



Technical Report

Security hardening guide: BlueXP Cloud Backup for Applications

ONTAP TME Team, NetApp
July 2023 | TR-4963

Abstract

This guide is targeted for customers of the Cloud Backup for Applications solution, and contains details on NetApp's recommended best practices for securing Cloud Backup for Applications against unauthorized use which can impact confidentiality, integrity, and availability of the solution.

TABLE OF CONTENTS

Hardening Cloud Backup for Applications	4
Introduction	4
Integrity verification of installed components	4
Protection for cloud native applications	5
Network security	5
Connector network requirements	5
TLS security and certificate management.....	6
Configure a CA certificate with the SnapCenter Plug-in Loader service (SPL) on a Linux host for cloud native protection.....	6
Configure CA certificate with BlueXP Connector for cloud native protection.....	7
Ciphers supported by SPL	8
Bi-directional SSL	9
Application plug-in deployment and configuration	9
Network security	9
Fingerprint verification during push install deployment of Oracle plug-in.....	9
Oracle database authentication	10
DB authentication.....	10
ASM authentication	10
Securing the operating system	10
Port security	10
Prescripts and postscripts in workflow execution.....	11
Protection for hybrid applications	12
Network security	12
TLS security and certificate management.....	12
Enable a CA certificate with the SnapCenter Server	13
Ciphers supported by SPL	15
Bi-directional SSL	15
Auditing	16
Where to find additional information.....	17
Version history.....	18

LIST OF TABLES

Table 1) Port requirement.....	5
Table 2) Ports for Cloud Backup Applications operations.....	9
Table 3) Port for hybrid applications.	12

LIST OF FIGURES

Figure 1) Audit log.....	17
--------------------------	----

Hardening Cloud Backup for Applications

Introduction

These guidelines and tools are provided to help you securely perform operations with the goal of making them hack-proof. This involves eliminating or mitigating vulnerabilities. The term vulnerability refers to software flaws and weaknesses, which might occur in the implementation, configuration, design, or the administration of a system. Hardening techniques typically involve locking down configurations and achieving a balance between operational functionality and security. This guide seeks to help operators and administrators in that task with the confidentiality, integrity, and availability integral to the NetApp® solution.

Integrity verification of installed components

Cloud Backup for Applications is a SaaS (software-as-a-service) based service that provides data protection capabilities for applications running on NetApp cloud storage and on-premises NetApp ONTAP storage. Cloud Backup for Applications enabled within NetApp BlueXP (formerly Cloud Manager) offers efficient, application consistent, policy-based protection.

Cloud Backup Applications SaaS, UI and plugin components are validated for integrity using verification tools.

Cloud Backup Applications SaaS - docker image and helm chart signing and verification

[Cosign](#) tool is used to sign docker images and helm charts. The procedure for signing and verification is:

1. A signature is attached to the docker image and helm charts generated by Cloud Backup for Applications during build time, using a Remote Support Agent (RSA) key pair.
2. The images/charts are verified before they are installed in the Cloud Backup for Applications SaaS cluster.

Cloud Backup Applications UI and plugin - binary signing and checksum validation

Details regarding binary signing and the verification mechanism are captured below:

1. Linux plugin binaries are signed during the build time using an RSA key pair.
2. The plugin binary is bundled as a helm chart, which is also signed, as explained above.
3. The binary signature is verified before the plugin binary is pulled by the agent running in the BlueXP Connector.
4. The checksum is generated for the plugin binary during build time; the checksum also is verified by the agent running the BlueXP Connector before pulling the plug-in binary.
5. The UI bundle is also signed using an RSA key pair, and the checksum for the bundle is generated as well, during build time.
6. The UI bundle is verified for signature and checksum when it gets updated as part of the Cloud Backup for Applications build update process.

Protection for cloud native applications

Network security

The purpose of this section is to provide appropriate guidelines for network security against a wide variety of potential threats.

