従来のソリューション
E-Series Systems

NetApp
March 22, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/e-series/cloud-connector/index.html on March 22, 2024. Always check docs.netapp.com for the latest.

目次

従来のソリューション 1
Cloud Connector の場合 1

従来のソリューション

Cloud Connector の場合

SANtricity ® Cloud Connector の概要

SANtricity Cloud Connector はホストベースの Linux アプリケーションです。 E シリーズボリュームを S3 準拠のアカウント（ Amazon Simple Storage Service および NetApp StorageGRID など）および NetApp AltaVault アプライアンスへブロックベースおよびファイルベースでフルバックアップし、リカバリすることができます。

SANtricity Cloud Connector は、 RedHat および SUSE の Linux プラットフォームにインストールできるパッケージ解決策（ .bin ファイル）です。SANtricity Cloud Connector のインストールが完了したら、 AltaVault アプライアンスや既存の Amazon S3 または StorageGRID アカウントへの E シリーズボリュームのバックアップジョブとリストアジョブを実行するように設定することができます。SANtricity Cloud Connector で実行されるすべてのジョブは REST ベースの API を使用します。

SANtricity Cloud Connectorツールは廃止され、ダウンロードできなくなりました。

考慮事項

これらの手順を使用する場合は、次の点に注意してください。

- これらの手順で説明する設定ジョブとバックアップ / リストアジョブは、 SANtricity Cloud Connector のグラフィカルユーザインターフェイスバージョンに該当します。
- SANtricity Cloud Connector アプリケーションの REST API のワークフローについては、この手順では説明していません。経験豊富な開発者向けに、 SANtricity Cloud Connector の各処理について、 API ドキュメントでエンドポイントを使用できます。API ドキュメントには ' ブラウザ経由で http://<hostname.domain>:<port>/docs`` に移動することでアクセスできます

バックアップのタイプ

SANtricity Cloud Connector には、イメージベースとファイルベースの 2 種類のバックアップがあります。

- * イメージベースのバックアップ *

  イメージベースのバックアップは、 Snapshot ボリュームから生のデータブロックを読み取り、イメージと呼ばれるファイルにバックアップします。空のブロック、削除されたファイルが占有しているブロック、パーティショニングに関連付けられているブロック、ファイルシステムメタデータを含む、 Snapshot ボリューム上のすべてのデータブロックがバックアップされます。イメージバックアップには、パーティショニングスキームやファイルシステムに関係なく、すべての情報を Snapshot ボリュームを使用して格納できるという利点があります。

  イメージは、バックアップターゲットに 1 つのファイルとして格納されるのではなく、 64MB の一連のデータチャンクに分割されて格納されます。データチャンクに分割することで SANtricity Cloud Connector からバックアップターゲットへの複数の接続を利用できるため、バックアッププロセスのパフォーマンスが向上します。

  StorageGRID および Amazon Web Services （ S3 ）へのバックアップでは、データチャンクごとに別々

の暗号化キーを使用してチャンクが暗号化されます。このキーには、ユーザが指定したパスフレーズとユーザデータの SHA256 ハッシュを組み合わせた SHA256 ハッシュが使用されます。AltaVault へのバックアップでは、 AltaVault で暗号化が行われるため、 SANtricity Cloud Connector はデータチャンクを暗号化しません。

- * ファイルベースのバックアップ *

  ファイルベースのバックアップは、ファイルシステムパーティションに格納されているファイルを読み取り、 64MB の一連のデータチャンクにバックアップします。ファイルベースのバックアップでは、削除されたファイルやパーティショニングおよびファイルシステムのメタデータはバックアップされません。イメージベースのバックアップと同様に、データチャンクに分割することで SANtricity Cloud Connector からバックアップターゲットへの複数の接続を利用できるため、バックアッププロセスのパフォーマンスが向上します。

  StorageGRID および Amazon Web Services へのバックアップでは、データチャンクごとに別々の暗号化キーを使用してチャンクが暗号化されます。このキーには、ユーザが指定したパスフレーズとユーザデータの SHA256 ハッシュを組み合わせた SHA256 ハッシュが使用されます。AltaVault へのバックアップでは、 AltaVault で暗号化が行われるため、 SANtricity Cloud Connector はデータチャンクを暗号化しません。

Cloud Connector のシステム要件

ご使用のシステムが SANtricity Cloud Connector の互換性に関する要件を満たしている必要があります。

ホストハードウェアの要件

ハードウェアは、次の最小要件を満たしている必要があります。

- 最低 5 GB のメモリ、設定されている最大ヒープサイズの 4 GB
- ソフトウェアのインストールには、少なくとも 5GB の空きディスクスペースが必要です

SANtricity Cloud Connector を使用するには、 SANtricity Web サービスプロキシをインストールする必要があります。Web Services Proxy はローカルにインストールすることも、別のサーバでリモートで実行することもできます。SANtricity Web サービスプロキシのインストールについては、を参照してください "Web Services Proxy のトピック"。

サポートされているブラウザ

SANtricity Cloud Connector アプリケーションでサポートされるブラウザと最小バージョンは次のとおりです。

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge 、 EdgeHTML 12
- Safari v9.

Microsoft Internet Explorer 11 の互換表示設定を使用している場合、 SANtricity Cloud Connector アプリケーションの API ドキュメントはロードされません。Microsoft Internet Explorer 11 で API ドキュメントが正しく表示されるようにするため、互換表示設定を無効にすることを推奨します。

互換性があるストレージアレイとコントローラファームウェア

SANtricity Cloud Connector アプリケーションを使用する前に、ストレージアレイとファームウェアの互換性を確認する必要があります。

SANtricity Cloud Connector と互換性があるすべてのストレージアレイおよびファームウェアの最新のリストについては、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

互換性のあるオペレーティングシステム

SANtricity Cloud Connector 4.0 アプリケーションと互換性があり、次のオペレーティングシステムでサポートされています。

オペレーティングシステム	バージョン	アーキテクチャ
Red Hat Enterprise Linux （ RHEL ）	7.x	64 ビット
SUSE Linux Enterprise Server （ SLES ）	12.x	64 ビット

サポートされているファイルシステム

SANtricity Cloud Connector アプリケーションを使用してバックアップとリストアを実行するには、サポートされているファイルシステムを使用する必要があります。

