オンプレミスのアプリケーションデータのバックアップとリストア

BlueXP backup and recovery

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-backup-recovery/concept-protect-app-data-to-cloud.html on April 18, 2024. Always check docs.netapp.com for the latest.

目次

オンプレミスのアプリケーションデータのバックアップとリストア 1
オンプレミスアプリケーションのデータを保護 1
SnapCenter サーバを登録します 2
アプリケーションをバックアップするポリシーを作成する 4
オンプレミスアプリケーションのデータをAmazon Web Servicesにバックアップ 4
オンプレミスアプリケーションのデータをMicrosoft Azureにバックアップ 5
オンプレミスアプリケーションのデータをGoogle Cloud Platformにバックアップ 6
オンプレミスのアプリケーションデータをStorageGRID にバックアップ 7
アプリケーションの保護を管理します 9
オンプレミスアプリケーションのデータをリストア 13

オンプレミスのアプリケーションデータのバックアップとリストア

オンプレミスアプリケーションのデータを保護

アプリケーション向けのBlueXPバックアップ/リカバリ機能は、オンプレミスのONTAPプライマリからクラウドプロバイダに至るまで、アプリケーションと整合性のあるSnapshotを保護するためのデータ保護機能を提供します。

Oracle、Microsoft SQL、SAP HANA、MongoDB、MySQL、 オンプレミスのONTAPシステムからAmazon Web Services、Microsoft Azure、Google Cloud Platform、StorageGRIDに至るまで、PostgreSQLアプリケーションのデータをバックアップできます。

アプリケーションのBlueXPのバックアップとリカバリの詳細については、以下を参照してください。

- "BlueXPのバックアップ/リカバリ機能とSnapCenter を使用した、アプリケーション対応のバックアップ"
- "BlueXPの「Backup and Recovery for Applications」ポッドキャスト"

