テクニカル レポート

セキュリティ強化ガイド：
BlueXP Cloud Backup for Applications

NetApp
ONTAP TME Team
2023年7月| TR-4963

概要

このガイドは、Cloud Backup for Applications解決策のお客様を対象としており、解決策の機密性、整合性、可用性に影響を及ぼす可能性のある不正使用からCloud Backup for Applicationsを保護するためのNetApp推奨のベストプラクティスについて詳しく説明しています。

目次

表一覧

図一覧

アプリケーション向けのCloud Backupを強化

はじめに

これらのガイドラインとツールは、安全に操作を実行し、ハッキングを防止するために提供されています。これには、脆弱性の排除または軽減が含まれます。脆弱性という用語は、システムの実装、構成、設計、または管理に発生する可能性のあるソフトウェアの欠陥と弱点を指します。強化技術には、通常、構成をロックダウンし、運用機能とセキュリティのバランスを取ることが含まれます。このガイドでは、NetApp® 解決策に不可欠な機密性、整合性、可用性について、オペレータと管理者を支援することを目的としています。

インストール済みコンポーネントの整合性検証

Cloud Backup for Applicationsは、NetAppクラウドストレージとオンプレミスのNetApp ONTAPストレージで実行されるアプリケーションにデータ保護機能を提供するSaaS（ソフトウェアサービス）ベースのサービスです。NetApp BlueXP（旧称Cloud Manager）で有効なアプリケーション向けCloud Backupは、アプリケーションと整合性のある効率的なポリシーベースの保護を提供します。

Cloud Backup Applications SaaS、UI、プラグインの各コンポーネントの整合性は、検証ツールを使用して検証されます。

Cloud Backup Applications SaaS-DockerイメージとHelmチャートの署名と検証

Cosignツールは、DockerイメージとHelmチャートに署名するために使用されます。署名と検証の手順は次のとおりです。

1. ビルド時にCloud Backup for Applicationsによって生成されるDockerイメージチャートとHelmチャートには、Remote Support Agent（RSA）キーペアを使用して署名が添付されます。
2. イメージ/グラフは、Cloud Backup for Applications SaaSクラスタにインストールする前に検証されます。

Cloud Backup ApplicationsのUIとプラグイン-バイナリの署名とチェックサム検証

バイナリ署名と検証メカニズムに関する詳細は以下のとおりです。

1. Linuxプラグインバイナリは、ビルド時にRSAキーペアを使用して署名されます。
2. プラグインバイナリは、前述のように署名されたHelmチャートとしてバンドルされています。
3. バイナリ署名は、BlueXPコネクタで実行されているエージェントによってプラグインバイナリがプルされる前に検証されます。
4. プラグインバイナリのチェックサムはビルド時に生成されます。プラグインバイナリをプルする前に、BlueXPコネクタを実行しているエージェントによってもチェックサムが検証されます。
5. UIバンドルもRSAキーペアを使用して署名され、ビルド時にバンドルのチェックサムも生成されます。
6. UIバンドルは、Cloud Backup for Applicationsのビルド更新プロセスで更新されるときに署名とチェックサムが検証されます。

クラウドネイティブアプリケーションの保護

ネットワークセキュリティ

このセクションの目的は、さまざまな潜在的な脅威に対するネットワークセキュリティの適切なガイドラインを提供することです。

コネクタネットワークの要件

BlueXP Connectorのインバウンド/アウトバウンドの一般的な要件は、NetAppのドキュメントに記載されています。このセクションでは、Cloud Backup for Applicationsのその他の要件について説明します。

インバウンド

Cloud Backup for Applicationsに追加のインバウンドルールは必要ありません。

アウトバウンド

クラウドネイティブのアプリケーション保護を実現するには、Amazon Web Services（AWS）環境またはAzure環境に配置されているアプリケーションホストにBlueXPコネクタを接続できる必要があります。また、必要に応じてAmazon FSx for NetApp ONTAPストレージ管理IP、およびAWS / Azure上のNetApp Cloud Volumes ONTAPに接続できる必要があります。次の表に、これらのポート要件を示します（表1）。