Connector network requirements

The BlueXP Connector inbound/outbound requirements in general are captured in NetApp documentation. This section captures a few additional requirements of Cloud Backup for Applications.

Inbound

No additional inbound rules are required for Cloud Backup for Applications.

Outbound

For cloud native application protection, the BlueXP connector needs to be able to connect to the application hosts which may reside on Amazon Web Services (AWS) or Azure environments. It should also be able to connect to the Amazon FSx for NetApp ONTAP storage management IP, and NetApp Cloud Volumes ONTAP on AWS/Azure, wherever applicable. The following table captures those port requirement (Table 1):

Table 1) Port requirement.

Support	Destination	Application	Cloud platforms	Port	Comments
BlueXP Connector	AWS EC2 Oracle database (DB) host	Oracle	AWS	Secure Shell (SSH) Port (Default: 22)	Required only for SSH based deployments covered below
BlueXP Connector	AWS EC2 Oracle DB host	Oracle	AWS	Plugin Port (Default: 8145)	
BlueXP Connector	AWS FSx	Oracle	AWS	Mgmt API (default: 443)	Connector should have outbound connectivity to FSx mgmt to invoke REST API
BlueXP Connector	Cloud Volumes ONTAP	Oracle	AWS, Azure	Mgmt API (default: 443)	
BlueXP Connector	Azure Compute SAP HANA System Host	SAP HANA	Azure	Plugin Port (Default: 8145)	

For each of the above cases:

1. If the source and destination are on a different virtual port channel (vPC) or Azure Virtual Network (VNet), ensure that there is connectivity between them via vPC/VNet peering etc.
2. Ensure that the network security group in the respective cloud platform allows outbound connection from the BlueXP connector to the application host's port.
3. Ensure that the host side firewall is configured to allow the same communication.

TLS security and certificate management

For communication to occur between a BlueXP connector and a Linux plug-in host, self-signed certificates are used. This section explains how self-signed certificates can be replaced by a Certificate Authority (CA) signed certificate which provides more authenticity and security to the certificate validation involved during HTTPS traffic between these components.

Configure a CA certificate with the SnapCenter Plug-in Loader service (SPL) on a Linux host for cloud native protection

The certificate authority (CA) is a trusted entity that issues Secure Sockets Layer (SSL) certificates. These digital certificates are data files used to cryptographically link an entity with a public key. NetApp SnapCenter® has added support for server and plug-in cross-communication using the authorized CA certificates. All HTTPS calls are validated based on secure SSL standards.

SPL uses the file 'keystore.jks', which is located at '/var/opt/snapcenter/spl/etc' both as its trust-store and key-store on plug-in hosts running on AWS/Azure.

Manage password for SPL key-store and alias of the CA signed key pair in use

Steps

1. Login to the Linux host running SPL.
2. You can retrieve the SPL keystore default password from the SPL property file "spl.properties" located at /var/opt/snapcenter/spl/etc.

It is the value corresponding to the key 'SPL_KEYSTORE_PASS'.

3. Change the key-store password:

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

4. Change the password for all aliases of private key entries in the key-store to the same password used for the key-store:

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

Update the same for the key SPL_KEYSTORE_PASS in the spl.properties file.

5. Restart the SPL service after changing the password.

```
systemctl restart spl
```

Note: The password for the SPL key-store and for all the associated alias passwords of the private key should be the same.

Configure CA signed key pair to SPL trust-store

You should configure the CA signed key pair to the SPL trust-store.

Steps

1. Login to the Linux host running SPL.
2. Navigate to the folder containing the SPL's keystore /var/opt/snapcenter/spl/etc.
3. Locate the file 'keystore.jks'.
4. List the added certificates in the keystore:

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

5. Add the CA certificate, having both a private and a public key.

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

6. List the added certificates in the key-store.

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

7. Verify that the key-store contains the alias corresponding to the new CA certificate, which was added to the key-store.
8. Change the added private key password for the CA certificate to the key-store password.
The default SPL key-store password is the value of the key SPL_KEYSTORE_PASS in the `spl.properties` file.