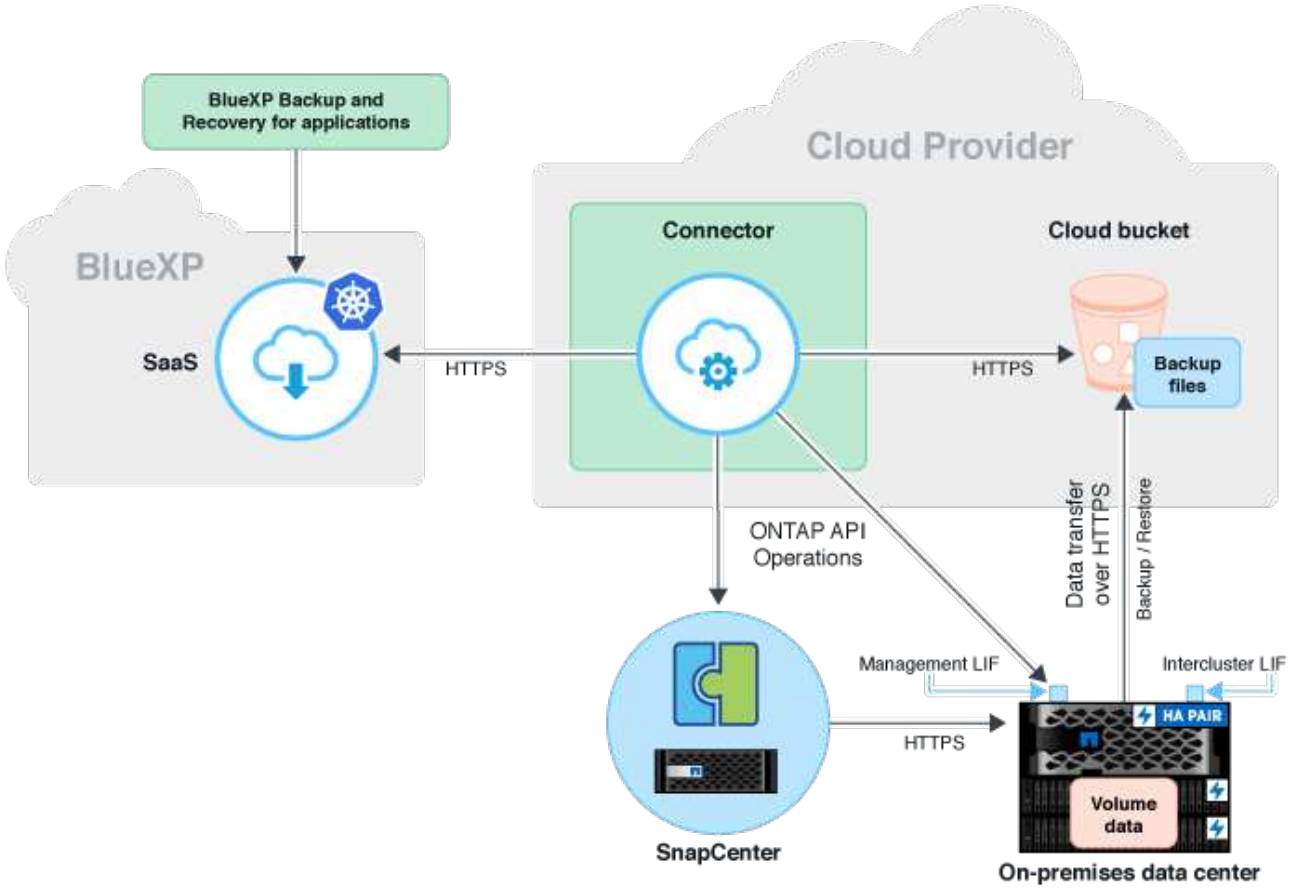
要件

クラウドプロバイダへのアプリケーションデータのバックアップを開始する前に、次の要件を読み、サポートされる構成があることを確認してください。

- ONTAP 9.8以降
- BlueXP
- SnapCenterサーバ4.6以降
  - 次の機能を使用する場合は、SnapCenterサーバ4.7以降を使用してください。
    - オンプレミスのセカンダリストレージからバックアップを保護
    - SAP HANAアプリケーションを保護
    - VMware環境上にあるOracleアプリケーションやSQLアプリケーションを保護
    - バックアップのストレージエクスポート
    - バックアップの非アクティブ化
    - SnapCenter サーバを登録解除します
  - 次の機能を使用する場合は、SnapCenterサーバ4.9以降を使用してください。
    - Oracleデータベースバックアップをマウントします
    - 代替ストレージにリストアします
  - MongoDB、MySQL、PostgreSQLのアプリケーションを保護する場合は、SnapCenter Server 4.9P1を使用する必要があります。
- SnapCenter サーバでは、各アプリケーションに使用可能なバックアップを少なくとも 1 つ用意する必要があります
- SnapCenterで、BlueXPのポリシーとラベルがない、または同じラベルのない日次、週次、または月次の

ポリシーを1つ以上設定

次の図は、クラウドにバックアップする場合の各コンポーネントと、それらの間の準備に必要な接続を示しています。



SnapCenter サーバを登録します

SnapCenterAdminロールのユーザだけが、SnapCenter サーバ4.6以降が実行されているホストを登録できます。BlueXPには複数のSnapCenter サーバホストを登録できます。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [SnapCenter サーバ *] をクリックします。
3. [* SnapCenter サーバーの登録 *] をクリックします。
4. 次の情報を指定します。
   a. SnapCenter Server フィールドで、 SnapCenter サーバホストの FQDN または IP アドレスを指定します。
   b. [ポート]フィールドで、SnapCenter サーバホストが実行されているポート番号を指定します。

      SnapCenter サーバとBlueXPの間で通信するためには、ポートが開いていることを確認する必要があ

ります。

c. [タグ] フィールドで、 SnapCenter サーバーにタグを付けるサイト名、都市名、またはカスタム名を指定します。

   タグはカンマで区切って指定します。

d. Username and Password フィールドで、 SnapCenterAdmin ロールを持つユーザのクレデンシャルを指定します。

5. コネクター*ドロップダウンからコネクターを選択します。
6. [*Register] をクリックします。

完了後

[* バックアップと復元 **>** アプリケーション *] をクリックして、登録済み SnapCenter サーバ・ホストを使用して保護されているすべてのアプリケーションを表示します。デフォルトでは、アプリケーションは毎日午前0時に自動的に検出されます。

サポートされるアプリケーションとその構成は次のとおりです。

- Oracleデータベース：
  - フルバックアップ（データ+ログ）：少なくとも1つの日次、週次、または月次スケジュールで作成されます
  - SAN、NFS、VMDK - SAN、VMDK - NFS、RDM
- Microsoft SQL Server データベース：
  - スタンドアロン、フェイルオーバークラスタインスタンス、および可用性グループ
  - フルバックアップ：日単位、週単位、または月単位のスケジュールを少なくとも 1 つずつ設定して作成します
  - SAN、VMDK SAN、VMDK - NFS、RDM
- SAP HANAデータベース：
  - シングルコンテナ1.x
  - 複数のデータベースコンテナ2.x
  - HANAシステムレプリケーション（HSR）