表1）ポートの要件

サポート	デスティネーション	アプリケーション	クラウドプラットフォーム	ポート	コメント
BlueXPコネクタ	AWS EC2 Oracleデータベース（DB）ホスト	Oracle	AWS	Secure Shell（SSH）ポート（デフォルト：**22**）	以下で説明するSSHベースの導入にのみ必要
BlueXPコネクタ	AWS EC2 Oracle DBホスト	Oracle	AWS	プラグインポート（デフォルト：**8145**）	
BlueXPコネクタ	AWS FSx	Oracle	AWS	管理API（デフォルト：**443**）	REST APIを呼び出すには、コネクタからFSx管理へのアウトバウンド接続が必要
BlueXPコネクタ	Cloud Volumes ONTAP	Oracle	AWS、Azure	管理API（デフォルト：**443**）	
BlueXPコネクタ	Azure Compute SAP HANAシステムホスト	SAP HANA	Azure	プラグインポート（デフォルト：**8145**）	

上記の場合は、それぞれ次のようになります。

1. ソースとデスティネーションが別の仮想ポートチャネル（vPC）またはAzure Virtual Network（VNet）にある場合は、vPC / VNetピアリングなどを介してそれらの間に接続が確立されていることを確認します。
2. それぞれのクラウドプラットフォームのネットワークセキュリティグループで、BlueXPコネクタからアプリケーションホストのポートへのアウトバウンド接続が許可されていることを確認してください。
3. ホスト側のファイアウォールが同じ通信を許可するように設定されていることを確認します。

TLSセキュリティと証明書の管理

BlueXPコネクタとLinuxプラグインホストの間の通信には、自己署名証明書が使用されます。ここでは、自己署名証明書を認証局（CA）署名証明書に置き換える方法について説明します。これにより、これらのコンポーネント間のHTTPSトラフィック中に関連する証明書の検証の信頼性とセキュリティが向上します。

クラウドネイティブの保護のために、Linuxホスト上でSnapCenter Plug-in Loaderサービス（SPL）を使用してCA証明書を設定する

認証局（CA）は、Secure Sockets Layer（SSL）証明書を発行する信頼されたエンティティです。これらのデジタル証明書は、暗号化によってエンティティを公開鍵とリンクするために使用されるデータファイルです。NetApp SnapCenter® では、許可されたCA証明書を使用したサーバとプラグインの相互通信がサポートされるようになりました。すべてのHTTPS呼び出しは、セキュアなSSL標準に基づいて検証されます。

SPLは、`'keystore.jks'/var/opt/snapcenter/spl/etc` AWS / Azureで実行されているプラグインホストの信頼ストアとキーストアの両方としてにあるファイルを使用します。

SPLキーストアのパスワードと、使用中のCA署名キーペアのエイリアスを管理します。

手順

1. SPLを実行しているLinuxホストにログインします。
2. SPLキーストアのデフォルトパスワードは`spl.properties`、にあるSPLプロパティファイル""から取得できます `/var/opt/snapcenter/spl/etc`。

   これは、キー「SPL_KEYSTORE_PASS」に対応する値です。
3. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

4. キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   `spl.properties` ファイルのSPL_KEYSTORE_PASSキーについても同じ内容を更新します。
5. パスワードを変更したら、SPLサービスを再起動します。

```
systemctl restart spl
```

   注： SPLキーストアのパスワードと、秘密鍵に関連付けられているすべてのエイリアスパスワードは同じである必要があります。

SPLトラストストアに対するCA署名付きキー ペアの設定

SPLトラストストアに対してCA署名付きキー ペアを設定する必要があります。

手順

1. SPLを実行しているLinuxホストにログインします。
2. SPLのキーストアが格納されているフォルダに移動し `/var/opt/snapcenter/spl/etc`ます。
3. ファイル'`keystore.jks`'を見つけます。
4. キーストアに追加された証明書を一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