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

9. If the alias name in the CA certificate is long and contains a space or special characters ("*", ",",), change the alias name to a simple name:

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

10. Configure the alias name from the key-store located in the `spl.properties` file.
Update this value against the key SPL_CERTIFICATE_ALIAS.

11. Restart the SPL service after configuring the CA signed key pair to the SPL trust-store.

```
Systemctl restart spl
```

Configure SPL CA certificate in BlueXP Connector

You should configure the CA certificate generated for SPL in the `cloudmanager_scs_cloud` docker container running inside the BlueXP connector.

Steps:

1. Log in to the BlueXP Connector host as a non-root user.
2. You can run the following command to get the `<base_mount_path>` of `cloudmanager_scs_cloud` docker container.

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

3. Create the server folder if it does not exist.

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

4. Copy the entire chain of CA certificates to the persistent volume located at `<base_mount_path>/server`.
5. Connect to the `cloudmanager_scs_cloud` container and modify the `enableCACert` in `config.yml` to `true`.

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

6. Restart `cloudmanager_scs_cloud` container.

```
sudo docker restart cloudmanager_scs_cloud
```

Configure CA certificate with BlueXP Connector for cloud native protection

The BlueXP Connector uses a self-signed certificate to communicate with plug-ins. The self-signed certificate is imported to the SPL key-store by the installation script. You can perform the following steps to replace the self-signed certificate with a CA signed certificate.

Steps:

1. Log in to the BlueXP Connector host as a non-root user.
2. You can run the following command to get the `<base_mount_path>` of `cloudmanager_scs_cloud` docker container.

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

3. Delete all the existing files located at `<base_mount_path>/client/certificate` in the BlueXP Connector host.
4. Copy the CA signed certificate and key file to the `<base_mount_path>/client/certificate` in the BlueXP Connector host.
The file name should be `certificate.pem` and `key.pem`. The `certificate.pem` should have the entire chain of the certificates like intermediate CA and root CA.
5. Create the PKCS12 format of the certificate with the name `certificate.p12` and keep at `<base_mount_path>/client/certificate`.

Import BlueXP connector's CA certificate to the SPL key-store

Steps:

1. Log in to the BlueXP Connector host as a non-root user.
2. Copy the `certificate.p12` and certificates for all the intermediate CA and root CA kept at `<base_mount_path>/client/certificate` to the Linux plug-in host running SPL at `/var/opt/snapcenter/spl/etc/`. Log in to the plug-in host.
3. Login to the Linux host running SPL.
4. Navigate to `/var/opt/snapcenter/spl/etc` and run the `keytool` command to import the `certificate.p12` file.

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

5. Import the root CA and intermediate certificates.

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

Note: The `certfilecertificate.crt` file refers to the certificates of the root CA as well as the intermediate CA.

6. Restart the SPL service.

```
systemctl restart spl
```

Ciphers supported by SPL

SPL supports AES128 and AES256 ciphers only to communicate between the server and the Linux client.

```
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
```


Bi-directional SSL

Two-way SSL between a BlueXP Connector and Linux plug-in communications (through SPL) is enabled by default, and the steps mentioned above need to be performed for the mutual SSL validation to be successful.

In two-way SSL, both client and server authenticate each other to ensure that both parties involved in the communication are trusted.

For SPL, these parameters can be specified in the `spl.properties` file located at `/var/opt/snapcenter/spl/etc/spl.properties`. The above values are set to true by default, which means that two-way mutual SSL validation is enabled by default for enhanced communication.

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

Application plug-in deployment and configuration

Network security

Inbound

Application hosts need to allow the below ports for Cloud Backup Applications operations (Table 2).

Table 2) Ports for Cloud Backup Applications operations.