    プライマリサイトとセカンダリサイトの両方に少なくとも1つのバックアップが必要です。プロアクティブな障害にするか、セカンダリへの遅延フェイルオーバーを行うかを選択できます。

  - HANAバイナリ、HANAアーカイブログボリューム、HANA共有ボリュームなどの非データボリューム（NDV）リソース
- MongoDB
- MySQL
- PostgreSQL

次のデータベースは表示されません。

- バックアップがないデータベース

- オンデマンドまたは毎時ポリシーのみのデータベース
- NVMe上にあるOracleデータベース

アプリケーションをバックアップするポリシーを作成する

アプリケーションデータをクラウドにバックアップするポリシーを作成する必要があります。

作業を開始する前に

- オブジェクトストアからアーカイブストレージにバックアップを移動する場合は、必要なバージョンのONTAPを使用していることを確認します。
  - Amazon Web Servicesを使用している場合は、ONTAP 9.10.1以降を使用している必要があります
  - Microsoft Azureを使用している場合は、ONTAP 9.10.1以降を使用している必要があります
  - Google Cloudを使用している場合は、ONTAP 9.12.1以降を使用してください
  - StorageGRIDを使用している場合は、ONTAP 9.12.1以降を使用してください。
- 各クラウドプロバイダにアーカイブアクセス階層を設定する必要があります。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [設定]ドロップダウンから、[ポリシー>*ポリシーの作成*]をクリックします。
3. [ポリシーの詳細]セクションで、ポリシー名を指定します。
4. 保持セクションで、保持タイプの1つを選択し、保持するバックアップの数を指定します。
5. バックアップストレージソースとして、プライマリまたはセカンダリを選択します。
6. （オプション）コストを最適化するために一定の日数が経過したバックアップをオブジェクトストアからアーカイブストレージに移動する場合は、「*ティアBackup to Archival *」チェックボックスを選択します。
7. [作成（ Create ）] をクリックします。

> アプリケーションに関連付けられているポリシーを編集または削除することはできません。

オンプレミスアプリケーションのデータを**Amazon Web Services**にバックアップ

いくつかの手順を実行して、ONTAP からAmazon Web Servicesにアプリケーションデータをバックアップします。

BlueXPは、データロックとランサムウェア対策をサポートしています。ONTAPクラスタがONTAP 9.11.1以降で実行されていて、アーカイブストレージを設定していない場合は、上書き、削除、ランサムウェアの脅威からバックアップを保護できます。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。
   c. * 作業環境の追加 * をクリックします。
5. クラウドプロバイダとして「* Amazon Web Services *」を選択します。
   a. AWS アカウントを指定します。
   b. AWS Access Key フィールドで、キーを指定します。
   c. AWS Secret Key フィールドで、パスワードを指定します。
   d. バックアップを作成するリージョンを選択します。
   e. IPスペースを指定してください。
   f. ポリシーでアーカイブストレージを設定している場合は、アーカイブ階層を選択します。

      アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。
6. データロックとランサムウェア対策を設定
7. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

オンプレミスアプリケーションのデータを**Microsoft Azure**にバックアップ

いくつかの手順を実行して、ONTAP からMicrosoft Azureにアプリケーションデータをバックアップします。

BlueXPは、データロックとランサムウェア対策をサポートしています。ONTAPクラスタがONTAP 9.12.1以降で実行されていて、アーカイブストレージを設定していない場合は、上書き、削除、ランサムウェアの脅威からバックアップを保護できます。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。
   c. * 作業環境の追加 * をクリックします。
5. クラウドプロバイダとして「* Microsoft Azure *」を選択します。
   a. Azure サブスクリプション ID を指定します。
   b. バックアップを作成するリージョンを選択します。
   c. 新しいリソースグループを作成するか、既存のリソースグループを使用してください。
   d. IPスペースを指定してください。
   e. ポリシーでアーカイブストレージを設定している場合は、アーカイブ階層を選択します。

      アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。
6. データロックとランサムウェア対策を設定
7. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

オンプレミスアプリケーションのデータを**Google Cloud Platform**にバックアップ

いくつかの手順を実行して、ONTAP からGoogle Cloud Platformにアプリケーションデータをバックアップします。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。

4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。

   c. * 作業環境の追加 * をクリックします。
5. クラウドプロバイダとして「* Google Cloud Platform *」を選択します。
   a. バックアップ用に Google Cloud Storage バケットを作成する Google Cloud Project を選択します。
   b. Google Cloud Access Keyフィールドで、キーを指定します。
   c. Google Cloud Secret Keyフィールドで、パスワードを指定します。
   d. バックアップを作成するリージョンを選択します。
   e. IPスペースを指定してください。
   f. アーカイブ階層を選択します。

      アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。

6. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

オンプレミスのアプリケーションデータを**StorageGRID** にバックアップ

アプリケーションデータをONTAP からStorageGRID にバックアップするには、いくつかの手順を実行します。

BlueXPは、データロックとランサムウェア対策をサポートしています。ONTAPクラスタがONTAP 9.11.1以降で実行されている場合、StorageGRIDシステムは11.6.0.3以降です。アーカイブストレージを設定していない場合は、上書き、削除、ランサムウェアの脅威からバックアップを保護できます。

作業を開始する前に

StorageGRID にデータをバックアップするときは、オンプレミスのコネクタが必要です。新しいコネクタをインストールするか、現在選択されているコネクタがオンプレミスにあることを確認する必要があります。コネクタは、インターネットに接続するかどうかに関係なく、サイトにインストールできます。

詳細については、を参照してください "StorageGRID のコネクタを作成します"。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。
   c. * 作業環境の追加 * をクリックします。
5. 「* StorageGRID *」を選択します。
   a. StorageGRID サーバのFQDNと、StorageGRID サーバが実行されているポートを指定します。

      FQDN：portの形式で詳細を入力します。
   b. [Access Key]フィールドで、キーを指定します。
   c. Secret Keyフィールドで、パスワードを指定します。
   d. IPスペースを指定してください。
   e. ポリシーでアーカイブストレージを設定している場合は、アーカイブ階層を指定します。

を選択した場合は	実行する手順
AWS	i. ドロップダウンからStorageGRIDを選択するか、StorageGRIDクラスタを追加します。 ii. AWS アカウントを指定します。 iii. AWS Access Key フィールドで、キーを指定します。 iv. AWS Secret Key フィールドで、パスワードを指定します。 v. バックアップを作成するリージョンを選択します。 vi. [保存（ Save ）] をクリックします。

を選択した場合は	実行する手順
Azure	i. ドロップダウンからStorageGRIDクラスタを選択するか、クラスタを追加します。 ii. Azure サブスクリプション ID を指定します。 iii. バックアップを作成するリージョンを選択します。 iv. 新しいリソースグループを作成するか、既存のリソースグループを使用してください。 v. [保存（ Save ）] をクリックします。

アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。

6. データロックとランサムウェア対策を設定
7. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

アプリケーションの保護を管理します

アプリケーションの保護を管理するには、ポリシーの表示、バックアップの表示、データベースレイアウト、ポリシー、リソースグループへの変更の確認、すべての処理の監視をBlueXP UIから実行します。

ポリシーを表示します

すべてのポリシーを表示できます。これらの各ポリシーについて、関連するすべてのアプリケーションの詳細を表示すると表示されます。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [ポリシー *] をクリックします。
3. 詳細を表示するポリシーに対応する **View Details** をクリックします。

   関連するアプリケーションがリスト表示されます。

   アプリケーションに関連付けられているポリシーを編集または削除することはできません。

を実行して、クラウド拡張SnapCenter ポリシーを表示することもできます `Get-SmResources` SnapCenter のコマンドレット。
コマンドレットで使用できるパラメータとその説明は、Get-Helpコマンドnameで確認できます。

クラウド上のバックアップを表示します

クラウド上のバックアップは、BlueXP UIで確認できます。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * 詳細を表示 * をクリックします。

> バックアップが表示されるまでの時間は、ONTAPのデフォルトのレプリケーションスケジュールによって異なります。

- Oracleデータベースの場合は、データバックアップとログバックアップの両方、各バックアップのSystem Change Number（SCN；システム変更番号）、各バックアップの終了日が表示されます。データバックアップのみを選択し、データベースを元の場所にリストアできます。データバックアップとログバックアップを別の場所にマウントできます。
- Microsoft SQL Server データベースの場合は、各バックアップのフルバックアップと終了日だけが表示されます。バックアップを選択して、元の場所または別の場所にデータベースをリストアできます。
- Microsoft SQL Serverインスタンスの場合は、そのインスタンスのデータベースのバックアップが表示されます。
- SAP HANAデータベースの場合は、各バックアップのデータバックアップと終了日だけが表示されます。バックアップを選択して、特定のホストでストレージのエクスポートを実行できます。
- MongoDB、MySQL、PostgreSQLでは、データバックアップと各バックアップの終了日のみが表示されます。バックアップを選択して、特定のホストでストレージのエクスポートを実行できます。