5. 秘密鍵と公開鍵の両方を持つCA証明書を追加します。

```
keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore
keystore.jks -deststoretype JKS
```

6. キーストアに追加された証明書を一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

7. キーストアに、キーストアに追加された新しいCA証明書に対応するエイリアスが含まれていることを確認します。
8. CA証明書に追加した秘密鍵のパスワードをキーストアのパスワードに変更します。デフォルトのSPLキーストアパスワードは `spl.properties`、ファイルのSPL_KEYSTORE_PASSキーの値です。

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks
```

9. CA証明書のエイリアス名が長く、スペースまたは特殊文字（"*"、"、"）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore
keystore.jks
```

10. `spl.properties` ファイルにあるキーストアからエイリアス名を設定します。

    SPL_CERTIFICATE_ALIASキーに対するこの値を更新します。
11. SPL信頼ストアにCA署名キーペアを設定したら、SPLサービスを再起動します。

```
Systemctl restart spl
```

BlueXP ConnectorでのSPL CA証明書の設定

SPL用に生成されたCA証明書は、BlueXPコネクタ内で実行されるcloudmanager_scs_cloud Dockerコンテナに設定する必要があります。

手順：

1. BlueXP Connectorホストにroot以外のユーザとしてログインします。
2. 次のコマンドを実行すると `<base_mount_path>`、cloudmanager_scs_cloud Dockerコンテナのを取得できます。

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

3. サーバフォルダが存在しない場合は作成します。

```
sudo mkdir <base_mount_path>/server
sudo chmod 755 <base_mount_path>/server
```

4. CA証明書のチェーン全体を、にある永続ボリュームにコピーします `<base_mount_path>/server`。
5. `cloudmanager_scs_cloud` コンテナに接続し、`enableCACert` のを `config.yml` trueに変更します。

```
sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert: false/enableCACert: true/g'
/opt/netapp/cloudmanager-scs-cloud/config/config.yml
```

6. `cloudmanager_scs_cloud` コンテナを再起動します。

```
sudo docker restart cloudmanager_scs_cloud
```

BlueXP ConnectorでCA証明書を設定してクラウドネイティブの保護を実現

BlueXP Connectorは、自己署名証明書を使用してプラグインと通信します。インストールスクリプトによって、自己署名証明書がSPLキーストアにインポートされます。次の手順を実行して、自己署名証明書をCA署名証明書に置き換えることができます。

手順：

1. BlueXP Connectorホストにroot以外のユーザとしてログインします。
2. 次のコマンドを実行すると <base_mount_path>、cloudmanager_scs_cloud Dockerコンテナのを取得できます。

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

3. <base_mount_path>/client/certificate BlueXP Connectorホストにある既存のファイルをすべて削除します。
4. CA署名証明書とキーファイルを <base_mount_path>/client/certificate BlueXPコネクタホストのにコピーします。

   ファイル名は certificate.pem とである必要があります key.pem。には certificate.pem、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。
5. 証明書のPKCS12形式をcertificate.p12という名前で作成し、のままにします <base_mount_path>/client/certificate。

BlueXP ConnectorのCA証明書をSPLキーストアにインポートする

手順：

1. BlueXP Connectorホストにroot以外のユーザとしてログインします。
2. に保持されているすべての中間CAとルートCAの証明書.p12と証明書を <base_mount_path>/client/certificate、SPLを実行するLinuxプラグインホストにコピーします /var/opt/snapcenter/spl/etc/。プラグインホストにログインします。
3. SPLを実行しているLinuxホストにログインします。
4. /var/opt/snapcenter/spl/etcに移動し、keytoolコマンドを実行して証明書.p12ファイルをインポートします。

```
keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter -deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt
```

5. ルートCA証明書と中間証明書をインポートします。

```
keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter -alias trustedca -file <certificate.crt>
```

   注： certfilecertificate.crt ファイルには、ルートCAと中間CAの証明書が含まれています。

6. SPLサービスを再起動します。

```
systemctl restart spl
```

SPLテサホオトサレルアンコウ

SPLでは、AES128およびAES256暗号がサポートされるのは、サーバとLinuxクライアントの間の通信のみです。

```
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
AES256-GCM-SHA384
AES256-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
AES128-GCM-SHA256
AES128-SHA256
```

双方向SSL

BlueXP ConnectorとLinuxプラグインの通信（SPLを使用）の間の双方向SSLはデフォルトで有効になっており、相互のSSL検証を成功させるためには上記の手順を実行する必要があります。

双方向SSLでは、クライアントとサーバの両方が相互に認証して、通信に関与する両方の当事者が信頼されていることを確認します。

SPLの場合、これらのパラメータは `spl.properties` にあるファイルで指定できます `/var/opt/snapcenter/spl/etc/spl.properties`。上記の値はデフォルトでtrueに設定されています。つまり、双方向の相互SSL検証は、通信を強化するためにデフォルトで有効になっています。

```
ENABLE_CERTIFICATE_VALIDATION=true
ENABLE_CLIENT_CERTIFICATE_AUTHENTICATION=true
```

アプリケーションプラグインの導入と構成

ネットワークセキュリティ

インバウンド

アプリケーションホストは、Cloud Backup Applicationsの処理で以下のポートを許可する必要があります（表2）。

表2）Cloud Backup Applications処理用のポート

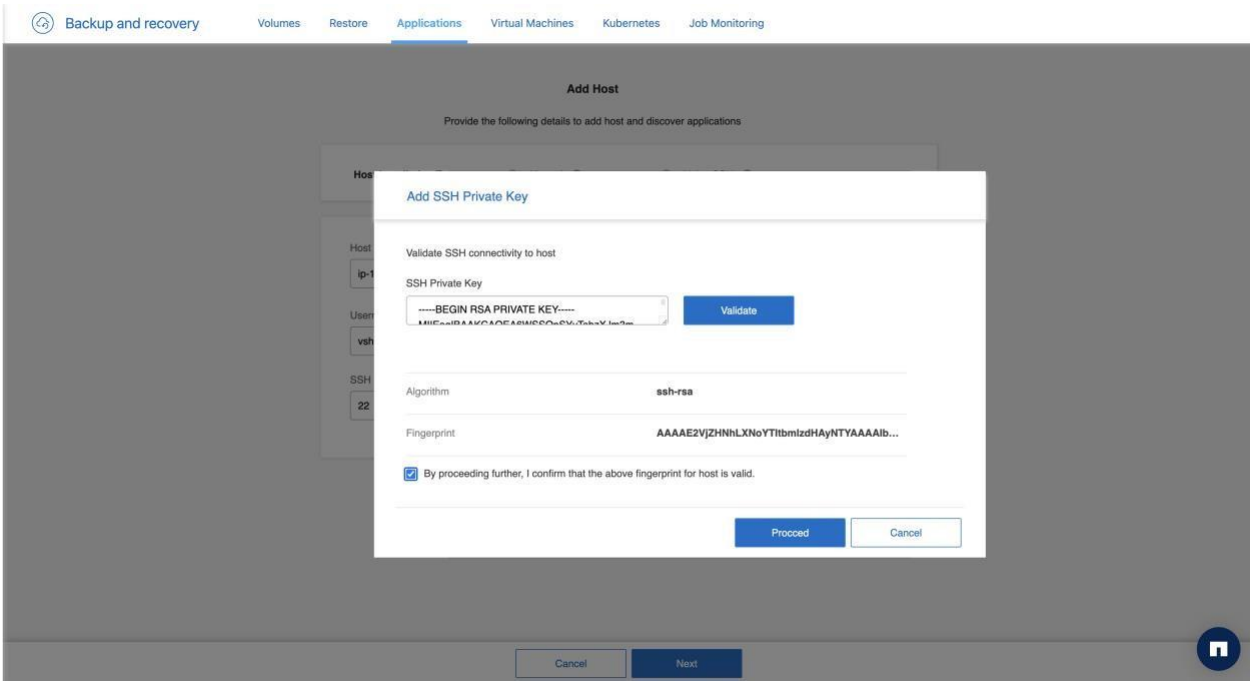
アプリケーション	クラウドプラットフォーム	ポート	目的
Oracle	AWS	SSHポート（デフォルト：22）	現在Oracleでサポートされているアプリケーションプラグインの SSHベースの導入にのみ必要
Oracle	AWS	プラグインポート（デフォルト：8145）	通常運用時に必要
SAP HANA	Azure	プラグインポート（デフォルト：8145）	通常運用時に必要