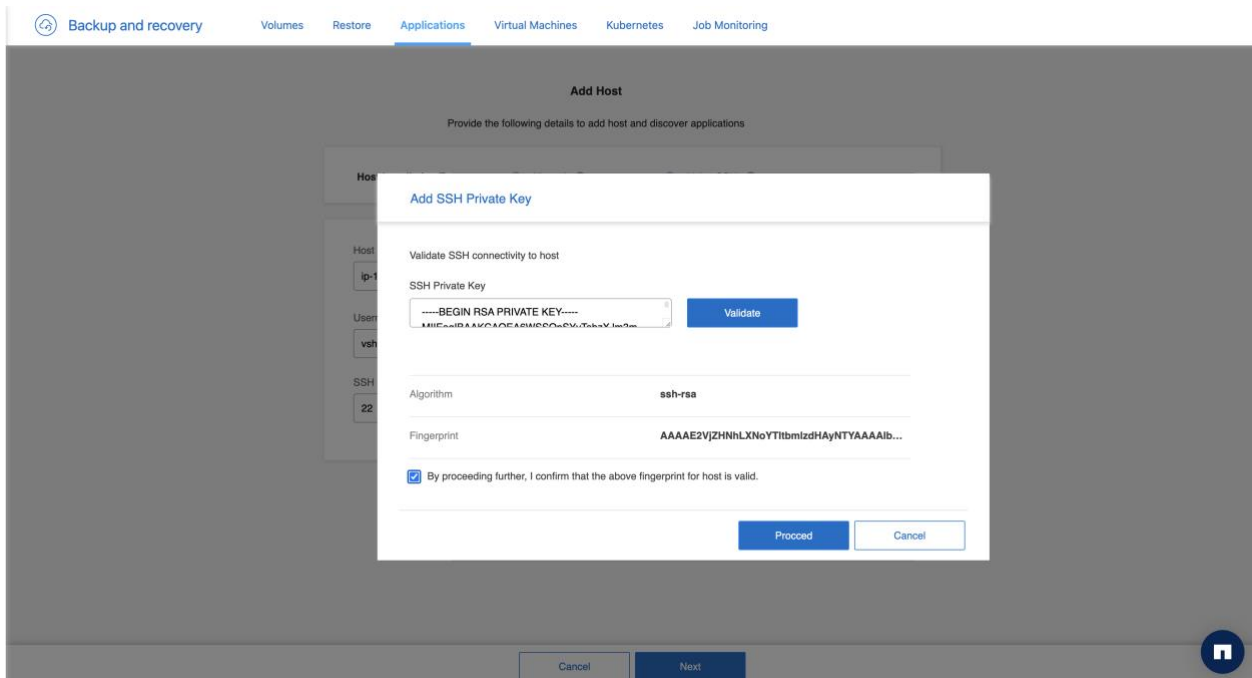
Application	Cloud platforms	Port	Purpose
Oracle	AWS	SSH Port (Default: 22)	Required only for SSH based deployment of application plug-in which is currently supported for Oracle
Oracle	AWS	Plug-in Port (Default: 8145)	Required for regular operations
SAP HANA	Azure	Plug-in Port (Default: 8145)	Required for regular operations

Outbound

No outbound requirements exist for plug-in hosts running Cloud Backup for Applications operations.

Fingerprint verification during push install deployment of Oracle plug-in

- The push install of a plug-in using SSH from the Cloud Backup Applications UI is supported for Oracle applications on AWS FSx.
- As part of the installation operation, before packages are being pushed to the host, you should verify the fingerprint and confirm it by visually confirming against the host. You need to enable the checkbox in the UI to confirm that the fingerprint is a valid one. Please see below screenshot of same.



Oracle database authentication

DB authentication

The Oracle database authentication method authenticates against an Oracle database. You need Oracle database authentication to perform operations on the Oracle database if the operating system (OS) authentication is disabled on the database host. Therefore, before adding an Oracle database credential, you should create an Oracle user in the Oracle database with sysdba privileges.