> クラウド保護を有効にする前に作成したバックアップはリストア対象として表示されません。

これらのバックアップは、を実行して確認することもできます `Get-SmBackup` SnapCenter のコマンドレット。
コマンドレットで使用できるパラメータとその説明は、Get-Helpコマンドnameで確認できます。

バックアップを無効にします

オブジェクトストアに移動されたバックアップは、SnapCenterとオブジェクトストアの両方から削除できます。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応し、[Deactivate Backup]をクリックします。

   デフォルトではこのチェックボックスがオンになっており、オブジェクトストアに移動されたすべてのバックアップがSnapCenterとオブジェクトストアの両方から削除されます。

   チェックボックスをオフにすると、バックアップはオブジェクトストアにのみ保持されますが、アプリケーションレベルのリストアには使用できません。あとでこのアプリケーションのバックアップをアクティブ化すると、オブジェクトストアに保持されているバックアップはリストア対象のリストに表示されません。

3. [バックアップの非アクティブ化]*をクリックします。

データベースレイアウトの変更

ボリュームがデータベースに追加されると、SnapCenter サーバは、ポリシーおよびスケジュールに従って、新しいボリューム上のSnapshotに自動的にラベルを付けます。これらの新しいボリュームにはオブジェクトストアエンドポイントは設定されません。次の手順を実行してボリュームを更新する必要があります。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [SnapCenter サーバ *] をクリックします。
3. をクリックします ••• アプリケーションをホストしている SnapCenter サーバーに対応し、 [更新] をクリックします。

   新しいボリュームが検出されます。

4. をクリックします ••• アプリケーションに対応し、 * 保護の更新 * をクリックして、新しいボリュームのクラウド保護を有効にします。
   - クラウドプロバイダの設定後にアプリケーションにストレージボリュームを追加すると、SnapCenter サーバは、アプリケーションが存在する新しいバックアップのラベルをSnapshotに付けます。
   - 削除したボリュームが他のアプリケーションで使用されていない場合は、オブジェクトストア関係を手動で削除する必要があります。
   - アプリケーションインベントリを更新すると、アプリケーションの現在のストレージレイアウトが反映されます。

ポリシーまたはリソースグループの変更

SnapCenter ポリシーまたはリソースグループに変更がある場合は、保護関係を更新する必要があります。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 [* 保護の更新 *] をクリックします。

SnapCenter サーバを登録解除します

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [SnapCenter サーバ *] をクリックします。
3. をクリックします ••• SnapCenter サーバーに対応して、*登録解除*をクリックします。

   デフォルトではこのチェックボックスがオンになっており、オブジェクトストアに移動されたすべてのバックアップがSnapCenterとオブジェクトストアの両方から削除されます。

   チェックボックスをオフにすると、バックアップはオブジェクトストアにのみ保持されますが、アプリケーションレベルのリストアには使用できません。あとでこのアプリケーションのバックアップをアクティブ化すると、オブジェクトストアに保持されているバックアップはリストア対象のリストに表示されません。

ジョブを監視します

すべてのクラウドバックアップ処理に対してジョブが作成されます。すべてのジョブと、各タスクの一部として実行されるすべてのサブタスクを監視できます。

手順

1. [バックアップとリカバリ>*ジョブ監視*]をクリックします。

   処理を開始すると、ジョブが開始されたことを示すウィンドウが表示されます。リンクをクリックするとジョブを監視できます。

2. プライマリタスクをクリックすると、これらの各サブタスクのサブタスクとステータスが表示されます。

CA 証明書を設定します

環境のセキュリティを強化する場合は、CA署名証明書を設定します。

BlueXP ConnectorでSnapCenterのCA署名証明書を設定します

SnapCenterの証明書を検証できるように、BlueXP ConnectorでSnapCenterのCA署名証明書を設定する必要があります。

作業を開始する前に

BlueXPコネクタで次のコマンドを実行して_<base_mount_path>_を取得する必要があります。

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

手順

1. コネクタにログインします。
   ```
   cd <base_mount_path> mkdir -p server/certificate
   ```
2. ルートCAファイルと中間CAファイルを_<base_mount_path>/ server/certificate_directoryにコピーします。

   CAファイルは.pem形式である必要があります。

3. CRLファイルがある場合は、次の手順を実行します。
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. <base_mount_path>ファイルを_CRL/server/crl_ディレクトリにコピーします。
4. cloudmanager_snapcenterに接続し、config.ymlのenableCACertをtrueに変更します。
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert:
   false/enableCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. cloudmanager_snapcenterコンテナを再起動します。
   ```
   sudo docker restart cloudmanager_snapcenter
   ```