SANtricity Cloud Connector アプリケーションでは、次のファイルシステムのバックアップ処理とリストア処理がサポートされます。

- ext2
- ext3
- ext4

SANtricity Cloud Connector をインストール

SANtricity Cloud Connector Packaged 解決策（ .bin ファイル）は、 RedHat および SUSE Linux プラットフォームでのみ使用できます。

SANtricity Cloud Connector アプリケーションは、互換性がある Linux オペレーティングシステムにグラフィカルモードまたはコンソールモードを使用してインストールできます。インストール時に、 SANtricity Cloud Connector の非 SSL と SSL のポート番号を指定する必要があります。インストールが完了すると、 SANtricity Cloud Connector はデーモンプロセスとして実行されます。

SANtricity Cloud Connectorツールは廃止され、ダウンロードできなくなりました。

作業を開始する前に

次の注意事項を確認してください。

- SANtricity Web Services Proxy が SANtricity Cloud Connector と同じサーバにすでにインストールされている場合は、非 SSL のポート番号と SSL のポート番号に競合が発生します。この場合は、 SANtricity Cloud Connector のインストール時に、非 SSL のポートと SSL のポートに適切な番号を選択してください。
- ホストのハードウェアに何らかの変更があった場合は、 SANtricity Cloud Connector アプリケーションを再インストールして暗号化の整合性を確保します。
- SANtricity Cloud Connector 3.1 で作成されたバックアップは、 SANtricity Cloud Connector バージョン 4.0 とは互換性がありません。これらのバックアップを維持する場合は、以前のバージョンの SANtricity Cloud Connector を引き続き使用する必要があります。SANtricity Cloud Connector の 3.1 と 4.0 のリリースを別々にインストールする場合は、アプリケーションのバージョンごとに一意のポート番号を割り当てる必要があります。

Device Mapper Multipath （ DM-MP ）のインストール

SANtricity Cloud Connector を実行するホストは Linux Device Mapper Multipath （ DM-MP ）も実行する必要があり、マルチパスツールパッケージがインストールされている必要があります。

SANtricity Cloud Connector の検出プロセスでは、バックアップまたはリストアの対象となるボリュームやファイルの検出と認識にマルチパスツールパッケージを使用します。Device Mapper をセットアップおよび設定する方法の詳細については、で使用している SANtricity のリリースに対応した『 SANtricity ストレージマネージャマルチパスドライバガイド』を参照してください "E シリーズおよび SANtricity のドキュメントリソース"。

Cloud Connector をインストール

SANtricity Cloud Connector は、 Linux オペレーティングシステムにグラフィカルモードまたはコンソールモードでインストールできます。

グラフィカルモード

Linux オペレーティングシステムでグラフィカルモードを使用して SANtricity Cloud Connector をインストールできます。

作業を開始する前に

SANtricity Cloud Connector をインストールするホストの場所を指定します。

手順

1. SANtricity Cloud Connector インストールファイルを目的のホストの場所にダウンロードします。
2. ターミナルウィンドウを開きます。
3. SANtricity Cloud Connector インストールファイルが格納されているディレクトリに移動します。
4. SANtricity Cloud Connector のインストールプロセスを開始します。

```
./cloudconnector-xxxx.bin -i gui
```

このコマンドでは 'xxxx' はアプリケーションのバージョン番号を示します

インストーラウィンドウが表示されます。

5. Introduction 文を確認し、 * Next * をクリックします。

   ソフトウェアのライセンス契約がインストーラウィンドウに表示されます。

6. ライセンス契約の条項に同意し、 [次へ] をクリックします。

   以前のリリースの SANtricity Cloud Connector で作成されたバックアップページが表示されます。

7. 以前のリリースの SANtricity Cloud Connector で作成されたバックアップを確認するには、「 * Next * 」をクリックします。

   以前のバージョンを維持したまま SANtricity Cloud Connector バージョン 4.0 をインストールするには、アプリケーションの各バージョンに一意のポート番号を割り当てる必要があります。

   インストーラウィンドウにインストールの選択ページが表示されます。Where would you like to Install フィールドには、デフォルトのインストールフォルダ「 /opt/netapp/santricity_cloud_connector4/ 」が表示されます

8. 次のいずれかのオプションを選択します。
   - デフォルトの場所を使用するには、 [次へ] をクリックします。
   - デフォルトの場所を変更するには、新しいフォルダの場所を入力します。Enter the Non SSL Jetty Port Number ページが表示されます。非 SSL ポートにはデフォルト値の 8080 が割り当てられています。
9. 次のいずれかのオプションを選択します。
   - デフォルトの SSL ポート番号を受け入れるには、 * Next * をクリックします。
   - デフォルトの SSL ポート番号を変更するには、新しいポート番号を入力します。
10. 次のいずれかのオプションを選択します。
    - デフォルトの非 SSL ポート番号を受け入れるには、 * Next * をクリックします。
    - デフォルトの非 SSL ポート番号を変更するには、新しいポート番号を入力します。Pre-Installation Summary ページが表示されます。
11. 表示されたインストール前の概要を確認し、 * Install * をクリックします。

    SANtricity Cloud Connector のインストールが開始され、 Webserver Daemon Setup プロンプトが表示されます。

12. [OK] をクリックして Webserver Daemon Setup プロンプトを確認します。

    「 Installation Complete 」というメッセージが表示されます。

13. 「 * Done * 」をクリックして、 SANtricity Cloud Connecter インストーラを終了します。

コンソールモード

Linux オペレーティングシステムでコンソールモードを使用して SANtricity Cloud Connector をインストールできます。

作業を開始する前に

SANtricity Cloud Connector をインストールするホストの場所を指定します。

手順

1. SANtricity Cloud Connector インストールファイルを目的の IO ホストの場所にダウンロードします。
2. ターミナルウィンドウを開きます。
3. SANtricity Cloud Connector インストールファイルが格納されているディレクトリに移動します。
4. SANtricity Cloud Connector のインストールプロセスを開始します。

