



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 Cloud Backup

NetApp
June 20, 2022

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
オンプレミスアプリケーションのデータをクラウドにバックアップ	3
アプリケーションの保護を管理します	6
アプリケーションデータをリストアする	9

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

Cloud Backup for Applications を Cloud Manager とオンプレミスの SnapCenter に統合することで、アプリケーションと整合性のある Snapshot をオンプレミスの ONTAP からクラウドにバックアップできます。必要に応じて、クラウドからオンプレミスの SnapCenter サーバにリストアできます。

OracleおよびMicrosoft SQLアプリケーションのデータをオンプレミスのONTAP システムから次のクラウドプロバイダにバックアップできます。

- Amazon Web Services の
- Microsoft Azure



SnapCenter ソフトウェア 4.6 を使用している必要があります。

Cloud Backup for Applications の詳細については、以下を参照してください。

- ["クラウドバックアップと SnapCenter を使用したアプリケーション対応バックアップ"](#)
- ["アプリケーション向けのクラウドバックアップ"](#)

要件

アプリケーションデータを クラウド サービス にバックアップする前に、次の要件を参照して、サポートされる構成になっていることを確認してください。

- ONTAP 9.8 以降
- Cloud Manager 3.9
- SnapCenter サーバ 4.6
- 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 の、Cloud Manager の Cloud Backup for Applications ポリシーと同じラベルまたはラベルのない日次、週次、または月単位のポリシーが少なくとも 1 つ必要です。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



保護ポリシー

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には、Cloud Backup for Applications で定義されているいずれかのポリシーを使用する必要があります。



カスタムポリシーはサポートされません。

ポリシー名	ラベル	保持値
1 年ごとの LTR	毎日	366
5 年ごとの LTR	毎日	1830 年に
7 年ごとの LTR	毎週	370
10 年間の月単位 LTR	毎月	120

これらのポリシーのラベルと保持の値は、ポリシーがアプリケーションに関連付けられるまで REST API を使用して変更できます。1 つのアプリケーションに関連付けることができるポリシーは 1 つだけで、関連付けが完了すると、関連付けを解除できません。

クラウドへのアプリケーションデータのバックアップには、Cloud Backup for Applications のポリシーに加えて、少なくとも 1 つの SnapCenter ポリシーが必要です。

オンプレミスアプリケーションのデータをクラウドにバックアップ

Cloud Backup for Applications を Cloud Manager とオンプレミスの SnapCenter に統合することで、ONTAP からクラウドにアプリケーションデータをバックアップできます。

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 が実行されているホストを登録できます。複数の SnapCenter サーバホストを登録できますが、登録後に SnapCenter サーバホストを削除することはできません。

• 手順 *

1. Cloud Manager UI で、* Backup & Restore * > * Applications * の順にクリックします。
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. Port フィールドで、SnapCenter サーバが稼働しているポート番号を指定します。

SnapCenter サーバと Cloud Backup for Applications の間の通信用にポートが開いていることを確認してください。

- c. [タグ] フィールドで、SnapCenter サーバ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. [*Register] をクリックします。

• 終了後 *

[* 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。



SQL Server データベースの場合、[アプリケーション名] 列には、名前が _application_name (ホスト名) 形式で表示されます。名前を _application_name (ホスト名) _format で指定して検索する場合、SQL Server データベースの詳細は表示されません。

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：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 つ使用して作成されたフルバックアップ（データ + ログ）。

- 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ティンスタンス、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

次の Oracle データベースおよび SQL Server 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
- RDM または VMDK にあるデータベース

アプリケーションデータをバックアップ

単一のポリシーを使用して、1 つ以上のアプリケーションをクラウドで同時に保護することができます。アプリケーションを保護するために割り当てることができるのは、デフォルトの組み込みポリシーだけです。



Cloud Manager の GUI を使用している場合、一度に保護できるアプリケーションは 1 つだけです。ただし、REST API を使用する場合は、複数のアプリケーションを同時に保護できます。