BlueXP ConnectorのCA署名証明書を設定します

SnapCenterで2way SSLが有効になっている場合、コネクタがSnapCenterに接続しているときにCA証明書を

クライアント証明書として使用するには、コネクタで次の手順を実行する必要があります。

作業を開始する前に

次のコマンドを実行して_<base_mount_path>_を取得する必要があります。

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

手順

1. コネクタにログインします。
   ```
   cd <base_mount_path> mkdir -p client/certificate
   ```
2. CA署名証明書とキーファイルをコネクタの_<base_mount_path> / client/certificate_にコピーします。

   ファイル名はcertificate.pemとkey.pemである必要があります。certificate.pemには、中間CAやルートCAなどの証明書のチェーン全体が含まれている必要があります。

3. certificate.p12という名前でPKCS12形式の証明書を作成し、_<base_mount_path>/client/certificate__に保持してください。

   例：openssl pkcs12 -inkey key.pem -in certificate.pem -export-out certificate.p12

4. cloudmanager_snapcenterに接続し、config.ymlのsendCACertをtrueに変更します。
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert:
   false/sendCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. cloudmanager_snapcenterコンテナを再起動します。
   ```
   sudo docker restart cloudmanager_snapcenter
   ```
6. SnapCenterで次の手順を実行して、コネクタから送信された証明書を検証します。
   a. SnapCenterサーバホストにログインします。
   b. **>**[検索の開始]*をクリックします。
   c. mmcと入力し、* Enter*キーを押します。
   d. 「 * はい * 」をクリックします。
   e. [ファイル]メニューの*[スナップインの追加と削除]*をクリックします。
   f. **>**[追加]**>**[コンピュータアカウント]**>**[次へ]*をクリックします。
   g. **>**[完了]*をクリックします。
   h. コンソールに追加するスナップインがない場合は、*[OK]*をクリックします。
   i. コンソールツリーで、*[証明書]*をダブルクリックします。
   j. [Trusted Root Certification Authorities]ストア*を右クリックします。
   k. をクリックして証明書をインポートし、[証明書のインポートウィザード]*の手順に従います。

オンプレミスアプリケーションのデータをリストア

Oracle データベースをリストアします

Oracleデータベースは元の場所にリストアすることも、別の場所にリストアすることもできます。RACデータベースの場合、バックアップが作成されたオンプレミスノードにデータがリストアされます。

制御ファイルのリストアを含むフルデータベースのみがサポートされます。アーカイブログが AFS 内にない場合は、リカバリに必要なアーカイブログが格納されている場所を指定する必要があります。

> single File Restore（SFR；単一ファイルリストア）はサポートされません。

- 手順 *

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [* フィルター条件 *] フィールドで、フィルター * タイプ * を選択し、ドロップダウンから [* Oracle*] を選択します。
3. リストアするデータベースに対応する **View Details** をクリックし、 **Restore** をクリックします。
4. [Restore options]ページで、データベースファイルをリストアする場所を指定します。

状況	手順
元の場所にリストアします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 「 * 次へ * 」をクリックします。 d. データベースの状態をリストアおよびリカバリ処理の実行に必要な状態に変更する場合は、「* Database State *」を選択します。 データベースの状態は、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。 ◦ データベースの状態が上位で、リストア処理を実行するために下位の状態に変更する必要がある場合は、このチェックボックスを選択する必要があります。 ◦ リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェックボックスをオンにしなくても自動的に状態が変更されます。 ◦ データベースが OPEN 状態で、リストアのためにデータベースが MOUNTED 状態である必要がある場合、データベースの状態はこのチェックボックスをオンにした場合にのみ変更されます。 e. リカバリの範囲を指定します。 ◦ 最後のトランザクションまでリカバリする場合は、*[すべてのログ]*を選択します。 ◦ 特定のSCNにリカバリする場合は、* Until SCN（System Change Number）*を選択します。 ◦ 特定のデータと時刻にリカバリする場合は、*[日付と時刻]*を選択します。 データベースホストのタイムゾーンの日付と時刻を指定する必要があります。 ◦ リカバリしない場合は*[リカバリなし]*を選択します。 f. アーカイブログがアクティブファイルシステムにない場合は、リカバリに必要なアーカイブログを格納する場所を指定する必要があります。 リカバリ後にデータベースを開く場合は、チェックボックスを選択します。 RAC セットアップでは、リカバリに使用され

状況	手順
別のストレージに一時的にリストアし、リストアしたファイルを元の場所にコピーします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 d. 「 * 次へ * 」をクリックします。 e. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを一時的に格納する代替ストレージの場所の詳細を指定します。 オンプレミスのONTAPシステムを選択し、オブジェクトストレージへのクラスタ接続を設定していない場合は、オブジェクトストアに関する追加情報の入力を求められます。 f. 「 * 次へ * 」をクリックします。 g. データベースの状態をリストアおよびリカバリ処理の実行に必要な状態に変更する場合は、「* Database State *」を選択します。 データベースの状態は、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。 ◦ データベースの状態が上位で、リストア処理を実行するために下位の状態に変更する必要がある場合は、このチェックボックスを選択する必要があります。 ◦ リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェックボックスをオンにしなくても自動的に状態が変更されます。 ◦ データベースが OPEN 状態で、リストアのためにデータベースが MOUNTED 状態である必要がある場合、データベースの状態はこのチェックボックスをオンにした場合にのみ変更されます。 h. リカバリの範囲を指定します。 最後のトランザクションまでリカバリする場合は、*[すべてのログ]*を選択します。

状況	手順
別の場所にリストアする	a. [別の場所にリストアする]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 代替ストレージにリストアする場合は、次の手順を実行します。 i. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 ii. 「 * 次へ * 」をクリックします。 iii. [ストレージマッピング]ページで、オブジェクトストアのデータをリストアする代替ストレージの場所の詳細を指定します。 d. 「 * 次へ * 」をクリックします。 e. [Destination host]ページで、データベースをマウントするホストを選択します。 i. （オプション）NAS環境の場合は、オブジェクトストアからリストアしたボリュームのエクスポート先となるホストのFQDNまたはIPアドレスを指定します。 ii. （オプション）SAN環境の場合は、オブジェクトストアからリストアしたボリュームのLUNをマッピングするホストのイニシエータを指定します。 f. 「 * 次へ * 」をクリックします。

5. 詳細を確認して、 * リストア * をクリックします。

[別の場所にリストア]オプションを指定すると、選択したバックアップが指定したホストにマウントされます。データベースは手動で起動する必要があります。

マウントしたバックアップは、アンマウントするまで再マウントできません。UIの* Unmount *オプションを使用して、バックアップをアンマウントできます。

Oracleデータベースを起動する方法については、を参照してください。 "ナレッジベースの記事"。

SQL Server データベースをリストアする

SQL Serverデータベースは元の場所にリストアすることも、別の場所にリストアすることもできます。

> Single File Restore（SFR；単一ファイルのリストア）、ログバックアップのリカバリ、および可用性グループの再シードはサポートされていません。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [* フィルター条件 *] フィールドで、フィルター * タイプ * を選択し、ドロップダウンから * SQL* を選択します。
3. 「 * 詳細表示 * 」をクリックすると、使用可能なすべてのバックアップが表示されます。
4. バックアップを選択し、 * リストア * をクリックします。
5. [Restore options]ページで、データベースファイルをリストアする場所を指定します。

状況	手順
元の場所にリストアします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 「 * 次へ * 」をクリックします。
別のストレージに一時的にリストアし、リストアしたファイルを元の場所にコピーします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 d. 「 * 次へ * 」をクリックします。 e. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを一時的に格納する代替ストレージの場所の詳細を指定します。 f. 「 * 次へ * 」をクリックします。

状況	手順
別の場所にリストアする	a. [別の場所にリストアする]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 「 * 次へ * 」をクリックします。 d. [Destination host]ページで、ホスト名を選択し、データベース名を指定し（オプション）、インスタンスを選択し、リストアパスを指定します。 ⓘ 代替パスに指定するファイル拡張子は、元のデータベースファイルのファイル拡張子と同じにする必要があります。 e. 「 * 次へ * 」をクリックします。

状況	手順
別のストレージに一時的にリストアし、リストアしたファイルを別の場所にコピーする	a. [別の場所にリストアする]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 d. 「 * 次へ * 」をクリックします。 e. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを一時的に格納する代替ストレージの場所の詳細を指定します。 f. 「 * 次へ * 」をクリックします。 g. [Destination host]ページで、ホスト名を選択し、データベース名を指定し（オプション）、インスタンスを選択し、リストアパスを指定します。 ⓘ 代替パスに指定するファイル拡張子は、元のデータベースファイルのファイル拡張子と同じにする必要があります。 h. 「 * 次へ * 」をクリックします。