   ```
   ./cloudconnector-xxxx.bin -i console
   ```

   このコマンドでは 'xxxx' はアプリケーションのバージョン番号を示します

   SANtricity Cloud Connector のインストールプロセスが開始されます。

5. Enter キーを押してインストール処理を続行します。

   ネットアップソフトウェアのエンドユーザライセンス契約がインストーラウィンドウに表示されます。

   インストールプロセスをいつでもキャンセルするには、インストーラウィンドウで「 quit 」と入力します。

6. Enter キーを押して、エンドユーザライセンス契約の各部分を進めます。

   ライセンス契約への同意を求めるメッセージがインストーラウィンドウに表示されます。

7. エンドユーザライセンス契約の条項に同意し、 SANtricity Cloud Connector のインストールを続行するには、「 Y 」と入力して、インストーラウィンドウの下に **Enter** キーを押します。

   以前のリリースの SANtricity Cloud Connector で作成されたバックアップページが表示されます。

   エンドユーザ契約の条項に同意しない場合は、「 N 」と入力してから Enter キーを押し、 SANtricity Cloud Connector のインストールプロセスを終了します。

8. 以前のリリースの SANtricity Cloud Connector で作成されたバックアップを確認するには、「 * Enter * 」キーを押します。

   以前のバージョンを維持したまま SANtricity Cloud Connector バージョン 4.0 をインストールするには、アプリケーションの各バージョンに一意のポート番号を割り当てる必要があります。

   「 Choose Install Folder 」というメッセージが表示され、 SANtricity Cloud Connector のデフォルトのインストールフォルダ「 /opt/netapp/santricity_cloud_connector4/ 」が表示されます。

9. 次のいずれかのオプションを選択します。
   - デフォルトのインストール場所を使用するには、 **Enter** キーを押します。

◦ デフォルトのインストール場所を変更するには、新しいフォルダの場所を入力します。「 Enter the Non SSL Jetty Port Number 」というメッセージが表示されます。非 SSL ポートにはデフォルト値の 8080 が割り当てられています。

10. 次のいずれかのオプションを選択します。
    ◦ デフォルトの SSL ポート番号を受け入れるには、 * Next * を押します。
    ◦ デフォルトの SSL ポート番号を変更するには、新しいポート番号を入力します。
11. 次のいずれかのオプションを選択します。
    ◦ デフォルトの非 SSL ポート番号を使用する場合は、 **Enter** キーを押します。
    ◦ デフォルトの非 SSL ポート番号を変更するには、新しいポート番号の値を入力します。SANtricity Cloud Connector のインストール前の概要が表示されます。
12. 表示されたインストール前の概要を確認し、 **Enter** キーを押します。
13. Enter キーを押して Webserver Daemon Setup プロンプトを確認します。

    「 Installation Complete 」というメッセージが表示されます。

14. Enter キーを押して SANtricity Cloud Connecter インストーラを終了します。

キーストアにサーバ証明書と **CA** 証明書を追加します

ブラウザから SANtricity Cloud Connector ホストへのセキュアな https 接続を使用するには、 SANtricity Cloud Connector ホストからの自己署名証明書を受け入れるか、ブラウザと SANtricity Cloud Connector アプリケーションの両方で認識される証明書と信頼チェーンを追加します。

作業を開始する前に

SANtricity Cloud Connector アプリケーションをホストにインストールする必要があります。

手順

1. 「 systemctl 」コマンドを使用してサービスを停止します。
2. デフォルトのインストール場所から、作業ディレクトリにアクセスします。

   SANtricity Cloud Connector のデフォルトのインストール場所は、 /opt/netapp/santricity_cloud_connector4` です。

3. keytool コマンドを使用して ' サーバ証明書と証明書署名要求 (CSR) を作成します
    ◦ 例 *

```
keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
-sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
keystore_cloudconnect.jks -storepass changeit
keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
-storepass changeit -file cloudconnect.csr
```

4. 生成された CSR を任意の認証局（ CA ）に送信します。

   認証局によって署名された署名済みの証明書が返送されます。さらに、 CA 自体から証明書を受け取ります。この CA 証明書をキーストアにインポートする必要があります。

5. 証明書と CA 証明書チェーンをアプリケーションキーストアにインポートします :`/<install Path>/working/keystore`

   ◦ 例 *

```
keytool -import -alias ca-root -file root-ca.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
-keystore keystore_cloudconnect.jks -storepass <password>
```

6. サービスを再起動します。

キーストアに **StorageGRID** 証明書を追加します

SANtricity を StorageGRID Cloud Connector アプリケーションのターゲットタイプとして設定する場合は、まず SANtricity Cloud Connector キーストアに StorageGRID 証明書を追加する必要があります。

作業を開始する前に

- 署名済みの StorageGRID 証明書が必要です。
- SANtricity Cloud Connector アプリケーションをホストにインストールしておきます。

手順

1. 「 systemctl 」コマンドを使用してサービスを停止します。
2. デフォルトのインストール場所から、作業ディレクトリにアクセスします。

   SANtricity Cloud Connector のデフォルトのインストール場所は、/opt/netapp/santricity_cloud_connector4` です。

3. StorageGRID 証明書をアプリケーションキーストアにインポートします :`/<install Path>/working/keystore

   ◦ 例 *

```
opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
-trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
/home/ictlabsg01.cer -keystore
/opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
```

4. サービスを再起動します。

SANtricity Cloud Connector を初めて設定します

インストールが完了したら、設定ウィザードを使用して SANtricity Cloud Connector アプリケーションをセットアップできます。設定ウィザードは、 SANtricity Cloud Connector に最初にログインしたときに表示されます。

SANtricity Cloud Connector に初めてログインします

SANtricity Cloud Connector に初めてログインするときは、アプリケーションにアクセスするためのデフォルトのパスワードを入力する必要があります。

作業を開始する前に

インターネットに接続されたブラウザにアクセスできることを確認してください。

手順

1. サポートされているブラウザを開きます。
2. 構成済みの SANtricity Cloud Connector サーバに接続します（例：「 + http://localhost:8080/+` 」）。

   SANtricity Cloud Connector アプリケーションの初回ログインページが表示されます。
3. Administrator Password フィールドに 'password' のデフォルトのパスワードを入力します
4. * ログイン * をクリックします。

   SANtricity クラウドコネクタ構成ウィザードが表示されます。

設定ウィザードを使用する

SANtricity Cloud Connector への初回ログインが成功すると、設定ウィザードが表示されます。

設定ウィザードを使用して、管理者パスワード、 Web サービスプロキシログイン管理クレデンシャル、目的のバックアップターゲットタイプ、および SANtricity Cloud Connector の暗号化パスフレーズを設定します。

手順 1 ：管理者パスワードを設定します

管理者パスワードの設定ページを使用して、 SANtricity Cloud Connector への以降のログインに使用するパスワードをカスタマイズできます。

管理者パスワードの設定ページでパスワードを確立すると、 SANtricity Cloud Connector アプリケーションへの初回ログイン時に使用されていたデフォルトのパスワードが、実質的に置き換えられます。

手順

1. 管理者パスワードの設定ページで、 SANtricity クラウドコネクタに必要なログインパスワードを新しい管理者パスワードを入力 * フィールドに入力します。
2. 新しい管理者パスワードを再入力 * フィールドに、最初のフィールドからパスワードを再入力します。
3. 「 * 次へ * 」をクリックします。

   SANtricity Cloud Connector のパスワードセットアップが承認され、設定ウィザードの下にパスフレーズの設定ページが表示されます。

ユーザ定義の管理者パスワードは、設定ウィザードを完了するまで設定されません。

手順 **2** ：パスフレーズを設定する

[暗号化パスフレーズの入力] ページでは、 8 ～ 32 文字の英数字パスフレーズを指定できます。

ユーザ指定のパスフレーズは、 SANtricity Cloud Connector アプリケーションで使用されるデータ暗号化キーで必要です。

手順

1. [* パスフレーズを定義 *] フィールドに、必要なパスフレーズを入力します。
2. [* パスフレーズを再入力 *] フィールドに、最初のフィールドからパスフレーズを再入力します。
3. 「 * 次へ * 」をクリックします。

   入力した SANtricity Cloud Connector アプリケーションのパスフレーズが受け入れられ、設定ウィザードの [Select Target Type] ページが表示されます。

手順 **3** ：ターゲットタイプを選択します

AltaVault Cloud Connector では、バックアップ / リストア機能のターゲットタイプとして、 Amazon S3 、 StorageGRID 、 SANtricity を選択できます。ターゲットタイプの選択ページで、 SANtricity クラウドコネクタアプリケーションに必要なストレージターゲットタイプを指定できます。

作業を開始する前に

AltaVault マウントポイント、 Amazon AWS アカウント、または StorageGRID アカウントのいずれかがあることを確認します。

手順

1. ドロップダウンメニューで、次のいずれかのオプションを選択します。
   - Amazon AWS
   - AltaVault
   - StorageGRID

   選択したオプションの [ターゲットタイプ] ページが設定ウィザードに表示されます。
2. AltaVault 、 Amazon AWS 、または StorageGRID の該当する設定手順を参照してください。

AltaVault アプライアンスを設定します

[Select the Target Type] ページで AltaVault アプライアンスオプションを選択すると、 AltaVault ターゲットタイプの設定オプションが表示されます。

作業を開始する前に

- AltaVault アプライアンスの NFS マウントパスを確認しておきます。
- ターゲットタイプとして AltaVault アプライアンスを指定した。

手順

1. NFS マウントパス * フィールドに、 AltaVault ターゲットタイプのマウントポイントを入力します。

   NFS Mount Path * フィールドの値は、 Linux のパス形式に従う必要があります。

2. [このターゲットに構成データベースのバックアップを保存する *] チェックボックスをオンにして、選択したターゲットタイプの構成データベースのバックアップを作成します。

   接続のテスト時に指定したターゲットタイプで既存のデータベース設定が検出された場合は、 SANtricity Cloud Connector ホストの既存のデータベース設定情報を、設定ウィザードで入力した新しいバックアップ情報に置き換えることができます。

3. [接続のテスト *] をクリックして、指定した AltaVault 設定で接続をテストします。
4. 「 * 次へ * 」をクリックします。

   指定した SANtricity Cloud Connector のターゲットタイプが承認され、設定ウィザードに Web サービスプロキシページが表示されます。

5. 「手順 4 ： Web Services Proxy への接続」に進みます。

Amazon AWS アカウントを設定します

Select the Target Type ページで Amazon AWS オプションを選択すると、 Amazon AWS ターゲットタイプの設定オプションが表示されます。

作業を開始する前に

- Amazon AWS アカウントを確立しておきます。
- ターゲットタイプとして Amazon AWS を指定している。

手順

1. [Access Key ID*] フィールドに、 Amazon AWS ターゲットのアクセス ID を入力します。
2. [* Secret Access Key] フィールドに、ターゲットのシークレットアクセスキーを入力します。
3. [* Bucket Name*] フィールドに、ターゲットのバケット名を入力します。
4. [このターゲットに構成データベースのバックアップを保存する *] チェックボックスをオンにして、選択したターゲットタイプの構成データベースのバックアップを作成します。

   この設定を有効にして、データベースが失われた場合にバックアップターゲットからデータをリストアできるようにすることを推奨します。

   接続のテスト時に指定したターゲットタイプで既存のデータベース設定が検出された場合は、 SANtricity Cloud Connector ホストの既存のデータベース設定情報を、設定ウィザードで入力した新しいバックアップ情報に置き換えることができます。

5. [接続のテスト *] をクリックして、入力した Amazon AWS クレデンシャルを確認します。
6. 「 * 次へ * 」をクリックします。

   指定した SANtricity Cloud Connector のターゲットタイプが受け入れられ、設定ウィザードの下に Web サービスプロキシページが表示されます。

7. 「手順 4 ： Web Services Proxy への接続」に進みます。

StorageGRID アカウントを設定します

ターゲットタイプの選択ページで StorageGRID オプションを選択すると、 StorageGRID ターゲットタイプの設定オプションが表示されます。

作業を開始する前に

- StorageGRID アカウントを確立しておきます。
- SANtricity Cloud Connector キーストアに署名済みの StorageGRID 証明書を格納しておきます。
- StorageGRID をターゲットタイプとして指定しました。