ASM authentication

The Oracle ASM authentication method authenticates against an Oracle Automatic Storage Management (ASM) instance. If you are required to access the Oracle ASM instance and if the OS authentication is disabled on the database host, you need Oracle ASM authentication. Therefore, before adding an Oracle ASM credential, you should create an Oracle user with sysasm privileges in the ASM instance.

Securing the operating system

Port security

Network ports that are not being used should not be left open. Vulnerable ports specifically, such as port 23 for Telnet connections, should be closed on all systems. The below required ports for the Linux system need to be opened.

- By default, SPL_PORT is set to 8145. However these port values can be configured using the configurable parameters defined in the file `/var/opt/snapcenter/spl/etc/spl.properties`.
- Port 22 (SSH) is required to install the plug-in using either push install or the helper script in the Connector. However, you can skip port 22 from the firewall list if the plug-in is being deployed manually using the documented manual steps.
- Enable port 27216; the default JDBC port is used by the plug-in for Oracle for connecting to the Oracle database.

Use the following command to find a listing of the listening ports:

```
netstat -tulpn
```

With this information, you can determine which listening ports are needed, and which ones should be disabled.

To secure the remaining ports that will be let open, restrict the port access to specific host IP addresses. Depending on the Linux distribution, version, firewall, iptables etc., a common host side firewall is installed on Linux hosts. The host side firewall should enable the SSH and plug-in ports, as required above.

SELinux

Security-Enhanced Linux (SELinux) is a Kernel security mechanism for supporting access control security policy.

The below command can be run to check the current SELinux mode:

```
sestatus
```

You need to set SELinux to permissive so that the SnapCenter for Oracle plug-in is able to perform the operations; otherwise there is a chance of installation failure.

Prescripts and postscripts in workflow execution

Oracle

It is mandatory for the scripts to be placed in the `/var/opt/snapcenter/spl/scripts/` directory; this directory is accessible only to the root user.

SAP HANA

You can provide prescripts, postscripts, and exit scripts while creating a policy. These scripts are run on the HANA host while creating backups.

The supported format for scripts are .sh, python script, perl script, and so on.

The prescript and the postscript should be registered by the host admin into:
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config file

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

Protection for hybrid applications

Network security

For protecting on-premises applications to the cloud, the BlueXP Connector should be able to communicate to the SnapCenter Server. The BlueXP Connector can be deployed either on premises (recommended), or in the cloud (Table 3).

Table 3) Port for hybrid applications.

Source	Cloud platform	Destination port	Comment
BlueXP Connector	On premises, AWS, Azure, or Google Cloud	SnapCenter Server Port (Default: 8146)	The connector, wherever deployed, should have access to the SnapCenter Server whose backups need to be brought to the object store.

Ensure that the SnapCenter Server is reachable from the BlueXP Connector by enabling the same in the network infrastructure.

TLS security and certificate management

For communication to occur between a BlueXP connector and a Linux plug-in host, self-signed certificates are used. This section explains how a self-signed certificate can be replaced by a CA signed certificate which provides more authenticity and security to the certificate validation involved during HTTPS traffic between these components.

Configure a CA certificate with the SnapCenter Server for hybrid protection

Cloud Backup for Applications protection of on-premises applications to the cloud requires connecting to the SnapCenter Server running on the premises. A CA certificate can be configured in the SnapCenter Server by following these steps:

Steps

1. Open IIS Manager on the Windows Server where SnapCenter is installed.
2. In the left navigation pane, click Connections.
3. Expand the name of the server and Sites.
4. Select the SnapCenter website on which you want to install the SSL Certificate.
5. Navigate to Actions > Edit Site, click Bindings.
6. In the Bindings page, select binding for https.
7. Click Edit.
8. From the SSL certificate drop-down list, select the recently imported SSL Certificate.

9. Click OK.

Note: If the recently deployed CA certificate is not listed in the drop-down menu, check if the CA certificate is associated with the private key.

Note: Ensure that the certificate is added using the following path: Console Root > Certificates – