォルト値です。
- 1
  バックアップジョブが完了した後に、古いスナップショットを削除します。
- 2
  次回の検出ジョブの一環として、古いスナップショットを削除します。

- SNAPSHOT_CLEANUP_MIN の値は、スナップショットが削除されるまでの時間を分単位で指定します。デフォルト値は 1440 分 (24 時間) です。理想的な値は、分単位での 2 つのバックアップジョブの間隔です。
- SNAPSHOT_FETCH_RETRY_COUNT の値は、指定したストレージコンテナのスナップショットを確認するためのプラグインの再試行回数を指定します。デフォルト値は 60 であり、60 と 120 の間の値を指定できます。
- ASYNC_SNAPSHOT_SUPPORT の値は、非同期の REST API を使用して、管理対象外ディスクのスナップショットを作成することを指定します。デフォルト値は true です。この値を false に設定すると、非同期の REST API を使用する管理対象外ディスクのスナップショットが無効になります。
- SET_PUBLIC_IP_DURING_RESTORE の値は、VM のリストア時にパブリック IP アドレスを使用するかどうかを指定します。デフォルト値は true であり、VM がパブリック IP アドレスでリストアされることを指定します。プライベート IP アドレスを使用して VM をリストアするには、値を false に設定します。
- STAGING_STORAGE_ACCOUNTS の値は、Azure Stack ですでに利用可能なストレージアカウント名のカンマ区切りリストであり、この値は、管理対象ディスクの VM のリストアまたはリカバリにのみ必要です。このキーには、1 つ以上のストレージアカウント名を指定できます。管理対象ディスクの変換操作のために VHD BLOB をリストアするには、ストレージアカウント名が必要です。リストア場所として選択されたターゲットサブスクリプションの場所に応じて、Netbackup Azure Stack プラグインは、このキーに指定されたリストから 1 つのストレージアカウントのみを自動的に選択します。これは、各リストアジョブで選択されたターゲットの場所に応じて、すべてのリストアジョブに必要なすべてのストレージアカウントを指定できる 1 回限りのアクティビティです。

メモ: すべての VM のバックアップを取得する場合は、azurestack.conf ファイルに VM_STATE を追加しないでください。

NetBackup マスターサーバー上の構成ファイルパスのホワイトリスト

構成ファイルを作成した後、NetBackup でバックアップ操作が正常に実行されるようにするために、構成ファイルのパスをホワイトリストに追加する必要があります。NetBackup マスターサーバー上でホワイトリストへの追加手順を実行します。

ホワイトリストは、ソフトウェアまたはアプリケーションが安全な実行を承認されていないかぎり、それらを実行しないようにシステムを制限するセキュリティ手法です。

構成ファイルのパスをホワイトリストに追加するには

NetBackup マスターサーバー上で次のコマンドを実行します。

1. UNIX の場合:

   ```
   bpsetconfig -h masterserver_name
   bpsetconfig BPCD_WHITELIST_PATH = /usr/openv/var/global/
   ```

   コマンドラインを終了します。

   クラスタ化されたマスターサーバーの場合:

   ```
   bpsetconfig BPCD_WHITELIST_PATH = /<shared drive mount
   location>/var/global/
   ```

2. Windows の場合:

   ```
   bpsetconfig -h masterserver_name
   bpsetconfig BPCD_WHITELIST_PATH =
   <install_dir>¥NetBackup¥var¥global¥
   ```

   クラスタ化されたマスターサーバーの場合:

   ```
   bpsetconfig BPCD_WHITELIST_PATH = <Shared
   drive>¥NetBackup¥var¥global¥
   ```

   コマンドラインを終了します。

BPCD_WHITELIST_PATH について詳しくは、『NetBackup 管理者ガイド Vol. 1』の NetBackup サーバーの構成オプションに関するセクションを参照してください。

Microsoft Azure Stack クレデンシャルを含むファイルの作成

Microsoft Azure Stack と通信するために、プラグインに Microsoft Azure Stack クレデンシャルへのアクセス権が必要です。クレデンシャルは、NetBackup マスターサーバー上のファイルに保存する必要があります。クレデンシャルは暗号化された形式で格納され、プラグインは情報に安全にアクセスします。

Microsoft Azure Stack クレデンシャルを含むファイルをマスターサーバーに作成するには

- マスターサーバー上の任意の場所に、JSON 形式のファイルを作成します。
  たとえば、azurestack.creds という名前のファイルを /usr/openv/var/global/ ディレクトリに作成できます。

- ファイルを開いて次の内容を追加します。

```
{
"IdentityProvider":"ADFS",
"TenantId":"tenant.domain.com",
"ClientId":"1950a258-227b-4e31-a9cf-717495945fc2",
"ClientSecret":"client_secret",
"AuthResource":
"https://management.adfs.azurestack.local/metadata/a6ad92e4-5b80-4c88-b84f-a7f25c12ba27",
"teststorageac1":
"9ghIt35bQeSvjZxXUPj8LinMs6aXPb2tMFjXVIG6N2v2FO6LRg+HzLz2LX1xR/qRkQYwNPIaE/v+QnUovzaKpQ==",
"rg1disks540":
"R6Lu3buXZ4HVtRTrNEHzzJqo2gShjQytfjX1hRkvfqMVWnvKWmEt2CUfmhlbxI7JCE0Gh5TKA9r3I88eit2FdA==",
"StorageAccount3":"asasdlfkjaasdfasdfasdfasdf09sd8fhaopisdfbanpsdf98asdfpusadf====",
"StorageAccount11":"90asdfasdfasdfasd-98fha-sdf98asdb-fau9bsdf-auy8svfasd==",
"StorageAccount19":"90asdfasdfasdfasd-98fha-sdf98asdb-fau9bsdf-auy8svfasd==",
"StorageAccount121":"90asdfasdfasdfasd-98fha-sdf98asdb-fau9bsdf-auy8svfasd==",
"StorageAccount13":"90asdfasdfasdfasd-98fha-sdf98asdb-fau9bsdf-auy8svfasd==",
"StorageAccount14":"90asdfasdfasdfasd-98fha-sdf98asdb-fau9bsdf-auy8svfasd==",
"StorageAccount12":"90asdfasdfasdfasd-98fha-sdf98asdb-fau9bsdf-auy8svfasd=="
...
}
```

メモ: StorageAccount の詳細は、FETCH_STORAGE_KEYS = false が azurestack.conf ファイル内にある場合に必要です。

オプション	ID プロバイダ	説明
IdentityProvider	AAD および ADFS	値は、ADFS (Active Directory フェデレーションサービス) または AAD (Azure Active Directory) のいずれかにできます。
TenantId	AAD	値はテナントドメインです。たとえば、「*tenant.onmicrosoft.com*」です。 p.27 の「AAD の TenantId 値の取得」を参照してください。
ClientId	ADFS	値は、*1950a258-227b-4e31-a9cf-717495945fc2* です。
	AAD	値は、NetBackup が保護する必要があるサブスクリプションに対して、NetBackup のバックアップとリカバリの役割を持つサービスプリンシパルのアプリケーション ID です。 p.27 の「AAD の ClientId 値の取得」を参照してください。
ClientSecret	AAD	値は、NetBackup が保護する必要があるサブスクリプションに対して、NetBackup のバックアップとリカバリの役割を持つサービスプリンシパルのクライアントシークレットです。 p.27 の「AAD の ClientSecret 値の取得」を参照してください。

オプション	ID プロバイダ	説明
AuthResource	AAD および ADFS	Web ブラウザで次の URL を開いて取得できる、キーオーディエンスの値です。 https://managment.{*region*}.{*azurestackFQDN*}/metadata/endpoints?api-version=2015-01-01 次に例を示します。 *https://management.eng.azurestack.veritas.com/metadata/endpoints?api-version=2015-01-01* URL は、キーオーディエンスの値である JSON 値を返します。
StorageAccount	AAD および ADFS	アクセスキーを持つストレージアカウントです。 azurestack.conf ファイル内の fetchStorageKeys の値が ***false*** の場合は、このオプションを追加する必要があります。

AAD の TenantId 値の取得

1. https://portal.azure.com にサインインします。
2. [Azure Active Directory]、[プロパティ]の順に選択して、[ディレクトリ ID]が TenantId のものを探します。

AAD の ClientId 値の取得

ClientId 値を取得するには、新しいサービスプリンシパルを作成するか、既存のサービスプリンシパルを使用します。

1. https://portal.azure.com にサインインします。
2. [Azure Active Directory]、[アプリの登録]の順に開きます。
3. [名前またはアプリ ID で検索]フィールドで、*NBU-ASTK-1* を検索し、結果からサービスプリンシパルの[表示名]をクリックします。
4. ClientID を取得するための、次の手順のいずれかを使用します。
   - [設定]を開いて、[アプリケーション ID]が ClientId のものを特定してコピーします。
   - [プロパティ]を開いて、[アプリケーション ID]が ClientId のものを特定してコピーします。

AAD の ClientSecret 値の取得

ClientSecret 値を取得するには、新しいサービスプリンシパルを作成するか、既存のサービスプリンシパルを使用します。

1. https://portal.azure.com にサインインします。
2. [Azure Active Directory]、[アプリの登録]、[新しいアプリケーションの登録]の順に開きます。

3. [名前]が *NBU-ASTK-1* のアプリケーションを作成します。

   [アプリケーションの種類]に[Web アプリケーション/API]を選択します。

   [サインオン URL]を *https://astk.nbu.com* として入力します。

   [作成]をクリックします。

4. [Azure Active Directory]、[アプリの登録]の順に開きます。
5. [名前またはアプリ ID で検索]フィールドで、*NBU-ASTK-1* を検索し、結果からサービスプリンシパルの[表示名]をクリックします。
6. [設定]、[キー]の順に開いて、次のように新しいパスワード情報を追加して保存します。