手順

1. [* URL] フィールドに、 Amazon S3 クラウドサービスの URL を入力します
2. Access Key ID * フィールドに、 S3 ターゲットのアクセス ID を入力します。
3. 「 * Secret Access Key * 」フィールドに、 S3 ターゲットのシークレットアクセスキーを入力します。
4. 「 * Bucket Name * 」フィールドに、 S3 ターゲットのバケット名を入力します。
5. パス形式のアクセスを使用するには、 * パス形式のアクセスを使用 * チェックボックスを選択します。

   オフにすると、仮想ホスト形式のアクセスが使用されます。

6. [このターゲットに構成データベースのバックアップを保存する *] チェックボックスをオンにして、選択したターゲットタイプの構成データベースのバックアップを作成します。

   この設定を有効にして、データベースが失われた場合にバックアップターゲットからデータをリストアできるようにすることを推奨します。

   接続のテスト時に指定したターゲットタイプで既存のデータベース設定が検出された場合は、 SANtricity Cloud Connector ホストの既存のデータベース設定情報を、設定ウィザードで入力した新しいバックアップ情報に置き換えることができます。

7. Test Connection * をクリックして、入力した S3 クレデンシャルを確認します。

   S3 準拠のアカウントの中には、セキュアな HTTP 接続が必要なものがあります。キーストアへの StorageGRID 証明書の格納については、を参照してください "キーストアに StorageGRID 証明書を追加します"。

8. 「 * 次へ * 」をクリックします。

   指定した SANtricity Cloud Connector のターゲットタイプが承認され、設定ウィザードの下に Web サービスプロキシページが表示されます。

9. 「手順 4 ： Web Services Proxy への接続」に進みます。

手順 4 ： Web Services Proxy に接続する

SANtricity Cloud Connector と一緒に使用する Web サービスプロキシのログイン情報と接続情報は、 Web サービスプロキシの URL とクレデンシャルの入力ページで入力します。

作業を開始する前に

SANtricity Web サービスプロキシへの接続が確立されていることを確認してください。

手順

1. [* URL] フィールドに、 SANtricity クラウドコネクタで使用する Web サービスプロキシの URL を入力します。
2. 「 * User Name * 」フィールドに、 Web Services Proxy 接続のユーザ名を入力します。
3. 「 * Password * 」フィールドに、 Web Services Proxy 接続のパスワードを入力します。
4. [接続のテスト *] をクリックして、入力した Web Services Proxy クレデンシャルの接続を確認します。
5. 入力した Web Services Proxy クレデンシャルを接続テストで確認したら、
6. 「 * 次へ * 」をクリックします

   SANtricity クラウドコネクタの Web サービスプロキシのクレデンシャルが承認され、ストレージアレイの選択ページが設定ウィザードに表示されます。

手順 5 ：ストレージアレイを選択します

設定ウィザードで入力した SANtricity Web サービスプロキシのクレデンシャルに基づいて、使用可能なストレージアレイのリストがストレージアレイの選択ページに表示されます。このページから、 SANtricity Cloud Connector でのバックアップジョブとリストアジョブに使用するストレージアレイを選択できます。

作業を開始する前に

SANtricity Web サービスプロキシアプリケーションにストレージアレイが設定されていることを確認してください。

> 到達不能なストレージアレイが SANtricity Cloud Connector アプリケーションで検出された場合、ログファイルに API 例外が出力されます。これは、到達不能なアレイからボリュームリストが取得された場合の SANtricity Cloud Connector アプリケーションの想定される動作です。ログファイルにこの API 例外が出力されないようにするには、ルート問題をストレージアレイで直接解決するか、該当するストレージアレイを SANtricity Web サービスプロキシアプリケーションから削除します。

手順

1. バックアップとリストアの処理用に SANtricity Cloud Connector アプリケーションに割り当てるストレージアレイの横にある各チェックボックスを選択します。
2. 「 * 次へ * 」をクリックします。

   選択したストレージアレイが受け入れられ、ホストの選択ページが設定ウィザードに表示されます。

> ストレージアレイの選択ページで選択したストレージアレイに有効なパスワードを設定する必要があります。ストレージアレイのパスワードは、 SANtricity Web サービスプロキシ API のドキュメントを参照して設定してください。

手順 **6** ：ホストを選択する

設定ウィザードで選択した Web サービスプロキシでホストされるストレージアレイに基づいて、バックアップとリストアの候補ボリュームを SANtricity Cloud Connector アプリケーションにマッピングするホストを選択できます。ホストの選択ページを使用します。

作業を開始する前に

SANtricity Web サービスプロキシ経由でホストを使用できることを確認してください。

手順

1. 表示されたストレージアレイのドロップダウンメニューで、目的のホストを選択します。
2. ホストの選択ページに表示されたその他のストレージアレイについて、手順 1 を繰り返します。
3. 「 * 次へ * 」をクリックします。

   選択した SANtricity クラウドコネクタ用のホストが承認され、設定ウィザードに確認ページが表示されます。

手順 **7** ：初期設定を確認する

SANtricity Cloud Connector 設定ウィザードの最後のページには、入力内容の概要が確認用に表示されます。

検証済みの構成データの結果を確認します。

- すべての設定データが正常に検証され、確立されたら、 [* 終了] をクリックして設定プロセスを完了します。
- 構成データのいずれかのセクションを検証できない場合は、 ［ * 戻る ］ をクリックして、構成ウィザードの該当するページに移動し、送信されたデータを改訂します。

SANtricity Cloud Connector にログインします

SANtricity Cloud Connector アプリケーションのグラフィカルユーザインターフェイスには、設定されたサーバからサポートされているブラウザ経由でアクセスできます。SANtricity Cloud Connector アカウントが確立されていることを確認します。

手順

1. サポートされているブラウザで、構成されている SANtricity Cloud Connector サーバ（「 + http://localhost:8080/+` 」など）に接続します。

   SANtricity Cloud Connector アプリケーションのログインページが表示されます。

2. 設定した管理者パスワードを入力します。
3. [* ログイン] をクリックします。

   SANtricity Cloud Connector アプリケーションのランディングページが表示されます。

バックアップ

SANtricity Cloud Connector アプリケーションの左側のナビゲーションパネルで、バック

アップオプションにアクセスできます。Backups オプションを使用すると、 Backups ページが表示され、イメージベースまたはファイルベースのバックアップジョブを新たに作成することができます。