アウトバウンド

Cloud Backup for Applicationsの処理を実行するプラグインホストにはアウトバウンド要件がありません。

Oracleプラグインのプッシュインストール導入時のフィンガープリント検証

- Cloud Backup Applications UIからSSHを使用してプラグインをプッシュインストールすることは、AWS FSx上のOracleアプリケーションでサポートされています。
- インストール処理の一環として、パッケージをホストにプッシュする前に、フィンガープリントを検証し、ホストに対して目視で確認する必要があります。フィンガープリントが有効であることを確認するには、UIでチェックボックスを有効にする必要があります。以下のスクリーンショットを参照してください。



Oracleデータベース認証

DB認証

Oracleデータベース認証方式は、Oracleデータベースに照らして認証します。データベースホストでオペレーティングシステム（OS）認証が無効になっている場合は、Oracleデータベースで処理を実行するためにOracleデータベース認証が必要になります。そのため、Oracleデータベースのクレデンシャルを追加する前に、Oracleデータベースでsysdba権限を持つOracleユーザを作成しておく必要があります。

ASM認証

Oracle ASM認証方式は、Oracle Automatic Storage Management（ASM）インスタンスに照らして認証します。Oracle ASMインスタンスにアクセスする必要があり、データベースホストでOS認証が無効になっている場合は、Oracle ASM認証が必要です。そのため、Oracle ASMのクレデンシャルを追加する前に、ASMインスタンスでSYSASM権限を持つOracleユーザを作成しておく必要があります。

オペレーティングシステムの

ポートセキュリティの保護

使用していないネットワークポートは開いたままにしないでください。特に、Telnet接続用のポート23などの脆弱なポートは、すべてのシステムで閉じる必要があります。Linuxシステムに必要な以下のポートを開く必要があります。

- デフォルトでは、spl_portは8145に設定されています。ただし、これらのポート値は、ファイルで定義されている設定可能なパラメータを使用して設定できます `/var/opt/snapcenter/spl/etc/spl.properties`。
- コネクタでプッシュインストールまたはヘルパースクリプトを使用してプラグインをインストールするには、ポート22（SSH）が必要です。ただし、ここに記載されている手動の手順に従ってプラグインを手動で導入する場合は、ファイアウォールリストのポート22をスキップできます。
- ポート27216を有効にします。デフォルトのJDBCポートは、Oracleデータベースへの接続にOracle用プラグインで使用されます。

リスニングポートのリストを確認するには、次のコマンドを使用します。

```
netstat -tulpn
```

この情報を使用して、必要なリスニングポートと無効にするポートを特定できます。

開いておく残りのポートを保護するには、ポートへのアクセスを特定のホストIPアドレスに制限します。Linuxディストリビューション、バージョン、ファイアウォール、iptablesなどに応じて、共通のホスト側ファイアウォールがLinuxホストにインストールされます。上記の必要に応じて、ホスト側のファイアウォールでSSHポートとプラグインポートが有効になっている必要があります。

SELinux

Security-Enhanced Linux（SELinux）は、アクセス制御セキュリティポリシーをサポートするカーネルセキュリティメカニズムです。

次のコマンドを実行して、現在のSELinuxモードを確認できます。

```
sestatus
```

SnapCenter for Oracleプラグインが操作を実行できるようにするには、SELinuxをPermissiveに設定する必要があります。そうしないと、インストールに失敗する可能性があります。

ワークフロー実行

Oracleでのプリスクリプトとポストスクリプト

スクリプトは `/var/opt/snapcenter/spl/scripts/` ディレクトリに配置する必要があります。このディレクトリには、rootユーザのみがアクセスできます。