   [説明]: *Credential_1*

   [有効期限]: *なし*

   [値]: *seedvalue_1*

7. 表示される[値]は、ClientSecret です。値は 1 回だけ表示されます。ウィンドウを閉じると、値は再度表示されません。

Microsoft Azure Stack AAD 認証との通信のためのプロキシ設定の構成

バックアップホストがインターネットに接続できるように、ネットワークにプロキシ設定が必要な場合、次の方法のいずれかを使用します。

- プロキシ URL、ポート番号、ユーザー名とパスワードを次の形式で指定する標準的な環境変数 https_proxy を使用します (単純な構成)。

  ```
  https_proxy=https://USERNAME:PASSWORD@PROXYIP_HOSTNAME:PROXYPORT
  ```

- NetBackup Azure Stack プラグインに別のプロキシが必要な場合、または https_proxy 変数を使用しない場合、次のプロキシ詳細をクレデンシャルファイル内に追加できます。

キー (Key)	説明
InternetProxyUrl	プロキシ URL とポート番号を指定し、インターネット経由で AAD 認証サービスと login.microsoftonline.com に接続します。たとえば https://myproxyInternet.com:8000 のようになります。
InternetProxyUsername	必要に応じて、プロキシインターネット URL を認証するユーザー名を指定します。

キー (Key)	説明
InternetProxyPassword	必要に応じて、プロキシインターネットURLを認証するユーザー名を指定します。

```
{
"IdentityProvider":"AAD",
"TenantId":"tenant.domain.com",
"ClientId":"1950a007-227b-4e31-a9cf-717495945fc2",
"ClientSecret":"client_secret",
"AuthResource": "https://management.adfs.azurestack.local/metadata/
a6ad92e4-5b80-4c88-b055-a7f25c12ba27",
"InternetProxyUrl":"proxy.domain.com:8080",
"InternetProxyUsrename":"myusername",
"InternetProxyPassword":"mypassword"
}
```

NetBackup での Microsoft Azure Stack クレデンシャルの追加

正常なバックアップとリストア操作のために Microsoft Azure Stack クラスタと NetBackup との間でシームレスな通信を確立するには、Microsoft Azure Stack クレデンシャルを NetBackup マスターサーバーに追加して更新する必要があります。

tpconfig コマンドを使用して、NetBackup マスターサーバーでクレデンシャルを追加します。

tpconfig 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。

NetBackup でクレデンシャルを追加するには

1. 次のディレクトリパスから tpconfig コマンドを実行します。

   UNIX システムでは、/usr/openv/volmgr/bin/

2. 次のコマンドを各パラメータに適切な値を入力して実行し、Microsoft Azure Stack クレデンシャルを追加します。

   ```
   tpconfig -add -application_server_user_id user_ID
   -application_type application_type -application_server
   application_server_name -password password_of_the_nbu_azst_user
   -application_server_conf "/usr/<file_path>/azurestack.creds"
   ```

- AAD の場合、NetBackup は clientID と clientSecret を使用するため、-application_server_user_id の値を dummy として入力し、-password の値を dummy として入力します。

メモ: 追加するユーザーは、保護するサブスクリプションの共同所有者権限を持っている必要があります。

次に例を示します。

```
tpconfig -add -application_server_user_id example_user_ID
-application_type azurestack -application_server
application_server_name -password password_of_the_nbu_azst_user
-application_server_conf "/usr/openv/var/global/azurestack.creds"
```

ここで、数値 8 は、Microsoft Azure Stack に対応する -application_type パラメータにも指定できます。

3 tpconfig -dappservers コマンドを実行し、NetBackup マスターサーバーに追加された Azure クレデンシャルがあることを確認します。

例として、サンプル出力を示します。

```
Application Server Host Name:        management.local.azurestack.external
Application Server Type:             azurestack
Required Port:                       0
User of Application Host:            root
```

4 tpconfig を使用してクレデンシャルを追加したら、tpconfig -add コマンドに使用した場所からクレデンシャルファイルを削除できます。

5 次のコマンドを実行して、tpconfig クレデンシャルを更新または削除します。

- 削除 (Delete)

  ```
  tpconfig -delete -application_server_user_id user_ID
  -application_type application_type -application_server
  application_server_name -password password_of_the_nbu_azst_user
  -application_server_conf "/usr/<file_path>/azurestack.creds"
  ```

- 更新 (Update)

  クレデンシャルファイル内の属性またはオプションを変更するには、クレデンシャルを更新し、tpconfig -update コマンドを使用します。

  ```
  tpconfig -update -application_server_user_id user_ID
  -application_type application_type -application_server
  ```

```
application_server_name -password password_of_the_nbu_azst_user
-application_server_conf "/usr/<file_path>/azurestack.creds"
```

NetBackup ポリシーユーティリティを使用した Microsoft Azure Stack 用 BigData ポリシーの作成

次の手順を実行して、NetBackup ポリシーユーティリティを使用し、BigData ポリシーを作成します。

NetBackup ポリシーユーティリティを使用して BigData ポリシーを作成するには

1. NetBackup 管理コンソールの左ペインで、[NetBackup の管理 (NetBackup Management)]>[ポリシー (Policies)]を展開します。
2. [処理 (Actions)]メニューで[新規 (New)]>[ポリシー (Policy)]をクリックします。
3. 新しいポリシー用の一意の名前を[新しいポリシーの追加 (Add a New Policy)]ダイアログボックスに入力します。

   [OK]をクリックします。
4. [属性 (Attributes)]タブで、ポリシー形式に[BigData]を選択します。
5. [属性 (Attributes)]タブには、BigData ポリシー形式のストレージユニットを選択します。
6. [スケジュール (Schedules)]タブで[新規 (New)]をクリックして、新しいスケジュールを作成します。

   BigData ポリシー向けに完全バックアップのスケジュールを作成できます。スケジュールを設定すると、Microsoft Azure データは、ユーザーがそれ以上介入しなくても、設定されたスケジュールに従って自動的にバックアップされます。
7. [クライアント (Clients)]タブで、ARM エンドポイントの IP アドレスまたはホスト名を入力します。

   次の ARM エンドポイントを追加できます。

   - プロバイダサブスクリプション
   - テナントサブスクリプション
8. [バックアップ対象 (Backup Selections)]タブで、次のようにパラメータとその値を入力します。

   - *Application_Type=azurestack*
     これらのパラメータ値では、大文字と小文字が区別されます。
   - *Backup_Host=IP_address or FQDN*
     複数のバックアップホストを指定できます。

- バックアップする資産の指定
  - サブスクリプションのすべての VM の場合: */Subscription ID*
  - リソースグループ内のすべての VM の場合: */Subscription ID/Resource Group*
  - 1 つの VM の場合: */Subscription ID/Resoutrce Group/VM Name*

メモ: BigData ポリシーを Application_Type = azurestack で定義するときにバックアップ対象に対して指定されるディレクトリまたはフォルダには、名前にスペースまたはカンマを含めることはできません。

9 ［OK］をクリックして、変更を保存します。

古いスナップショットのクリーンアップ

- `azurestack.conf` ファイル内の `ENABLE_SNAPSHOT_CLEANUP` の値は、古いスナップショットをクリーンアップするタイミングを指定します。次の値を使用できます。
  - 0
    古いスナップショットを削除しません。これはデフォルト値です。
  - 1
    バックアップジョブが完了した後に、古いスナップショットを削除します。
  - 2
    次回の検出ジョブの一環として、古いスナップショットを削除します。
- `azurestack.conf` ファイル内の `SNAPSHOT_CLEANUP_MIN` の値は、スナップショットが削除されるまでの時間を分単位で指定します。デフォルト値は 1440 分 (24 時間) です。理想的な値は、分単位での 2 つのバックアップジョブの間隔です。

バックアップジョブの一環として作成されたすべてのスナップショットは、同じバックアップジョブで削除されます。ただし、ネットワーク障害、停電など、何らかの理由によりスナップショットが Azure Stack 環境に残ることがあります。このような場合は、`ENABLE_SNAPSHOT_CLEANUP` パラメータを使用して 1 に設定します。

次の命名規則を使用して、NetBackup が作成するスナップショットを識別できます。

```
OSDisk

<Disk UUID_OSDisk_9999_<Snap id>_ BDAZSNAP>
```

次に例を示します。

```
/cb9b5b6d-0c60-4ed1-9cd7-7aaf054b899f_OSDisk_9999_1600405027_BDAZSNAP

DataDisk
```

```
<Disk UUID_DataDisk_1_<Snap id>_ BDAZSNAP>
```

次に例を示します。

```
/cb9b5b6d-0c60-4ed1-9cd7-7aaf054b899f_DataDisk_1_1600405027_BDAZSNAP
```

4

Microsoft Azure Stack のバックアップとリストアの実行

この章では以下の項目について説明しています。

- Microsoft Azure 仮想マシンのバックアップについて
- Microsoft Azure Stack の仮想マシンのリストアについて
- バックアップ、アーカイブおよびリストアインターフェースからの Microsoft Azure Stack VM のリストアシナリオについて
- 同じ場所にある Microsoft Azure Stack VM の[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]インターフェースを使用したリストア
- 同じ場所にある Microsoft Azure Stack VM の bprestore コマンドを使用したリストア
- バックアップ、アーカイブおよびリストアインターフェースを使用した Microsoft Azure Stack VM の別の場所へのリストア
- バックアップ、アーカイブおよびリストアインターフェースを使用した、変更したメタデータを持つ Microsoft Azure Stack VM の別の場所でのリストア
- bprestore コマンドを使用した、変更したメタデータを持つ Microsoft Azure VM の代替の場所へのリストア
- bprestore コマンドを使用した、変更したメタデータを持つ Microsoft Azure Stack VM の代替の領域へのリストア

Microsoft Azure 仮想マシンのバックアップについて

バックアップジョブはスケジュール設定して実行することもできれば、手動で実行することもできます。『NetBackup 管理者ガイド Vol. 1』を参照してください。

バックアップ処理の概要については、p.9 の「Microsoft Azure Stack VM のバックアップ」を参照してください。を参照してください。

バックアッププロセスは、次のステージで構成されます。

1. 事前処理: 事前処理のステージでは、BigData ポリシーで構成した最初のバックアップホストが検出をトリガします。この段階では、VM と関連するメタデータがバックアップ用に検出されします。
2. データ転送: データ転送処理中には、バックアップホストごとに 1 つの子ジョブが作成されます。

Microsoft Azure Stack の仮想マシンのリストアについて

NetBackup のバックアップ、アーカイブおよびリストアコンソールを使用して、リストア操作を管理します。

表 4-1 Microsoft Azure データのリストア

作業	参照先
リストア処理の理解	p.10 の「Microsoft Azure Stack VM のリストア」を参照してください。
リストアシナリオの理解	p.36 の「バックアップ、アーカイブおよびリストアインターフェースからの Microsoft Azure Stack VM のリストアシナリオについて」を参照してください。 p.38 の「Microsoft Azure Stack VM のリストアおよびリカバリに関する考慮事項」を参照してください。
同じ場所にある Microsoft Azure Stack VM のリストア	■ リストアウィザード p.40 の「同じ場所にある Microsoft Azure Stack VM の[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]インターフェースを使用したリストア」を参照してください。 ■ コマンドラインインターフェース p.42 の「同じ場所にある Microsoft Azure Stack VM の bprestore コマンドを使用したリストア」を参照してください。

作業	参照先
Microsoft Azure Stack VM の代替の場所へのリストア	■ リストアウィザード p.46 の「バックアップ、アーカイブおよびリストアインターフェースを使用した、変更したメタデータを持つ Microsoft Azure Stack VM の別の場所でのリストア 」を参照してください。 ■ コマンドラインインターフェース p.55 の「bprestore コマンドを使用した、変更したメタデータを持つ Microsoft Azure VM の代替の場所へのリストア」を参照してください。 p.59 の「bprestore コマンドを使用した、変更したメタデータを持つ Microsoft Azure Stack VM の代替の領域へのリストア」を参照してください。
Azure Stack の管理対象外ディスク VM の管理対象ディスク VM への移行	p.54 の「管理対象外ディスク VM の管理対象ディスク VM への変換」を参照してください。
Azure Stack VM の別の場所へのリストア	p.44 の「バックアップ、アーカイブおよびリストアインターフェースを使用した Microsoft Azure Stack VM の別の場所へのリストア」を参照してください。

バックアップ、アーカイブおよびリストアインターフェースからの Microsoft Azure Stack VM のリストアシナリオについて

バックアップ、アーカイブおよびリストアインターフェースから Microsoft Azure Stack VM をリストアする場合は、次のシナリオが可能です。

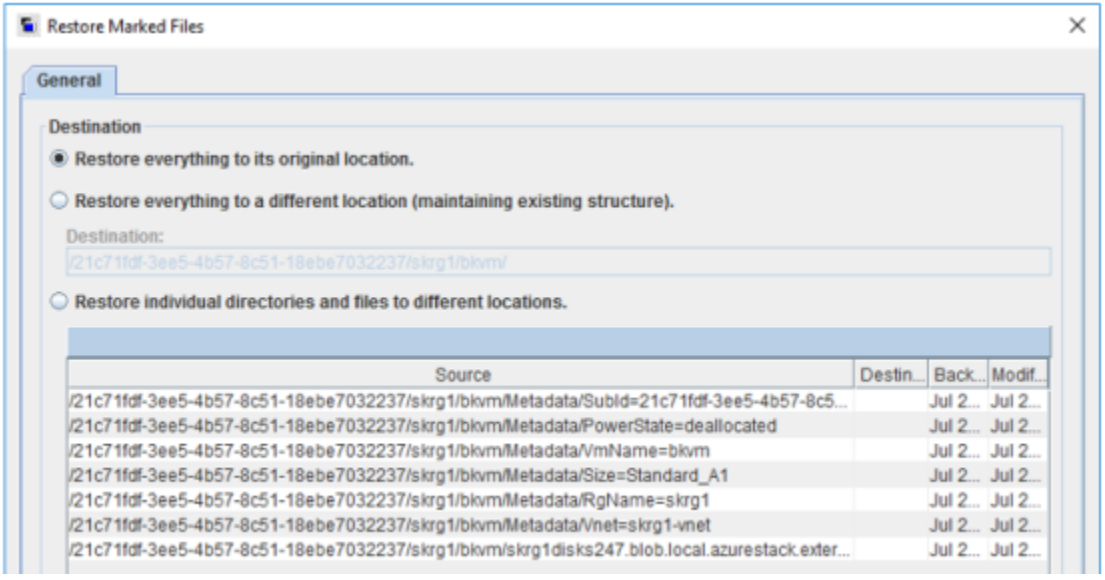
表 4-2 VM リストアのオプション

シナリオ	[マークされたファイルのリストア (Restore Marked Files)]ダイアログボックスのオプション
既存の構成を持つ Microsoft Azure Stack VM の同じ場所へのリストア (サブスクリプション ID とリソースグループ)	元の位置にすべてをリストア
既存の構成を持つ Microsoft Azure Stack VM の代替の場所へのリストア (サブスクリプション ID とリソースグループ)	すべてを異なる位置にリストア (既存の構造を維持)

シナリオ	[マークされたファイルのリストア (Restore Marked Files)]ダイアログボックスのオプション
構成を変更した Microsoft Azure Stack VM のリストア (VM メタデータと場所を含む)	個々のディレクトリやファイルを異なる位置にリストア

オプションは、バックアップ、アーカイブおよびリストアインターフェースに詳細を入力し、[マークされたファイルのリストア (Restore Marked Files)]ダイアログボックスに進むと利用可能になります。

図 4-1 [マークされたファイルのリストア (Restore Marked Files)]ダイアログボックスのリストアオプション



リストアのワークフロー

次の図は、リストアのワークフローの概要を示しています。

図 4-2 Azure Stack VM の元の場所へのリストア

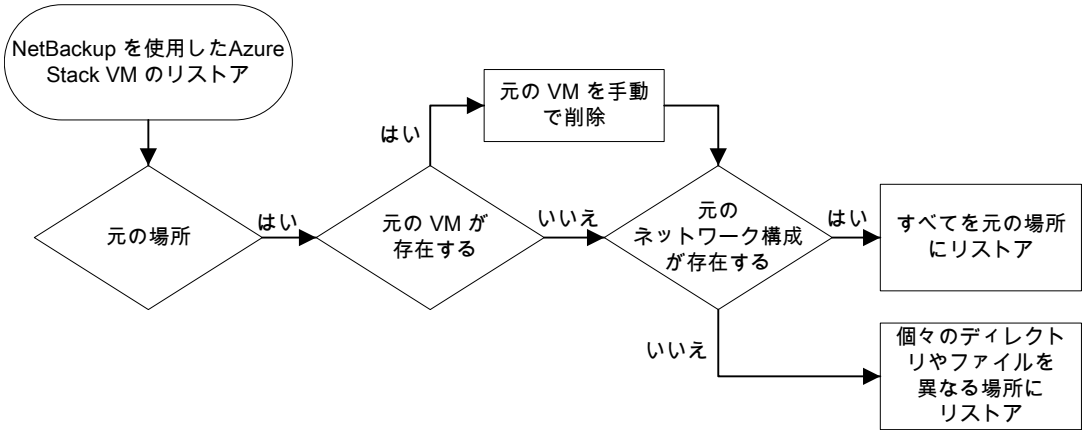
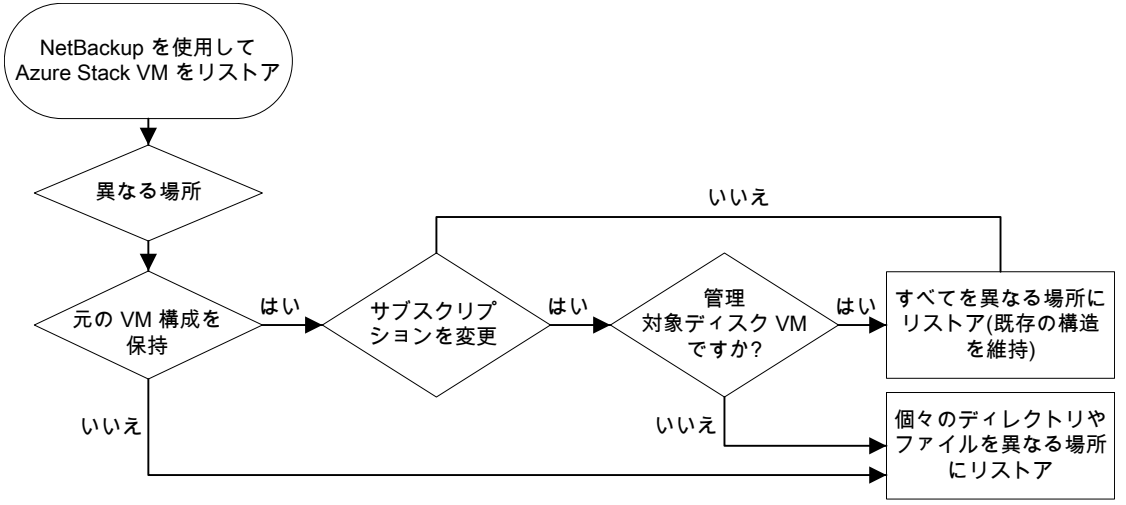