SQL Server インスタンスを保護する場合、そのインスタンスの対象となるデータベースのすべてのボリュームに対してクラウド保護が設定されます。SQL Server 可用性グループを保護する場合は、その可用性グループ内のデータベースのすべてのボリュームに対してクラウド保護が設定されます。ただし、バックアップの設定に基づいて、各ボリュームから Snapshot がコピーされます。

- 手順 *
 1. Cloud Manager UI で、* Backup & Restore * > * Applications * の順にクリックします。
 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. 作業環境を追加します。

アプリケーションが実行されている SVM をホストする ONTAP クラスタを設定します。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. ONTAP クラスタの IP アドレスを指定します。
 - ii. 管理クレデンシャルを指定します。

Cloud Backup for Applications でサポートされてい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。



作業環境の詳細が更新されるまで先に進まないでください。作業環境の詳細が更新されるまでに最大 30 分かかることがあります。30 分後にウィザードを閉じ、手順 1 から再試行して作業環境の詳細を確認してください。作業環境の詳細が更新されていない場合は再試行して、正しい作業環境が追加されていることを確認してください。

4. クラウドプロバイダを選択して設定します。

Amazon Web Services を設定します

- 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. 作業環境として追加した ONTAP クラスタの IP アドレスを指定します。

Microsoft Azure を設定

- 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. 作業環境として追加した ONTAP クラスタの IP アドレスを指定します。

5. [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。

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。

次のビデオでは、データベースを保護する簡単な手順を示します。

Microsoft SQL Server backup to AWS S3 or Azure blob

Manohar V Kulkarni
Technical Marketing Engineer

© 2022 NetApp, Inc. All rights reserved.



 NetApp



アプリケーションの保護を管理します

ポリシーとバックアップを表示できます。データベース、ポリシー、またはリソースグループの変更に応じて、Cloud Manager UI から更新情報を更新できます。

ポリシーを表示します

デフォルトの組み込みポリシーをすべて表示できます。これらの各ポリシーについて、関連付けられているすべての Cloud Backup for Applications ポリシーと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、それらが表示されます。

1. [* バックアップと復元 > 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 Cloud Backup for Applications ポリシーとすべてのアプリケーションが表示されます。



Cloud Backup for Applications ポリシーは削除しないでください。

「Get-SmResources」 SnapCenter コマンドレットを実行して、クラウド拡張 SnapCenter ポリシーを表示することもできます。コマンドレットで使用できるパラメータとその説明については、Get-Help コマンドレットを実行して確認できます。または、を参照することもできます ["SnapCenter ソフトウェアコマンドレットリファレンスガイド"](#)。

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、Cloud Manager の UI で確認できます。

1. [* バックアップと復元 > 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。



表示されるバックアップの所要時間は、ONTAP のデフォルトのレプリケーションスケジュール（最大 1 時間）と Cloud Manager（最大 6 時間）によって異なります。

- Oracle データベースの場合は、バックアップごとにデータバックアップとログバックアップの両方、SCN 番号、バックアップごと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、オンプレミスの SnapCenter サーバにデータベースをリストアできます。
- 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、オンプレミスの SnapCenter サーバ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、バックアップが表示されるのではなく、そのインスタンスのデータベースだけが表示されます。



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 'Get-SmBackup' SnapCenter コマンドレットを実行して表示することもできます。コマンドレットで利用できるパラメータとその説明については、Get-Help コマンドレットを実行して確認できます。または、を参照することもできます ["SnapCenter ソフトウェアコマンドレットリファレンスガイド"](#)。

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、ポリシーとスケジュールに基づいて、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がないため、次の手順を実行して更新する必要があります。

1. [* バックアップと復元 > 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。

クラウドサービスの設定後にストレージボリュームをアプリケーションから削除すると、SnapCenter サーバは、アプリケーションが存在する Snapshot にのみラベルを付けます。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、保護を更新する必要があります。