SANtricity Cloud Connector アプリケーションの「 * Backups * 」ページを使用して、 E シリーズボリュームのバックアップを作成、処理します。イメージベースまたはファイルベースのバックアップを作成し、それらの処理をただちにまたはあとから実行できます。また、フルバックアップを実行するか、最後に実行されたフルバックアップからの増分バックアップを実行するかを選択できます。SANtricity Cloud Connector アプリケーションで最後に実行されたフルバックアップをベースに、最大 6 つの増分バックアップを実行できます。

SANtricity Cloud Connector アプリケーションで表示されるバックアップジョブとリストアジョブのタイムスタンプは、いずれもローカル時間のタイムスタンプです。

イメージベースのバックアップの新規作成

イメージベースのバックアップを新規作成するには、 SANtricity Cloud Connector アプリケーションの Backups ページの Create 機能を使用します。

作業を開始する前に

Web Services Proxy から SANtricity Cloud Connector にストレージアレイが登録されていることを確認してください。

手順

1. バックアップページで、 * 作成 * をクリックします。

   [バックアップの作成] ウィンドウが表示されます。

2. [* イメージベースのバックアップの作成 *] を選択します。
3. 「 * 次へ * 」をクリックします。

   バックアップの作成ウィンドウに、使用可能な E シリーズボリュームのリストが表示されます。

4. 目的の E シリーズボリュームを選択し、 * Next * をクリックします。

   [概要バックアップの作成] 確認ウィンドウの [バックアップ名] ページと [バックアップの作成] ページが表示されます。

5. 自動生成されたバックアップ名を変更するには、 [* ジョブ名 *] フィールドに任意の名前を入力します。
6. 必要に応じて、 * Job 概要 * フィールドにバックアップ用の概要を追加します。

   バックアップの内容が簡単にわかるように、ジョブの概要を入力する必要があります。

7. 「 * 次へ * 」をクリックします。

   選択したイメージ・ベースのバックアップの概要が、 [バックアップ作成] ウィンドウの [バックアップ情報の確認] ページに表示されます。

8. 選択したバックアップを確認し、「 * 完了 * 」をクリックします。

バックアップの作成ウィンドウの確認ページが表示されます。

9. 次のいずれかのオプションを選択します。
   - * YES * — 選択したバックアップのフル・バックアップを開始します
   - * NO * — 選択したイメージベースのバックアップのフルバックアップは実行されません。

   > 選択したイメージベースのバックアップのフルバックアップは、バックアップページの実行機能を使用してあとから実行できます。

10. [OK] をクリックします。

    選択した E シリーズボリュームのバックアップが開始され、バックアップページの結果リストセクションにタスクのステータスが表示されます。

フォルダ / ファイルベースのバックアップの新規作成

フォルダ / ファイルベースのバックアップを新規に作成するには、 SANtricity Cloud Connector アプリケーションの Backups ページの Create 機能を使用します。

作業を開始する前に

Web Services Proxy から SANtricity Cloud Connector にストレージアレイが登録されていることを確認してください。

ファイルベースのバックアップでは、指定したファイルシステム上のすべてのファイルが無条件にバックアップされます。ただし、リストアはファイルとフォルダを選択して実行できます。

手順

1. バックアップページで、 * 作成 * をクリックします。

   [バックアップの作成] ウィンドウが表示されます。

2. [* フォルダー / ファイルベースのバックアップの作成 *] を選択します。
3. 「 * 次へ * 」をクリックします。

   バックアップに使用できるファイルシステムを含むボリュームのリストが、バックアップの作成ウィンドウに表示されます。

4. 目的のボリュームを選択し、 * 次へ * をクリックします。

   選択したボリュームで使用可能なファイル・システムのリストが ' バックアップの作成ウィンドウに表示されます

   > ファイルシステムが表示されない場合は、ファイルシステムの種類が SANtricity Cloud Connector アプリケーションでサポートされていることを確認します。詳細については、を参照してください "サポートされているファイルシステム"。

5. バックアップするフォルダまたはファイルが格納されているファイル・システムを選択し ' 次へをクリックします

[概要バックアップの作成] 確認ウィンドウの [バックアップ名] ページと [バックアップの作成] ページが表示されます。

6. 自動生成されたバックアップ名を変更するには、 [* ジョブ名 *] フィールドに任意の名前を入力します。
7. 必要に応じて、 * Job 概要 * フィールドにバックアップ用の概要を追加します。

   バックアップの内容が簡単にわかるように、ジョブの概要を入力する必要があります。

8. 「 * 次へ * 」をクリックします。

   選択したフォルダ / ファイルベースのバックアップの概要が、バックアップ作成ウィンドウの * バックアップ情報の確認 * ページの下に表示されます。

9. 選択したフォルダ / ファイルベースのバックアップを確認し、 [完了] をクリックします。

   バックアップの作成ウィンドウの確認ページが表示されます。

10. 次のいずれかのオプションを選択します。
    - * YES * — 選択したバックアップのフル・バックアップを開始します
    - * NO * — 選択したバックアップのフルバックアップは実行されません。

      選択したファイルベースのバックアップのフルバックアップは、後で Backups ページの Run 機能を使用して実行することもできます。

11. [* 閉じる *] をクリックします。

    選択した E シリーズボリュームのバックアップが開始され、バックアップページの結果リストセクションにタスクのステータスが表示されます。

フル・バックアップと増分バックアップを実行します

バックアップページの実行機能を使用して、フルバックアップと増分バックアップを実行できます。増分バックアップは、ファイルベースのバックアップでのみ使用できます。

作業を開始する前に

SANtricity Cloud Connector でバックアップジョブを作成しておきます。

手順

1. [バックアップ] タブで、目的のバックアップ・ジョブを選択し、 [* 実行] をクリックします。

   イメージベースのバックアップジョブまたは以前に実行された初期バックアップを含まないバックアップジョブを選択すると、自動的にフルバックアップが実行されます。

   バックアップの実行ウィンドウが表示されます。

2. 次のいずれかのオプションを選択します。
   - * フル * — 選択したファイルベースのバックアップのすべてのデータをバックアップします

◦ * Incremental * ：最後に実行されたバックアップ以降に行われた変更のみをバックアップします

SANtricity Cloud Connector アプリケーションで最後に実行されたフルバックアップをベースに、最大 6 つの増分バックアップを実行できます。