図 4-3 Azure Stack VM の別の場所へのリストア



Microsoft Azure Stack VM のリストアおよびリカバリに関する考慮事項

- NetBackup が VM データのリストア処理をトリガし、操作が成功すると、NetBackup に成功の状態が表示されます。Azure Stack ポータルを使用して、VM の作成プロセスを監視します。
- VM のリカバリ操作が失敗した場合、リストア中に作成されたリソースを手動で削除する必要があります。このリソースには IP アドレス、NIC、OS、およびデータディスクが

含まれる場合があります。リソースは接尾辞 -restorenic-、-restoreip-、-RESTORE- とその後に続くタイムスタンプで識別できます。

- VM が元の場所にまだ存在する場合は、同じ名前の VM をリストアできません。また、VM のリカバリを成功させるには、Vnet (バックアップされた VM の NSG) が存在する必要があります。
- VM をリカバリするには、NetBackup の役割に、指定したサブスクリプションとリソースグループに対するアクセス権が必要です。
- NetBackup では、次の VM のプロパティをリカバリできます。
  - タグ
  - OS ブート診断の設定
- その他のプロパティや構成設定については、リカバリが完了した後に手動で適用する必要があります。
- リカバリ中、ホスト名は変更されず、バックアップされる VM と同じままになります。VM にログオンし、OS コマンドを使用して、ホスト名を変更する必要があります。
- 元の場所にリストアするときは、新しいネットワーク構成が作成されます。1 つの NIC が作成され、バックアップ中に VM が接続されていた仮想ネットワークに接続されます。この手順の結果、MAC アドレスと IP アドレスは変更されます。
- VM リカバリ操作中に構成を更新する場合は、いずれかのメタデータファイルをダブルクリックして、すべてのメタデータファイルを選択する必要があります。変更する設定に対応するファイルの名前を変更できます。
- VM リカバリ操作中に構成を更新する場合、VM とは異なるリソースグループに属するリソースグループまたはネットワークセキュリティグループを次のように指定できます。

  Vnet=<*ResourceGroup_Name*>/<*virtual_network_Name*>
  Nsg=<*ResourceGroup_Name*>/<*NetworkSecurityGroup_Name*>

  ResourceGroup_Name が指定されず、仮想ネットワークまたは NetworkSecurityGroup 名がバックアップされる VM と同じ場合、バックアップ時の仮想ネットワークまたは NetworkSecurityGroup がリカバリ操作中に使用されます。それ以外の場合、指定された仮想ネットワークが、VM と同じリソースグループに属すると見なされます。
- 管理対象外ディスク VM から管理対象ディスク VM への変換はサポートされますが、その逆はサポートされません。つまり、管理対象ディスク VM は管理対象外ディスク VM に変換できません。
- インポートしたイメージからのリストアは、BAR GUI ではサポートされません。リストアを実行するには、bprestore コマンドを使用する必要があります。
- 代替領域のリストアは、bprestore コマンドを介してのみサポートされます。

同じ場所にある Microsoft Azure Stack VM の［バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)］インターフェースを使用したリストア

このトピックでは、NetBackup 管理コンソールの［バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)］インターフェースを使用して、同じ Microsoft Azure Stack 上の Microsoft Azure Stack をリストアする方法について説明します。

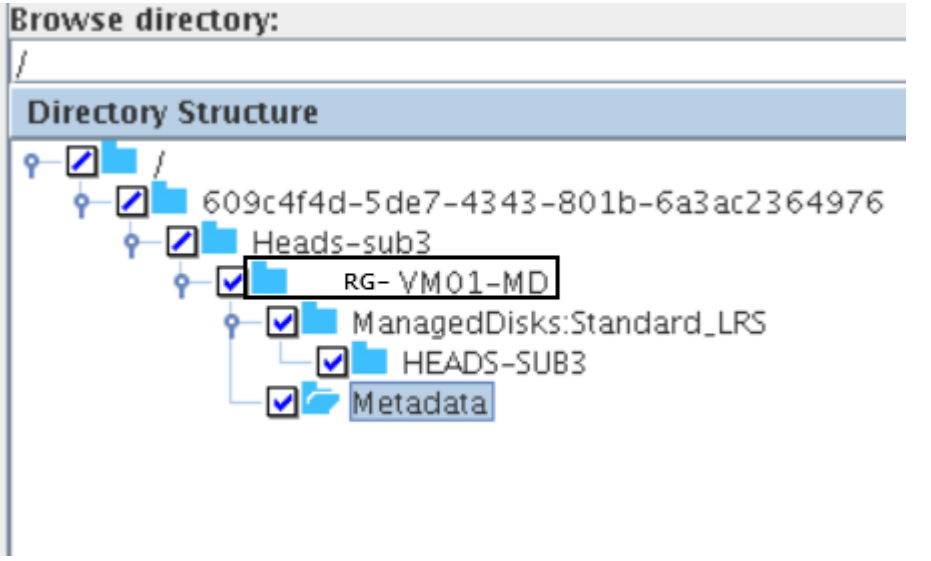
リストアを実行するために NetBackup 管理コンソールの［バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)］インターフェースを使用するには

1. ［バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)］インターフェースを開きます。
2. ［NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)］ウィザードで、リストアのソースと宛先の詳細を入力します。
   - リストア操作を実行するソースとして Microsoft Azure アプリケーションエンドポイントを指定します。
     ［リストアのソースクライアント (Source client for restores)］リストから、必要なアプリケーションサーバーを選択します。
   - バックアップホストを宛先クライアントとして指定します。
     ［リストアの宛先クライアント (Destination client for restores)］リストから、必要なバックアップホストを選択します。
   - ［NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)］ウィザードで、リストアのポリシー形式の詳細を入力します。
     ［リストアのポリシー形式 (Policy type for restores)］リストから、リストアのポリシー形式として BigData を選択します。
     ［OK］をクリックします。
3. データセット全体をリストアする適切な日付範囲を選択します。
4. ［ディレクトリの参照 (Browse directory)］で、参照するパスとしてルートディレクトリ (「/」) を指定します。
5. ［ファイル］メニュー (Windows の場合) または［処理］メニュー (UNIX の場合) から、［NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)］を選択します。
6. ［バックアップ履歴 (Backup History)］に移動し、リストアするバックアップイメージを選択します。

7 ［ディレクトリ構造 (Directory Structure)］ペインで、［ディレクトリ (Directory)］を展開します。

そのディレクトリの下にある後続のすべてのファイルとフォルダが、［選択されたディレクトリの内容 (Contents of Selected Directory)］ペインに表示されます。

8 ［選択されたディレクトリの内容 (Contents of Selected Directory)］ペインで、リストアする Microsoft Azure VM にチェックマークを付けます。



9 ［リストア (Restore)］をクリックします。

10 ［マークされたファイルのリストア (Restore Marked Files)］ダイアログボックスで、要件に応じてリストアの宛先を選択します。

- バックアップを実行したのと同じ場所にファイルをリストアするには、［元の位置にすべてをリストア (Restore everything to its original location)］を選択します。

メモ: リストアシナリオについて詳しくは、「p.36 の「バックアップ、アーカイブおよびリストアインターフェースからの Microsoft Azure Stack VM のリストアシナリオについて」を参照してください。」を参照してください。

11 ［リストアの開始 (Start Restore)］をクリックします。

12 VM がリストアされてインスタンス化されたことを確認します。

13 VM がリストアされたら、Microsoft Azure Stack の管理ポータルを開いて、VM ネットワークインターフェースを必要なネットワークセキュリティグループに割り当てます。

同じ場所にある Microsoft Azure Stack VM の bprestore コマンドを使用したリストア

bprestore コマンドを使用して、同じリソースグループ内の Microsoft Azure Stack VM をリストアできます。

バックアップの場所と同じ場所に Microsoft Azure データをリストアするには

1. それぞれの Windows または UNIX システムで、管理者または root ユーザーとして NetBackup マスターサーバーにログインします。
2. NetBackup マスターサーバー上で、適切な値を指定して、次のコマンドを実行します。

   ```
   bprestore -S master_server -D backup_host-C client -t 44 -X -s
   <bktime> -e <bktime> -L progress log -f listfile | filenames
   "/subscription ID/resource group/VmName"
   ```

   手順の詳細:

   ```
   -S master_server
   ```

   このオプションでは、NetBackup マスターサーバー名を指定します。

   ```
   -D backup host
   ```

   バックアップホストの名前を指定します。

   ```
   -C client
   ```

   ファイルのリストア元のバックアップまたはアーカイブの検索に使用するソースとして、設定サーバーを指定します。この名前は、NetBackup カタログに表示される名前と一致している必要があります。

   ```
   -f listfile
   ```

   このオプションでは、リストアを行うファイルのリストを含むファイル (`listfile`) を指定します。このオプションは、ファイル名オプション (`filenames`) の代わりに使用できます。`listfile` では、各ファイルパスを個別の行に指定する必要があります。