SAP HANA

ポリシーの作成時に、プリスクリプト、ポストスクリプト、および終了スクリプトを指定できます。これらのスクリプトは、バックアップの作成時にHANAホストで実行されます。

サポートされているスクリプトの形式は、.sh、Pythonスクリプト、perlスクリプトなどです。

プリスクリプトとポストスクリプトは、ホスト管理者によって次の `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` ファイルに登録されている必要があります。

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

ハイブリッドアプリケーションの保護

ネットワークセキュリティ

オンプレミスのアプリケーションをクラウドに保護するには、BlueXPコネクタがSnapCenterサーバと通信できる必要があります。BlueXP Connectorは、オンプレミス（推奨）とクラウド（表3）のどちらにも導入できます。

表3）ハイブリッドアプリケーション用のポート

ソース	クラウド プラットフォーム	デスティネーションポート	コメント
BlueXPコネクタ	オンプレミス、AWS、Azure、Google Cloud	SnapCenterサーバポート（デフォルト：8146）	コネクタは、導入されている場所にかかわらず、オブジェクトストアにバックアップを移動する必要があるSnapCenterサーバにアクセスできる必要があります。

ネットワークインフラでBlueXP Connectorを有効にして、SnapCenterサーバにアクセスできることを確認します。

TLSセキュリティと証明書の管理

BlueXPコネクタとLinuxプラグインホストの間の通信には、自己署名証明書が使用されます。ここでは、自己署名証明書をCA署名証明書に置き換える方法について説明します。これにより、これらのコンポーネント間のHTTPSトラフィック中に関連する証明書の検証の信頼性とセキュリティが向上します。

ハイブリッド保護のためにSnapCenterサーバでCA証明書を設定する

アプリケーション向けクラウドバックアップオンプレミスアプリケーションをクラウドに保護するには、オンプレミスで実行されているSnapCenterサーバに接続する必要があります。SnapCenterサーバでCA証明書を設定するには、次の手順を実行します。

手順

1. SnapCenterがインストールされているWindows ServerでIISマネージャを開きます。
2. 左側のナビゲーション ペインで、[Connections]をクリックします。
3. サーバ名と[Sites]を展開します。
4. SSL証明書をインストールするSnapCenterのWebサイトを選択します。
5. [アクション]>[サイトの編集]に移動し、[バインド]をクリックします。
6. [Bindings]ページで、[binding for https]を選択します。
7. [編集]をクリックします。
8. [SSL certificate]ドロップダウン リストから、最近インポートしたSSL証明書を選択します。

9. [OK]をクリックします。

注： 最近導入したCA証明書がドロップダウンメニューに表示されない場合は、CA証明書が秘密鍵に関連付けられているかどうかを確認します。

注： 証明書が次のパスを使用して追加されていることを確認します。[コンソールルート]>[証明書-ローカルコンピュータ]>[信頼されたルート証明機関]>[証明書]。

SnapCenterサーバでCA証明書を有効にする

CA証明書を設定し、SnapCenter ServerのCA証明書の検証を有効にする必要があります。

CA証明書を有効または無効にするには、`Set-SmCertificateSettings` コマンドレットを使用します。

SnapCenter Serverの証明書のステータスを表示するには、Get-SmCertificateSettingsコマンドレットを使用します。

コマンドレットで使用できるパラメータとその説明は、を実行して確認できます `Get-Help command_name`。または、SnapCenterソフトウェアコマンドレットリファレンスガイドを参照してください。

手順

1. [Settings]ページで、[Settings] > [Global Settings] > [CA Certificate Settings]に移動します。
2. [Enable Certificate Validation]を選択します。
3. [適用]をクリックします。