3. [ファイル名を指定して実行] をクリック

   バックアップが開始されます。

バックアップジョブを削除

削除機能を使用すると、選択したバックアップの指定したターゲット・ロケーションにあるバックアップ・データとバックアップ・セットが削除されます。

作業を開始する前に

バックアップのステータスが ［ 完了 ］ 、 ［ 失敗 ］ 、または ［ キャンセル済み ］ であることを確認します。

手順

1. [バックアップ] ページで、目的のバックアップを選択し、 [削除] をクリックします。

   フルベースバックアップを選択した場合は、関連する増分バックアップもすべて削除されます。

   削除の確認ウィンドウが表示されます。

2. 「 * タイプ DELETE * 」フィールドに「削除」と入力して、削除操作を確認します。
3. [削除（ Delete ）] をクリックします。

   選択したバックアップが削除されます。

リストアします

SANtricity Cloud Connector アプリケーションの左側のナビゲーションパネルで、リストアオプションにアクセスできます。Restore （復元）オプションを選択すると、 Restore （復元）ページが表示されます。このページでは、イメージベースまたはファイルベースの復元ジョブを新規作成できます。

SANtricity Cloud Connector では、「ジョブ」を使用して E シリーズボリュームのリストアを実行します。リストアを実行する前に、処理に使用する E シリーズボリュームを特定する必要があります。SANtricity Cloud Connector ホストにリストア用の E シリーズボリュームを追加すると、 SANtricity Cloud Connector アプリケーションの「リストア」ページを使用してリストアの作成と処理を行うことができます。

SANtricity Cloud Connector アプリケーションで表示されるバックアップジョブとリストアジョブのタイムスタンプは、いずれもローカル時間のタイムスタンプです。

イメージベースのリストアの新規作成

SANtricity Cloud Connector アプリケーションのリストアページの作成機能を使用して、イメージベースのリストアを新規作成できます。

作業を開始する前に

SANtricity Cloud Connector で使用可能なイメージベースのバックアップがあることを確認してください。

手順

1. SANtricity Cloud Connector アプリケーションの [リストア] ページで、 [* 作成] をクリックします。

   [復元] ウィンドウが表示されます。

2. 目的のバックアップを選択します。
3. 「 * 次へ * 」をクリックします。

   [リストア] ウィンドウに [バックアップ・ポイントの選択] ページが表示されます。

4. 目的の完了済みバックアップを選択します。
5. 「 * 次へ * 」をクリックします。

   [リストア先の選択] ページが [リストア] ウィンドウに表示されます。

6. 復元ボリュームを選択し、 * Next * （次へ）をクリックします。

   [リストア] ウィンドウに [レビュー] ページが表示されます。

7. 選択したリストア処理を確認し、「 * 完了 * 」をクリックします。

   選択したターゲットホストボリュームのリストアが開始され、リストアページの結果リストセクションにタスクのステータスが表示されます。

ファイルベースのリストアの新規作成

SANtricity Cloud Connector アプリケーションのリストアページの作成機能を使用すると、ファイルベースのリストアを新規作成できます。

作業を開始する前に

SANtricity Cloud Connector で使用可能なファイルベースのバックアップがあることを確認します。

手順

1. SANtricity Cloud Connector アプリケーションの [リストア] ページで、 [* 作成] をクリックします。

   [復元] ウィンドウが表示されます。

2. [復元] ウィンドウで、目的のファイルベースのバックアップを選択します。
3. 「 * 次へ * 」をクリックします。

   [リストア・ジョブの作成] ウィンドウに [バックアップ・ポイントの選択] ページが表示されます。

4. [バックアップ・ポイントの選択] ページで、目的の完了済みバックアップを選択します。
5. 「 * 次へ * 」をクリックします。

   使用可能なファイル・システムまたはフォルダ / ファイル・ページのリストがリストア・ウィンドウに表示されます

6. 復元するフォルダまたはファイルを選択し、 * 次へ * をクリックします。

   [リストア先の選択] ページが [リストア] ウィンドウに表示されます。

7. 復元ボリュームを選択し、 * Next * （次へ）をクリックします。

   [リストア] ウィンドウに [レビュー] ページが表示されます。

8. 選択したリストア処理を確認し、「 * 完了 * 」をクリックします。

   選択したターゲットホストボリュームのリストアが開始され、リストアページの結果リストセクションにタスクのステータスが表示されます。

リストアを削除する

削除機能を使用すると、選択したリストア・アイテムをリストア・ページの結果リスト・セクションから削除できます。

作業を開始する前に

ステータスが「 Completed 」、「 Failed 」、または「 Cancelled 」のリストアジョブがあることを確認します。

手順

1. [復元] ページで、 [削除 *] をクリックします。

   削除の確認ウィンドウが表示されます。

2. 「 *Type delete 」フィールドに「削除」と入力して、削除アクションを確認します。
3. [削除（ Delete ）] をクリックします。

   中断されているリストアは削除できません。

   選択したリストアが削除されます。

SANtricity クラウドコネクタの設定を変更します

Settings オプションでは、 S3 アカウント、管理対象のストレージアレイとホスト、および Web Services Proxy クレデンシャルのアプリケーションの現在の設定を変更できます。SANtricity Cloud Connector アプリケーションのパスワードは、設定オプションを使用して変更することもできます。

S3 アカウントの設定を変更します

SANtricity Cloud Connector アプリケーションの既存の S3 設定は、 S3 Account Settings ウィンドウで変更できます。

作業を開始する前に

URL または S3 バケットラベルの設定を変更すると、 SANtricity Cloud Connector で設定された既存のバックアップへのアクセスに影響する点に注意してください。

手順

1. 左側のツールバーで、 * Settings > Configuration * をクリックします。

   設定 - 設定ページが表示されます。

2. S3 アカウント設定の「 * 表示 / 設定の編集」をクリックします。

   S3 Account Settings ページが表示されます。

3. URL ファイルに、 S3 クラウドサービスの URL を入力します。
4. Access Key ID * フィールドに、 S3 ターゲットのアクセス ID を入力します。
5. 「 * Secret Access Key * 」フィールドに、 S3 ターゲットのアクセスキーを入力します。
6. S3 Bucket Name * フィールドに、 S3 ターゲットのバケット名を入力します。
7. 必要に応じて、 [パススタイルアクセスを使用（ * Use Path Style Access * ）] チェックボックスを選択します。
8. Test Connection * をクリックして、入力した S3 クレデンシャルの接続を確認します。
9. [保存（ Save ）] をクリックして、修正を適用する。