   ```
   -L progress_log
   ```

   このオプションでは、進捗情報を書き込むホワイトリストファイルパスの名前を指定します。

   ```
   -t 44
   ```

   ポリシー形式として BigData を指定します。

   ```
   "/subscription ID/resource group/VmName"
   ```

   リストアする Microsoft Azure Stack VM を指定します。

   ```
   -X -s bktime -e date
   ```

   バックアップイメージの選択の開始日と終了日。X オプションを使用して、人間が読み取り可能な形式でなくタイムスタンプを指定するには、『コマンドリファレンスガイド』で `bprestore` コマンドを参照してください。

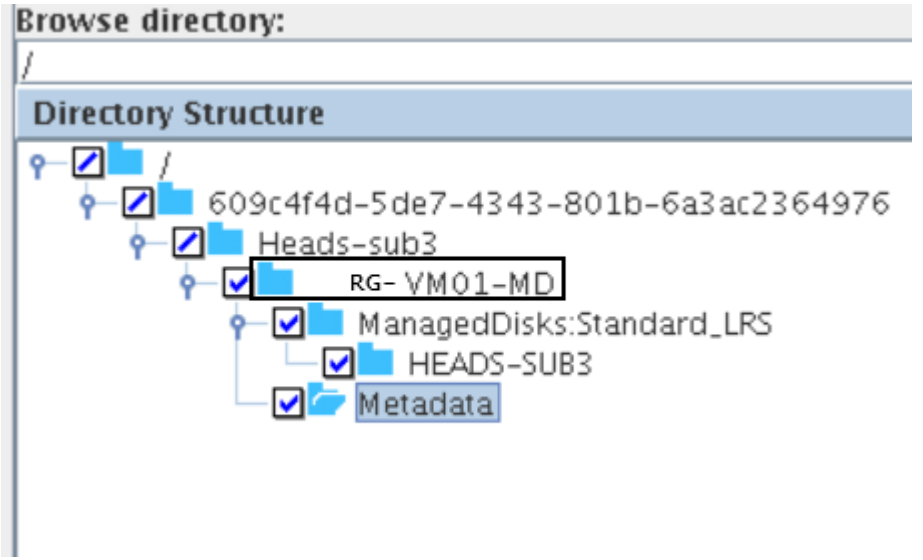
バックアップ、アーカイブおよびリストアインターフェースを使用した Microsoft Azure Stack VM の別の場所へのリストア

このトピックでは、NetBackup 管理コンソールのバックアップ、アーカイブおよびリストアインターフェースを使用して、同じ Microsoft Azure Stack 上の Microsoft Azure Stack を別の RG またはサブスクリプションにリストアする方法について説明します。

リストアを実行するために NetBackup 管理コンソールのバックアップ、アーカイブおよびリストアインターフェースを使用するには

1. バックアップ、アーカイブおよびリストアインターフェースを開きます。
2. [NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)]ウィザードで、リストアのソースと宛先の詳細を入力します。
   - リストア操作を実行するソースとして Microsoft Azure アプリケーションエンドポイントを指定します。[リストアのソースクライアント (Source client for restores)]リストから、必要なアプリケーションサーバーを選択します。
   - バックアップホストを宛先クライアントとして指定します。[リストアの宛先クライアント (Destination client for restores)]リストから、必要なバックアップホストを選択します。バックアップホストが VM をバックアップしたメディアサーバーの場合、リストアはより短時間になります。
   - [NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)]ウィザードで、リストアのポリシー形式の詳細を入力します。[リストアのポリシー形式 (Policy type for restores)]リストから、リストアのポリシー形式として BigData を選択します。[OK]をクリックします。
3. データセット全体をリストアする適切な日付範囲を選択します。
4. [ディレクトリの参照 (Browse directory)]で、参照するパスとしてルートディレクトリ(「/」) を指定します。
5. [ファイル]メニュー (Windows の場合) または[処理]メニュー (UNIX の場合) から、[NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)]を選択します。
6. [バックアップ履歴 (Backup History)]に移動し、リストアするバックアップイメージを選択します。
7. [ディレクトリ構造 (Directory Structure)]ペインで、[ディレクトリ (Directory)]を展開します。そのディレクトリの下にある後続のすべてのファイルとフォルダが、[選択されたディレクトリの内容 (Contents of Selected Directory)]ペインに表示されます。

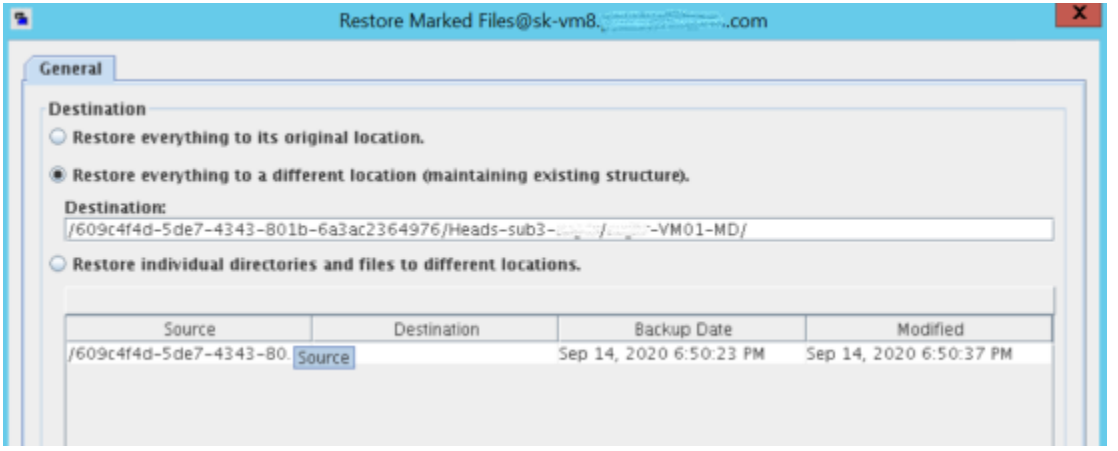
8 [選択されたディレクトリの内容 (Contents of Selected Directory)]ペインで、リストアする Microsoft Azure VM にチェックマークを付けます。



9 [リストア (Restore)]をクリックします。

10 [マークされたファイルのリストア (Restore Marked Files)]ダイアログボックスで、要件に応じてリストアの宛先を選択します。

VM を異なる RG またはサブスクリプションにリストアするには、[すべてを異なる位置にリストア (Restore everything to a different location)]を選択します。



VM パスの形式は /<subId>/<RgName>/<VmName> です。

このオプションでは、次のことを実行できます。

- リストア対象の VM が元の場所 (たとえば、同じサブスクリプションと RG) にリストアされるが、別の名前を使用して VM 名を変更します。
- RG を変更し、ターゲットサブスクリプションを同じにします。この場合、VM の RG のみが変更され、VM のネットワーク設定を含むすべての設定が同じままになります。
- ターゲットサブスクリプションと RG を変更します。これは管理対象ディスク VM のリストアでのみサポートされます。
  - 管理対象ディスク VM のネットワーク設定を別のターゲットサブスクリプションにリストアします。
  - Vnet および NSG がターゲット RG 内に存在する場合は、それらが NIC の作成時に使用されます。Vnet が存在しない場合は、ターゲット RG 内の NSG が使用されます。ターゲットサブスクリプションの異なる RG 内でも同じように検索されます。

メモ: リストアシナリオについて詳しくは、「バックアップ、アーカイブおよびリストアインターフェースからの Microsoft Azure Stack VM のリストアシナリオについて」を参照してください。

---

11 [リストアの開始 (Start Restore)] をクリックします。

12 VM がリストアされてインスタンス化されたことを確認します。

バックアップ、アーカイブおよびリストアインターフェースを使用した、変更したメタデータを持つ Microsoft Azure Stack VM の別の場所でのリストア

NetBackup では、Microsoft Azure Stack VM を別のリソースグループにリストアするか、VM のメタデータを変更して、同じリソースグループにリストアできます。この種類のリストア方法は、リダイレクトリストアと呼ばれます。

このトピックでは、NetBackup 管理コンソールのバックアップ、アーカイブおよびリストアインターフェースを使用して、Microsoft Azure Stack 上の代替の場所または別のリソースグループに変更したメタデータを持つ Microsoft Azure Stack VM をリストアする方法について説明します。

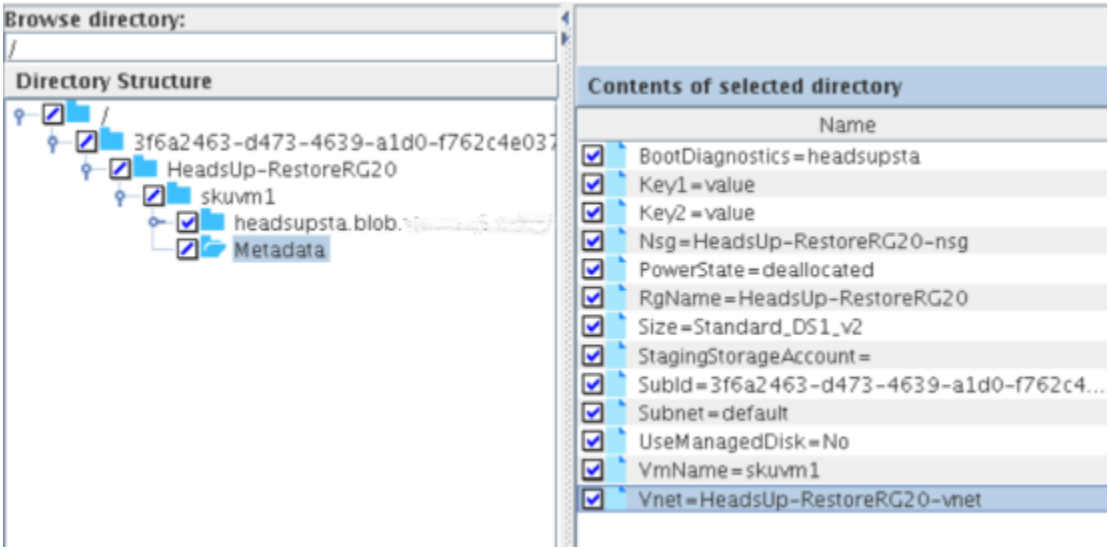
リストアを実行するために **NetBackup** 管理コンソールのバックアップ、アーカイブおよびリストアインターフェースを使用するには