6. [Pre-operations]*選択で、次のいずれかのオプションを選択します。
   - [リストア時に同じ名前でデータベースを上書きする] を選択して、同じ名前でデータベースをリストアします。
   - データベースをリストアし、既存のレプリケーション設定を保持するには、「 * SQL データベースのレプリケーション設定を保持 * 」を選択します。
7. [Post-operations]セクションで、追加のトランザクションログをリストアするためのデータベースの状態を指定するには、次のいずれかのオプションを選択します。
   - 必要なすべてのバックアップを今すぐリストアする場合は、 [* Operational 、 but unavailable] を選択します。

     これはデフォルトの動作で、コミットされていないトランザクションをロールバックすることでデータベースを使用可能な状態にします。バックアップを作成するまで追加のトランザクションログはリストアできません。

- コミットされていないトランザクションをロールバックせずにデータベースを非稼働状態のままにするには、 [**Non-operational, but available**] を選択します。

  追加のトランザクションログをリストアできます。データベースはリカバリされるまで使用できません。

- データベースを読み取り専用モードのままにするには、「 * 読み取り専用モード」と「使用可能 * 」を選択します。

  コミットされていないトランザクションはロールバックされますが、ロールバックされた操作がスタンバイファイルに保存されるため、リカバリ前の状態に戻すことができます。

[ディレクトリを元に戻す] オプションが有効になっている場合は、さらに多くのトランザクションログがリストアされます。トランザクションログのリストア処理が失敗した場合は、変更をロールバックできます。詳細については、 SQL Server のマニュアルを参照してください。

8. 「 * 次へ * 」をクリックします。
9. 詳細を確認して、 * リストア * をクリックします。

SAP HANAデータベースをリストア

SAP HANAデータベースは任意のホストにリストアできます。

- 手順 *

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. フィールドで、フィルタ Type を選択し、ドロップダウンから HANA *を選択します。
3. リストアするデータベースに対応する **View Details** をクリックし、 **Restore** をクリックします。
4. [Restore options]ページで、次のいずれかを指定します。
   a. NAS環境の場合は、オブジェクトストアからリストアするボリュームのエクスポート先となるホストのFQDNまたはIPアドレスを指定します。
   b. SAN環境の場合、オブジェクトストアからリストアするボリュームのLUNをマッピングするホストのイニシエータを指定します。
5. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。
6. ソースストレージに十分なスペースがないか、ソースストレージが停止している場合は、*[ストレージの場所を変更]*を選択します。

   [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。

7. 「 * 次へ * 」をクリックします。
8. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを格納する代替ストレージの場所の詳細を指定します。
9. 「 * 次へ * 」をクリックします。
10. 詳細を確認して、 * リストア * をクリックします。

この処理では、指定したホスト上の選択したバックアップのストレージエクスポートのみが実行されます。ファイルシステムを手動でマウントし、データベースを起動する必要があります。ボリュームを利用したあと、ストレージ管理者はONTAP クラスタからボリュームを削除できます。

SAP HANAデータベースを起動する方法については、を参照してください。 "TR-4667：『Overview of SAP system copy workflow with SnapCenter 』" および "TR-4667：『Overview of SAP system clone workflow with SnapCenter 』"。

MongoDB、MySQL、PostgreSQLデータベースのリストア

MongoDB、MySQL、PostgreSQLのデータベースを任意のホストにリストアできます。

- 手順 *

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. フィールドで、フィルタ Type を選択し、ドロップダウンから MongoDB 、 MySQL 、または PostgreSQL *を選択します。
3. リストアするデータベースに対応する **View Details** をクリックし、 **Restore** をクリックします。
4. [Restore options]ページで、次のいずれかを指定します。
   a. NAS環境の場合は、オブジェクトストアからリストアするボリュームのエクスポート先となるホストのFQDNまたはIPアドレスを指定します。
   b. SAN環境の場合、オブジェクトストアからリストアするボリュームのLUNをマッピングするホストのイニシエータを指定します。
5. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。
6. ソースストレージに十分なスペースがないか、ソースストレージが停止している場合は、*[ストレージの場所を変更]*を選択します。

   [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。

7. 「 * 次へ * 」をクリックします。
8. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを格納する代替ストレージの場所の詳細を指定します。
9. 「 * 次へ * 」をクリックします。
10. 詳細を確認して、 * リストア * をクリックします。

この処理では、指定したホスト上の選択したバックアップのストレージエクスポートのみが実行されます。ファイルシステムを手動でマウントし、データベースを起動する必要があります。ボリュームを利用したあと、ストレージ管理者はONTAP クラスタからボリュームを削除できます。

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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