1. [* バックアップと復元 > 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。

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。

1. [* バックアップと復元 * > * 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

CA 証明書がある場合は、ルート CA 証明書を Connector マシンに手動でコピーする必要があります。

CA 証明書がない場合は、CA 証明書を設定せずに続行できます。

• 手順 *

1. Docker エージェントからアクセス可能なボリュームに証明書をコピーします。

- 「`cd /var/lib/docker/dochels/cloudmanager_snapcenter _ volume/_data/mkdir sc_certs`」と入力します
- `chmod 777 SC_certs`

2. RootCA 証明書ファイルを Connector マシンの上のフォルダにコピーします。

```
`cp <path on connector> /<filename>/var/lib/docx/volumes/cloudmanager_snapcenter  
volume/_data/sc_certs'
```

3. CRL ファイルを、Docker エージェントからアクセス可能なボリュームにコピーします。

- 「`cd /var/lib/docker/volumes/cloudmanager_snapcenter _ volume/_data/mkdir sc_crl`」のように入力します
- `'chmod 777 SC_CRL`

4. CRL ファイルを Connector マシンの上のフォルダにコピーします。

```
cp <path on connector>  
/<filename>/var/lib/docx/volumes/cloudmanager_snapcenter volume/_data/sc_crl
```

5. 証明書と CRL ファイルをコピーしたら、Cloud Backup for Apps サービスを再起動します。

- 「`sudo Docker exec cloudmanager_snapcenter sed -i /skipscCertValidation :
true/skipSCCertValidation : false/g/opt/NetApp/cloudmanager-snapcenter agent/config/config.yml`

- 「sudo Docker restart cloudmanager_snapcenter」と入力します

アプリケーションデータをリストアする

Oracle データベースをリストアします

Oracle データベースは、同じ SnapCenter サーバホスト、同じ SVM、または同じデータベースホストにのみリストアできます。RAC データベースの場合は、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 内がない場合は、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。

• 手順 *

1. Cloud Manager UI で、* Backup & Restore * > * Applications * の順にクリックします。
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. [リストアタイプ] ページで、次の操作を実行します。
 - a. 制御ファイルとフルデータベースをリストアする場合は、「* 制御ファイル」を選択します。
 - b. リストアとリカバリに必要な場合は、「* データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

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。リストア処理を実行するために、データベースの状態を高いレベルから低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。

1. Recovery Scope ページで、次のアクションを実行します。
 - a. リカバリの範囲を指定します。

状況	手順
最後のトランザクションまでリカバリする場合	[* すべてのログ *] を選択します。
特定の System Change Number (SCN) までリカバリする場合	[* Until SCN (System Change Number)] を選択します。

状況	手順
特定の日時までリカバリする必要がある	[* 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。
リカバリが不要である場合	「 * リカバリなし * 」を選択します。
外部アーカイブログの場所を指定する	アーカイブログが AFS 内にはない場合は、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。

- b. 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る RAC インスタンスのみがリカバリ後に開きます。

2. 詳細を確認して、 * リストア * をクリックします。

SQL Server データベースをリストアする

SQL Server データベースは、同じホストまたは代替ホストにリストアできます。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. Cloud Manager UI で、 * Backup & Restore * > * Applications * の順にクリックします。
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. データベースファイルのリストア先を選択します。

オプション	説明
バックアップが作成されたホストにデータベースをリストアします	バックアップを作成した SQL Server にデータベースをリストアする場合は、このオプションを選択します。

オプション	説明
データベースを代替ホストにリストアします	<p>バックアップを作成したホストと同じまたは別のホストの別の SQL Server にデータベースをリストアする場合は、このオプションを選択します。</p> <p>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。</p> <div style="display: flex; align-items: center;">  <div> <p>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。</p> </div> </div> <p>[リストア範囲] ページに [データベースを別のホストにリストアする *] オプションが表示されない場合は、ブラウザキャッシュをクリアします。</p>

6. [* リストア前オプション *] ページで、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. [リストア後のオプション *] ページで、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。

1. 詳細を確認して、* リストア * をクリックします。

著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

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、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、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

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、またはその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り特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> 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。