1. バックアップ、アーカイブおよびリストアインターフェースを開きます。
2. [NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)]ウィザードで、リストアのソースと宛先の詳細を入力します。
   - リストア操作を実行するソースとして Microsoft Azure アプリケーションエンドポイントを指定します。
     [リストアのソースクライアント (Source client for restores)]リストから、必要なアプリケーションサーバーを選択します。
   - バックアップホストを宛先クライアントとして指定します。
     [リストアの宛先クライアント (Destination client for restores)]リストから、必要なバックアップホストを選択します。
   - [NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)]ウィザードで、リストアのポリシー形式の詳細を入力します。
     [リストアのポリシー形式 (Policy type for restores)]リストから、リストアのポリシー形式として BigData を選択します。
     [OK]をクリックします。
3. データセット全体をリストアする適切な日付範囲を選択します。
4. [ディレクトリの参照 (Browse directory)]で、参照するパスとしてルートディレクトリ(「/」) を指定します。
5. [ファイル]メニュー (Windows の場合) または[処理]メニュー (UNIX の場合) から、[NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)]を選択します。
6. [バックアップ履歴 (Backup History)]に移動し、リストアするバックアップイメージを選択します。
7. [ディレクトリ構造 (Directory Structure)]ペインで、[ディレクトリ (Directory)]を展開します。

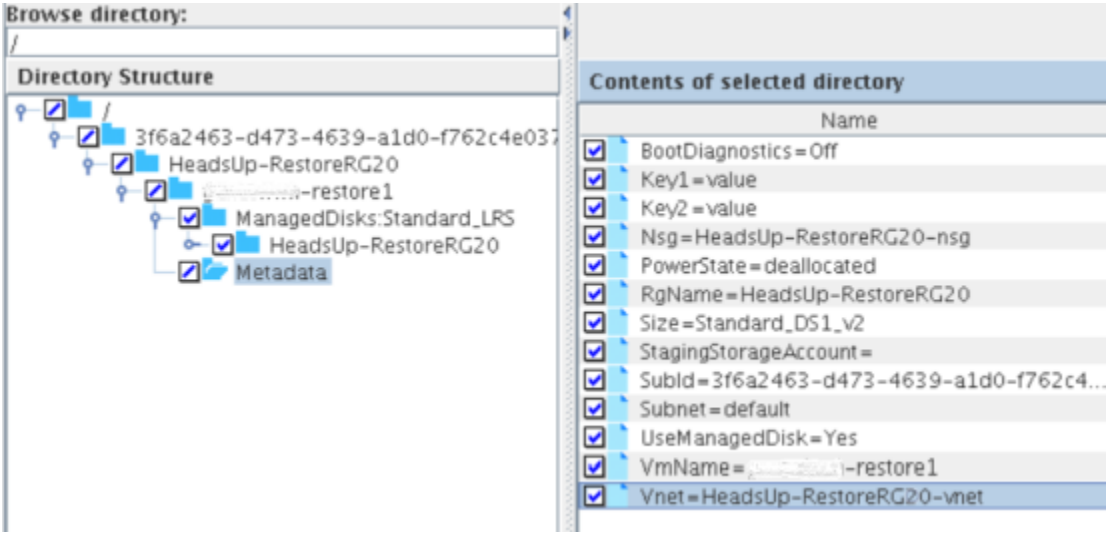
   そのディレクトリの下にある後続のすべてのファイルとフォルダが、[選択されたディレクトリの内容 (Contents of Selected Directory)]ペインに表示されます。

8 リストアする VM を選択します。ストレージアカウントのディレクトリが選択されていることを確認します。

次に例を示します。



管理対象ディスク VM の場合、ManagedDisks の下にあるすべてのディスクを選択します。



ディスク RG、ディスク名などのディスクのプロパティを変更する場合は、個々のディスクファイルを選択します。

メモ: すべてのメタデータファイルを選択し、変更するメタデータのみを変更、または名前を変更する必要があります。

リストア対象としてマーク付けされたファイルのダイアログボックスにすべてのオプションが表示されるように、Metadata フォルダを選択し、選択列の内容にあるすべてのメタデータを選択解除して選択します。

---

9 選択した[メタデータ (Metadata)]ディレクトリをクリックし、[選択されたディレクトリの内容 (Contents of Selected Directory)]ペインで、変更するメタデータを選択します。

次のメタデータを変更できます。

メタデータまたはプロパティ	説明	デフォルト値	有効な値
VmName	VM の名前。	バックアップ中の VM の名前。	リソースグループ内で一意の、有効な VM 名。
PowerState	リストア後の VM の状態。	バックアップ中の VM の電源状態。	`Stopped`、`Deallocate`、または `Running`
Size	Microsoft Azure Stack で推奨される形式での VM のサイズ。詳しくは、「Azure Stack でサポートされている仮想マシンのサイズ」を参照してください。	バックアップ中の VM のサイズ。	有効な VM サイズ。
Vnet	VM が含まれる仮想ネットワーク。	バックアップ中の VM の Vnet。	ターゲットサブスクリプション内の仮想ネットワーク。 空の値が `Vnet, RgName-vnet` などに対して指定された場合、VM のターゲット RG 内に存在する場合は使用されます。
Nsg	VM のネットワークセキュリティグループ。	バックアップ中の VM の NSG。	ターゲットサブスクリプション内の NSG。 空の値が `Nsg` などに対して指定された場合、VM にネットワークセキュリティグループは設定されません。
RgName	Microsoft Azure Stack VM の場所またはリソースグループ。	バックアップ中の VM のリソースグループ。	ターゲットサブスクリプションの一部であるリソースグループ。
Storage Account	管理対象外 VM ディスクが格納されているストレージアカウント。これは VHD パスの一部であり、個別のメタデータファイルではありません。	バックアップ中の VM のストレージアカウント。	ターゲットサブスクリプションの一部である有効なストレージアカウント。

メタデータまたはプロパティ	説明	デフォルト値	有効な値
SubId	Microsoft Azure Stack のサブスクリプション ID。	バックアップ中の VM のサブスクリプション ID。	NetBackup の役割がアクセスできるサブスクリプション ID。
Boot Diagnostics	ブート診断の設定。 リストア時に指定されたブート診断ストレージアカウントが宛先サブスクリプションまたは Azure Stack に存在しない場合は、ブート診断の設定は無効になります	バックアップ中の管理対象外 VM のブート診断の設定。	ターゲットサブスクリプションの一部である有効なストレージアカウント。
UseManagedDisk	VM に管理対象ディスクまたは管理対象外ディスクがあります	バックアップされた VM の管理対象ディスクの設定。	管理対象ディスクを備えた VM の場合は Yes。 管理対象外ディスクを備えた VM の場合は No。
StagingStorageAccount	管理対象ディスク VM のリストア中に一時 VHD ファイルを作成するために使用するストレージアカウント。	空	ターゲットサブスクリプションの一部である有効なストレージアカウント。
Storage Account Type	管理対象ディスクのストレージ形式。これは、管理対象ディスクのパスの一部であり、メタデータファイルではありません。 `StorageAccountType` がバックアップ中に検出されない場合。ユーザーがリストア中に指定する必要があります	バックアップされた管理対象ディスクのストレージアカウントの種類。	Azure Stack によってサポートされているストレージアカウントの種類の文字列 (Standard_LRS、Premium_LRS など)。
Disk RG	管理対象ディスクのリソースグループ。これは、管理対象ディスクのパスの一部であり、メタデータファイルではありません。	バックアップ管理対象ディスクのリソースグループ	ターゲットサブスクリプションの一部であるリソースグループ。

10 ［リストア (Restore)］をクリックします。

11 [マークされたファイルのリストア (Restore Marked Files)]ダイアログボックスで[個々のディレクトリやファイルを異なる位置にリストア (Restore individual directories and files to different locations)]を選択します。

メモ: リストアシナリオについて詳しくは、「p.36 の「バックアップ、アーカイブおよびリストアインターフェースからの Microsoft Azure Stack VM のリストアシナリオについて」を参照してください。」を参照してください。

変更するメタデータの値それぞれについて、値を選択して[選択された宛先の変更 (Change Selected Destination(s))]をクリックし、[宛先 (Destination)]フィールドで URL の末尾のメタデータの値を変更します。

たとえば、VmName を変更する場合は、次のように変更します。

/21c71fdf-3ee5-4b57-8c51-18ebe7032237/SKRG/MSvm15/Metadata/VmName=*OldVmName*
から

/21c71fdf-3ee5-4b57-8c51-18ebe7032237/SKRG/MSvm15/Metadata/VmName=*NewVmName*

ここで、VMName はキーで *OldVmName* は値です。メタデータとその値は Key=Value の形式になります。変更するすべてのメタデータの値を修正する必要があります。