終了後の操作

[管理対象ホスト]タブには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

プラグインホストに有効なCA証明書または割り当てられていないことを示します。

CA証明書が正常に検証されたことを示します。

CA証明書を検証できなかったことを示します。

接続情報を取得できなかったことを示します。

注： ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

BlueXP ConnectorでSnapCenterサーバCA証明書を設定してハイブリッド保護を実現

サーバのCA署名証明書をコネクタがSnapCenterの証明書を検証できるように、BlueXP ConnectorでSnapCenterサーバのCA署名証明書を設定する必要があります（コネクタについて説明します）。

手順：

1. BlueXP Connectorホストにroot以外のユーザとしてログインします。
2. BlueXPコネクタで次のコマンドを実行して、を取得する必要があります`<base_mount_path>`。

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

3. コネクタの証明書フォルダに移動します。

```
cd <base_mount_path>; mkdir -p server/certificate
```

4. ルートCAファイルと中間CAファイルを `<base_mount_path>/server/certificate` ディレクトリにコピーします。 CAファイルは.pem形式である必要があります。
5. 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. CRLファイルを *`<base_mount_path>/server/crl`* ディレクトリにコピーします。
6. 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
```

7. cloudmanager_snapcenterコンテナを再起動します。

```
sudo docker restart cloudmanager_snapcenter
```

また、SSL通信の一環として、以下の事項を検証するものとします。

1. 証明書の有効期限
2. 証明書キーの強度
   a. 証明書には、RSA、DSA、またはDHキーが3072ビット以上、ECCキーが224ビット以上のアルゴリズムが必要です。
3. CRL
   a. CRLファイルは、CA証明書を発行したCA機関によって発行されます。SnapCenterエージェントはCA証明書をCAが発行したCRLファイルと照合して検証し、CA証明書が失効しているかどうかを確認します。

注： Cloud Backup for Applicationsでは、Online Certificate Status Protocol（OCSP）ベースの証明書失効ステータスの検証が現在行われていません。製品の将来のバージョンで追加される可能性があります。

ハイブリッド保護のためのBlueXP ConnectorのCA署名証明書の設定

双方向SSLがSnapCenterで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。

手順

1. コネクタにログインします。
2. 次のコマンドを実行して、*`<base_mount_path>`*:

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

3. クライアント証明書フォルダが存在しない場合は作成する

```
cd <base_mount_path>; mkdir -p client/certificate
```

4. CA署名証明書とキーファイルを *<base_mount_path>/client/certificate* コネクタのにコピーします。 ファイル名はcertificate.pemおよびkey.pemにする必要があります。certificate.pemには、中間CAやルートCAなどの証明書チェーン全体が含まれている必要があります。

5. 証明書のPKCS12形式をcertificate.p12という名前で作成し、のままにします *<base_mount_path>/client/certificate*。

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

6. 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
```

7. cloudmanager_snapcenterコンテナを再起動します。

```
sudo docker restart cloudmanager_snapcenter
```

8. 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. **[スタート]>[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. **[Yes]**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. **［証明書 ］> ［追加］ > ［ コンピュータアカウント］ > ［次へ］をクリックします。**
   g. **[ローカルコンピュータ]> [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. **[インポート]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。

SPLテサホオトサレルアンコウ

SPLでサポートされるAES128およびAES256暗号は、サーバとLinuxクライアントの間の通信でのみ使用できます。

```
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
AES256-GCM-SHA384
AES256-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
AES128-GCM-SHA256
AES128-SHA256
```

双方向SSL

BlueXP ConnectorとLinuxプラグインの通信（SPLを使用）の間の双方向SSLはデフォルトで有効になっており、相互のSSL検証を成功させるためには上記の手順を実行する必要があります。

双方向SSLでは、クライアントとサーバの両方が相互に認証して、通信に関与する両方の当事者が信頼されていることを確認します。

SPLの場合、これらのパラメータは `spl.properties` にあるファイルで指定できます `/var/opt/snapcenter/spl/etc/spl.properties`。上記の値はデフォルトでtrueに設定されています。つまり、双方向の相互SSL検証は、通信を強化するためにデフォルトで有効になっています。

```
ENABLE_CERTIFICATE_VALIDATION=true
ENABLE_CLIENT_CERTIFICATE_AUTHENTICATION=true
```

監査

ユーザによるUIからの呼び出しを含むREST APIの呼び出しは、すべてCloud Backup for Applicationsで監査されます。

Cloud Backup for Applicationsは、監査ログの永続化にBlueXPのインフラを利用しています。ログは、Cloud Backup for Applications解決策やそのコンポーネント（BlueXP Connector仮想マシン（VM）やアプリケーションホストなど）には保持されません。Cloud Backup for Applications内でAPI要求が発生すると、API呼び出しが代行受信され、監査ログのコンテンツがキャプチャされて、APIの実行の開始時と終了時に送信されます。監査ログのコンテンツは、REST APIを使用して、Cloud Backup for Applications SaaSサービスによってBlueXPタイムラインに直接直接送信されます。ローカルまたは一時的な永続性はありません。

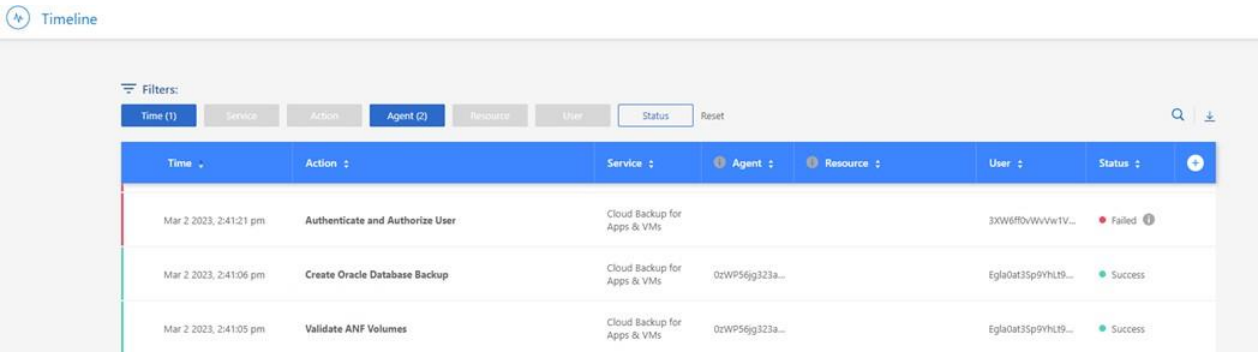
BlueXPのタイムライン機能は、BlueXPで監査ログを維持するために使用されます。これらのログは無期限に保持され、パージされることはありません。

監査ログは、次のような重要な情報で構成されます。

- アクション名。
- アクションを実行したユーザ/クライアントの詳細。
- 開始時刻と終了時刻。
- 処理のステータス（成功/失敗など）。
- クライアントIPアドレス、HTTP URI、ヘッダー、要求本文などの要求の詳細。
- 応答の詳細（ジョブID、エラー（ある場合）など）。

監査ログの例を次に示します（図1）。

図1）監査ログ



Cloud Backup Applications処理でキャプチャされたサンプルの要求ペイロードを次に示します。

```
{
  "host": "stage-request-bus:9430",
  "method": "POST",
  "request_uri": "/account/account-XXXXXXX/providers/cloudmanager_scs_cloud/api/1.0/operations",
  "header": {
    "Accept":
      [ "application/jso
      n"
    ],
    "Authorization":
      [ "******"
    ],
    "Content-Length":
      [ "1000"
    ],
    "Content-Type":
      [ "application/jso
      n"
    ],
    "Operation-Type":
      [ "SmGetMetadataReques
      t"
    ],
    "Referer":
      [ "SnapCenterServic
      e"
    ],
    "// Other request headers": ""
  },
```

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- Cloud Backupのドキュメント
  https://docs.netapp.com/us-en/cloud-manager-backup-restore/concept-protect-cloud-app-data-to-cloud.html#architecture
- BlueXPのドキュメント
  https://docs.netapp.com/us-en/cloud-manager-family/

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2023年3月	最初のドキュメントリリース。
バージョン1.1	2023年7月	7月リリースの追加コンテンツ

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4963-0323-JP