   変更した S3 アカウント設定が適用されます。

ストレージアレイを管理します

ストレージアレイの管理ページで、 SANtricity Cloud Connector ホストに登録された Web サービスプロキシからストレージアレイを追加または削除できます。

ストレージアレイの管理ページに、 SANtricity Cloud Connector ホストへの登録に使用できる Web サービスプロキシのストレージアレイのリストが表示されます。

手順

1. 左側のツールバーで、 * Settings > Storage Arrays * をクリックします。

   Settings - Storage Arrays （設定 - ストレージアレイ）画面が表示されます。

2. SANtricity Cloud Connector にストレージアレイを追加するには、 * Add * をクリックします。
   a. Add Storage Arrays （ストレージアレイの追加）ウィンドウで、結果リストから目的のストレージアレイの横にある各チェックボックスをオンにします。
   b. [追加（ Add ）] をクリックします。

選択したストレージアレイが SANtricity クラウドコネクタに追加され、 [Settings] - [Storage Arrays] 画面の [Result] リストセクションに表示されます。

3. 追加したストレージアレイのホストを変更するには、 Settings - Storage Arrays （設定 - ストレージアレイ）画面の結果リストセクションにある行アイテムの * Edit * （編集）をクリックします。
   a. 関連付けられているホストドロップダウンメニューで、ストレージアレイのホストを選択します。
   b. [保存（ Save ）] をクリックします。

      選択したホストがストレージアレイに割り当てられます。

4. SANtricity Cloud Connector ホストから既存のストレージアレイを削除するには、下部の結果リストから目的のストレージアレイを選択し、 * Remove * をクリックします。
   a. [ストレージアレイの削除の確認] フィールドに「 re move 」と入力します。
   b. [削除（ Remove ）] をクリックします。

      選択したストレージアレイが SANtricity Cloud Connector ホストから削除されます。

Web Services Proxy の設定を変更

SANtricity Cloud Connector アプリケーションの既存の Web サービスプロキシ設定は、 Web Services Proxy Settings ウィンドウで変更できます。

作業を開始する前に

SANtricity Cloud Connector で使用する Web サービスプロキシに適切なアレイが追加されていて、対応するパスワードが設定されている必要があります。

手順

1. 左側のツールバーで、 * MENU ： Settings （設定） [Configuration]* をクリックします。

   Settings - Configuration （設定 - 設定）画面が表示されます。

2. Web Services Proxy の [設定の表示 / 編集] をクリックします。

   Web Services Proxy の設定画面が表示されます。

3. [URL] フィールドに、 SANtricity Cloud Connector で使用する Web サービスプロキシの URL を入力します。
4. User Name フィールドに、 Web Services Proxy 接続のユーザ名を入力します。
5. Password フィールドに、 Web Services Proxy 接続のパスワードを入力します。
6. [接続のテスト *] をクリックして、入力した Web Services Proxy クレデンシャルの接続を確認します。
7. [保存（ Save ）] をクリックして、修正を適用する。

SANtricity Cloud Connector のパスワードを変更します

SANtricity Cloud Connector アプリケーションのパスワードは、パスワードの変更画面で変更できます。

手順

1. 左側のツールバーで、 * MENU ： Settings （設定） [Configuration]* をクリックします。

   Settings - Configuration （設定 - 設定）画面が表示されます。

2. SANtricity Cloud Connector のパスワードの変更 * をクリックします。

   Change Password （パスワードの変更）画面が表示されます。

3. Current password フィールドに、 SANtricity Cloud Connector アプリケーションの現在のパスワードを入力します。
4. [新しいパスワード] フィールドに、 SANtricity Cloud Connector アプリケーションの新しいパスワードを入力します。
5. [新しいパスワードの確認入力] フィールドに新しいパスワードを再入力します。
6. 新しいパスワードを適用するには、 [*Change] をクリックします。

   変更したパスワードが SANtricity Cloud Connector アプリケーションに適用されます。

SANtricity Cloud Connector をアンインストールします

SANtricity Cloud Connector は、グラフィカルなアンインストーラまたはコンソールモードを使用してアンインストールできます。

グラフィカルモードを使用してアンインストールします

Linux オペレーティングシステムでグラフィカルモードを使用して SANtricity Cloud Connector をアンインストールできます。

手順

1. ターミナルウィンドウで、 SANtricity Cloud Connector アンインストールファイルが格納されているディレクトリに移動します。

   SANtricity Cloud Connector のアンインストールファイルのデフォルトのディレクトリは次のとおりです。

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. SANtricity Cloud Connector アンインストールファイルが格納されているディレクトリから、次のコマンドを実行します。

   ```
   ./uninstall_cloud_connector4 -i gui
   ```

   SANtricity Cloud Connector のアンインストールプロセスが開始されます。

3. アンインストールウィンドウで、 **Uninstall** をクリックして、 SANtricity Cloud Connector のアンインストールを続行します。

アンインストールプロセスが完了し、 SANtricity Cloud Connector アプリケーションが Linux オペレーティングシステムからアンインストールされます。

コンソールモードを使用してをアンインストールします

Linux オペレーティングシステムでコンソールモードを使用して SANtricity Cloud Connector をアンインストールできます。

手順

1. ターミナルウィンドウで、 SANtricity Cloud Connector アンインストールファイルが格納されているディレクトリに移動します。

   SANtricity Cloud Connector のアンインストールファイルのデフォルトのディレクトリは次のとおりです。

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. SANtricity Cloud Connector アンインストールファイルが格納されているディレクトリから、次のコマンドを実行します。

   ```
   ./uninstall_cloud_connector4 -i console
   ```

   SANtricity Cloud Connector のアンインストールプロセスが開始されます。

3. アンインストールウィンドウで *Enter * を押して、 SANtricity Cloud Connector のアンインストールに進みます。

   アンインストールプロセスが完了し、 SANtricity Cloud Connector アプリケーションが Linux オペレーティングシステムからアンインストールされます。

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。