管理対象ディスクプロパティの変更

```
Change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HeadsUp-RestoreRG20/skvm1/
ManagedDisks:Standard_LRS/HeadsUp-RestoreRG20/
skvm1_OsDisk_1_be667512b2a44ecfb1ffa43506aaa48c-RESTORE-1598299429

to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HeadsUp-RestoreRG20/skvm1/
ManagedDisks:Premium_LRS/HeadsUp-RestoreRG30/osdisk_1
```

管理対象外ディスクストレージアカウントの変更

```
Change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HeadsUp-RestoreRG20/skuvm1/
headsupsta.blob.tasz.vxi.vwx.com/vhds/skuvm1-UMD-RESTORE-1599155872.vhd

to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HeadsUp-RestoreRG20/skuvm1/
stasub2testrgg.blob.tasz2.vxi.vwx.com/vhds/skuvm1-UMD-RESTORE-1599155872.vhd
```

メモ: VM サイズのメタデータの場合は、Microsoft Azure Stack 推奨の形式で変更後の値を指定します。新しい VM のサイズは、サブスクリプションの範囲内である必要があります。

詳しくは、
https://docs.microsoft.com/ja-jp/azure/azure-stack/user/azure-stack-vm-sizes
を参照してください。

12 [リストアの開始 (Start Restore)]をクリックします。

13 Azure Stack の管理ポータルを使用して、VM の作成プロセスを表示します。

管理対象外ディスク VM の管理対象ディスク VM への変換

BAR GUI を使用する場合、リストア時に設定を変更できるようにするために、オプション 3 の[個々のディレクトリやファイルを異なる位置にリストア (Restore individual directories and files to different locations)]を使用する必要があります。

次のファイルエントリの名前を変更します。

```
/d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/Metadata/UseManagedDisk=no
=>
/d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/Metadata/UseManagedDisk=yes

/d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/
nbusrgdisks439.blob.mtcazs.wwtatc.com/vhds/nbu-an-um-vm1120200625233142.vhd
=>
/d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/
ManagedDisks:Standard_LRS/NBU-SamRG2/osdisk
```

メモ: 小文字のストレージアカウント形式はディスク作成 API ではサポートされず、Standard_LRS、Premium_LRS などとして指定する必要があります。

古いプラグインを使用した管理対象外ディスク VM バックアップの管理対象ディスク VM への変換

BAR GUI を使用する場合、リストア時に設定を変更できるようにするために、オプション 3 の[個々のディレクトリやファイルを異なる位置にリストア (Restore individual directories and files to different locations)]を使用する必要があります。

次のファイルエントリの名前を変更します。

```
d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/Metadata/Key1=value
=>
/d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/Metadata/UseManagedDisk=yes

/d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/
nbusrgdisks439.blob.mtcazs.wwtatc.com/vhds/nbu-anil-um-vm1120200625233142.vhd
=>
/d182ecd4-23c5-4fde-90f3-8951146a385e/NBU-SRG/nbu-an-um-vm11/
ManagedDisks:Standard_LRS/NBU-SRG2/osdisk
```

メモ: 名前変更ファイルを使用してステージングストレージアカウントを指定することはできません。また、プラグイン構成ファイルの一部として指定する必要があります。

小文字のストレージアカウント形式はディスク作成 API ではサポートされず、Standard_LRS、Premium_LRS などとして指定する必要があります。

bprestore コマンドを使用した、変更したメタデータを持つ Microsoft Azure VM の代替の場所へのリストア

1. 次の bplist コマンドを実行して、ファイルの一覧を表示します。

   ```
   bplist -S master_server -C configuration_server_01 -unix_files
   -R 3 -t 44 -X -s <bktime> -e <bktime>
   "/21c71fdf-3ee5-4b57-8c51-18ebe7032237/skrg1/bkvm15" > listfile
   ```

   エディタで listfile を開き、行末の特殊文字を削除します。ディレクトリに対応するスラッシュ / で終わるすべてのパスを削除します。

2. 手順 1 で説明したパラメータに、変更した値を使用して、NetBackup マスターサーバーで次のコマンドを実行します。

   ```
   bprestore -S master_server -D backup_host -C client -R rename_file
   -t 44 -L progress log -f listfile | filenames
   ```

   手順の詳細:

   ```
   -S master_server
   ```

   このオプションでは、NetBackup マスターサーバー名を指定します。

   ```
   -D backup host
   ```

   バックアップホストの名前を指定します。

   ```
   -C client
   ```

ファイルのリストア元のバックアップまたはアーカイブの検索に使用するソースとして、設定サーバーを指定します。この名前は、NetBackup カタログに表示される名前と一致している必要があります。

`-f listfile`

このオプションでは、リストアを行うファイルのリストを含むファイル (`listfile`) を指定します。このオプションは、ファイル名オプション (`filenames`) の代わりに使用できます。`listfile` では、各ファイルパスを個別の行に指定する必要があります。

`-L progress_log`

このオプションでは、進捗情報を書き込むホワイトリストファイルパスの名前を指定します。

`-t 44`

ポリシー形式として BigData を指定します。

`-R rename_file`

このオプションでは、代替パスへのリストアのために名前を変更するファイル名を指定します。

次に例を示します。

```
bprestore.exe -S master_server_01 -D backup_host_01 -C
configuration_server_01 -t 44 -L "<install_dir>¥logs¥restore.log"
 -R "<install_dir>¥renam_file_path¥restore.chg" -f listfile
```

rename ファイルの例

管理対象外ディスクの管理対象ディスクへの変換

```
change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
headsrg4disks2.blob.vtasazs1.vxi.ver.com/vhds/sr-VM02-UMD20200826032144.vhd
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
ManagedDisks:Standard_LRS/Heads-RestoreRG20/osdisk1
```

管理対象外ディスク VM の管理対象ディスク VM への同じ RG への変換

```
change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/VmName=sr-VM02-UMD
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/VmName=sr-VM02-UMD-2md2
```

```
change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD
/Metadata/UseManagedDisk=No
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/UseManagedDisk=Yes

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
headsuprg4disks2.blob.vtasazs1.vxi.ver.com/vhds/
sr-VM02-UMD20200826032144.vhd
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
ManagedDisks:Standard_LRS/HEADS-SUB3-SR/osdisk1
```

別のサブスクリプションを使用した管理対象外ディスク VM の管理対象ディスク VM への変換

```
change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/Vnet=Heads-sub3-sr-vnet
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/Vnet=Heads-RestoreRG20-vnet

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/VmName=sr-VM02-UMD
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/VmName=sr-VM02-UMD-2md2

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/UseManagedDisk=No
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/UseManagedDisk=Yes

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/SubId=609c4f4d-5de7-4343-801b-6a3ac2364976
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
```

```
Metadata/SubId=3f6a2463-d473-4639-a1d0-f762c4e0371a

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/Size=Standard_DS1_v2
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/Size=Standard_DS2_v2

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/RgName=Heads-sub3-sr
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/RgName=Heads-RestoreRG20

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/Nsg=sr-VM02-UMD-nsg
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/Nsg=HeadsUp-RestoreRG20-nsg

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/BootDiagnostics=headsuprg4diag398
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
Metadata/BootDiagnostics=headsupsta

change
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
headsuprg4disks2.blob.vtasazs1.vxi.ver.com/vhds/
sr-VM02-UMD20200826032144.vhd
to
/609c4f4d-5de7-4343-801b-6a3ac2364976/Heads-sub3-sr/sr-VM02-UMD/
ManagedDisks:Standard_LRS/HeadsUp-RestoreRG20/osdisk1
```

メモ: NetBackup インストールパスの一部としてまだ組み込まれていない、<rename_file_path>、<progress_log_path> などのすべてのファイルパスをホワイトリストに載せたことを確認します。

---

bprestore コマンドを使用した、変更したメタデータを持つ Microsoft Azure Stack VM の代替の領域へのリストア

NetBackup では、Microsoft Azure Stack データを別のリソースグループにリストアして、メタデータを変更できます。この種類のリストア方法は、リダイレクトリストアと呼ばれます。

Microsoft Azure Stack のリダイレクトリストアを実行するには

1 *rename_file* および *listfile* の値を次のように変更します。

パラメータ	値
rename_file	代替領域の ARM エンドポイントを指定する ALT_APPLICATION_SERVER= エントリを追加します。 VmName メタデータを更新する場合は、次のように追加します。 変更前: /21c71fdf-3ee5-4b57-8c51-18ebe7032237/SKRG/MSvm15 /Metadata/VmName=*OldVmName* 変更後: /21c71fdf-3ee5-4b57-8c51-18ebe7032237/SKRG/MSvm15/ Metadata/VmName=*NewVmName* VM の電源状態を変更するには、次のように追加します。 変更前: /21c71fdf-3ee5-4b57-8c51-18ebe7032237/SKRG/MSvm15 /Metadata/PowerState=*running* 変更後: /21c71fdf-3ee5-4b57-8c51-18ebe7032237/SKRG/MSvm15 /Metadata/PowerState=*deallocate* ファイルパスは / (スラッシュ) で始まる必要があります。 変更するすべてのメタデータオプションに、新しいエントリを追加します。 **メモ:** VM サイズのメタデータの場合は、Microsoft Azure Stack 推奨の形式で変更後の値を指定します。新しい VM のサイズは、サブスクリプションの範囲内である必要があります。 詳しくは、「Azure Stack でサポートされている仮想マシンのサイズ」を参照してください。
listfile	リストアするすべての Microsoft Azure ファイルのリスト

2 代替の Azure Stack のクレデンシャル情報をフェッチするには、次の操作を行います。

新しい Azure Stack ARM エンドポイントの tpconfig エントリを追加します。

ソースクライアントの暗号化クレデンシャルファイルの名前と一致するように、/usr/openv/var/global で、生成された暗号化ファイルの名前を変更します。

たとえば、arm-end-point1.conf がソースクライアントの暗号化ファイルで、arm-end-point2.conf が代替クライアントの暗号化ファイルです。bprestore コマンドを実行する前に、arm-end-point1.conf のコピーを arm-end-point1.conf_org に作成し、arm-end-point2.conf を arm-end-point1.conf にコピーします。

3 ファイルのリストは、次の bplist コマンドを実行して取得できます。

```
bplist -S master_server -C configuration_server_01 -unix_files
-R 3 -t 44 -X -s <bktime> -e <bktime>
"/21c71fdf-3ee5-4b57-8c51-18ebe7032237/skrg1/bkvm15" > listfile
```

エディタで listfile を開き、行末の特殊文字を削除します。ディレクトリに対応する / で終わるすべてのパスを削除します。

4 手順 1 で説明したパラメータに、変更した値を使用して、NetBackup マスターサーバーで次のコマンドを実行します。

```
bprestore -S master_server -D backup_host-C client -R rename_file
-t 44 -X -s bktime -e bktime -L progress log -f listfile |
filenames
```

手順の詳細:

```
-S master_server
```

このオプションでは、NetBackup マスターサーバー名を指定します。

```
-D backup_host
```

バックアップホストの名前を指定します。

```
-C client
```

ファイルのリストア元のバックアップまたはアーカイブの検索に使用するソースとして、設定サーバーを指定します。この名前は、NetBackup カタログに表示される名前と一致している必要があります。

```
-f listfile
```

このオプションでは、リストアを行うファイルのリストを含むファイル (listfile) を指定します。このオプションは、ファイル名オプション (filenames) の代わりに使用できます。listfile では、各ファイルパスを個別の行に指定する必要があります。

```
-L progress_log
```

このオプションでは、進捗情報を書き込むホワイトリストファイルパスの名前を指定します。

```
-t 44
```

ポリシー形式として BigData を指定します。

```
-R rename_file
```

このオプションでは、代替パスへのリストアのために名前を変更するファイル名を指定します。

```
ALT_APPLICATION_SERVER=management.vtsz2.vxi.vs.com
```

```
change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/BootDiagnostics=hupsta
to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HeadsUp-RestoreRG20/skuvm1/Metadata/BootDiagnostics=stasub2testrgg

change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/Nsg=HUp-RestoreRG20-nsg
to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/Nsg=rs-md-21-nsg

change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/RgName=HUp-RestoreRG20
to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/RgName=rshney-perf-set6

change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/
SubId=3f6a2463-d473-4639-a1d0-f762c4e0371a
to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/
SubId=b326ed58-7537-4c81-b2ac-5b16d6a524b3

change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/VmName=skuvm1
to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/VmName=skuvm1-restore2

change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/Vnet=HUp-RestoreRG20-vnet
to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/Metadata/Vnet=rshney-perf-set6-vnet

change
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/HUpsta.blob.vtszs1.vxi.vs.com/vhds/
skuvm1-UMD-RESTORE-1599155872.vhd
to
/3f6a2463-d473-4639-a1d0-f762c4e0371a/HUp-RestoreRG20/skuvm1/stasub2testrgg.blob.vtszs2.vxi.veritas.com/
vhds/skuvm1-UMD-RESTORE-1599155872.vhd
```

5

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。

NetBackup for Microsoft Azure のデバッグログについて

NetBackup は、バックアップ操作とリストア操作に関連するさまざまなプロセスのプロセス固有のログを保持します。これらのログを調べて、問題の根本原因を見つけることができます。

これらのログフォルダは、ログの記録用にあらかじめ存在している必要があります。これらのフォルダが存在しない場合は作成する必要があります。

次のディレクトリにあるログフォルダ

- Windows の場合: `install_path¥NetBackup¥logs`
- UNIX または Linux の場合: `/usr/openv/netbackup/logs`

表 5-1 Microsoft Azure に関連する NetBackup ログ

ログフォルダ	メッセージの内容	ログの場所
`install_path/NetBackup/logs/bpVMutil`	ポリシーの構成	マスターサーバー
`install_path/NetBackup/logs/nbaapidiscv`	BigData フレームワーク、検出、および Microsoft Azure 構成ファイルのログ	バックアップホスト
`install_path/NetBackup/logs/bpbrm`	ポリシー検証、バックアップ、およびリストア操作	メディアサーバー
`install_path/NetBackup/logs/bpbkar`	バックアップ	バックアップホスト
`install_path/NetBackup/logs/tar`	リストアおよび Microsoft Azure 構成ファイル	バックアップホスト

詳しくは、『NetBackup ログリファレンスガイド』を参照してください。

NetBackup を使用した Microsoft Azure の保護に関する既知の制限事項

次の表に、NetBackup を使用した Microsoft Azure の保護に関する既知の制限事項を示します。

表 5-2 既知の制限事項

制限事項	回避方法
NetBackup 8.1.2 から 9.0 へのアップグレード後に認証トークンを取得できません。	暗号化アルゴリズムと復号アルゴリズムは NetBackup 9.0 で更新されます。既存のすべての Microsoft Azure サーバーを NetBackup から削除し、NetBackup を 9.0 にアップグレードした後で再び追加します。

制限事項	回避方法
正常に完了した以外のプロビジョニング状態の VM は正常にバックアップされますが、バックアップ時の VM の不整合状態が原因でリストアが失敗する可能性があります。	VM のリストアが失敗した場合は、ログファイルを調べて、バックアップ実行時の VM のプロビジョニング状態が正常な完了かどうか、またはそれ以外かどうかを確認します。プロビジョニングの状態が正常な完了以外である場合、その VM はリストアできません。

バックアップがエラー 6662 で失敗する

バックアップが次のエラーで失敗します。

```
(6662) Unable to find the configuration file.
```

回避方法:

クレデンシャルファイルを作成し、ファイルへのパスをホワイトリストに追加し、ファイルパスが tpconfig コマンドで指定されていることを確認します。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。

バックアップがエラー 6661 で失敗する

バックアップが次のエラーで失敗します。

```
(6661) Unable to find the configuration parameter.
```

回避方法:

tpconfigコマンドで指定されているクレデンシャルファイルに、正しい構成オプションが追加されていることを確認します。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。

バックアップがエラー 6646 で失敗する

バックアップが次のエラーで失敗します。

```
(6646) Unable to communicate with the server.
```

回避方法:

バックアップ操作を再度実行します。Azure Stack が過負荷になっていることがエラーの原因である可能性があります。

バックアップがエラー 6629 で失敗する

バックアップが次のエラーで失敗します。

```
(6629) Unable to complete the operation. Failed to authorize
the user or the server.
```

回避方法:

- 構成オプションとクレデンシャルファイルの値を検証します。
- `./tpconfig -dappservers` コマンドを実行するときの値を確認します。
- Azure Stack ユーザー名とパスワードの値を確認します。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。

バックアップがエラー 6626 で失敗する

バックアップが次のエラーで失敗します。

```
(6626) The server name is invalid.
```

回避方法:

ARM エンドポイントの名前を確認します。

バックアップがエラー 6630 で失敗する

バックアップが次のエラーで失敗します。

```
(6630) Unable to process the request because the server resources
are either busy or unavailable. Retry the operation.
```

回避方法:

- Azure Stack ポータルからバックアップ対象の値を確認します。
- バックアップの選択肢のクレデンシャルファイルの `AuthResource` の値を確認します。
- バックアップポリシーとバックアップの選択肢のクレデンシャルファイル内に、適切な ARM エンドポイントを追加したことを確認します。
- Azure Stack サブスクリプションのカスタムの役割を作成したことを確認します。

クレデンシャルファイルの変更後、`tpconfig -update` コマンドを実行します。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。

リストアがエラー 2850 で失敗する

リストアが次のエラーで失敗します。

```
(2850) Restore error.
```

回避方法:

有効なサポートされる VM のサイズを指定します。

バックアップがエラー 1 で失敗する

バックアップが次のエラーで失敗します。

```
(1) The requested operation was partially successful.
```

エラーの詳細には、バックアップされなかった VHD についても示されます。

回避方法:

次のパラメータが正しく構成されていることを確認します。

- FETCH_STORAGE_KEYS=true の場合、NetBackup 管理者が Azure Stack のストレージアカウントおよびアクセスキーのフェッチとアクセスのための権限を持っていることを確認します。
- FETCH_STORAGE_KEYS=false の場合、必要なストレージアカウントとアクセスキーをクレデンシャルファイルに追加したことを確認します。
  クレデンシャルファイルの変更後、`tpconfig -update` コマンドを実行します。

p.18 の「NetBackup 管理者にアクセス権を付与するための Microsoft Azure Stack カスタムロールの追加」を参照してください。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。

エラー 9101 で Azure Stack クレデンシャルの NetBackup への追加が失敗する

このエラーは、`tpconfig` コマンド内のファイルパスに指定された二重引用符形式に競合がある場合に発生します。

たとえば、application_server_conf "/usr/openv/var/global/azure.conf" です。

回避方法:

二重引用符なしでファイルパスを指定するか、コマンドプロンプトに二重引用符を手動で入力します。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。

エラー 7610 で Azure Stack クレデンシャルの NetBackup への追加が失敗する

このエラーは、クレデンシャルファイル内に形式エラーがある場合に発生します。

回避方法:

クレデンシャルファイル内の構文または形式を確認します。

クレデンシャルファイルの変更後、tpconfig -update コマンドを実行します。

p.29 の「NetBackup での Microsoft Azure Stack クレデンシャルの追加」を参照してください。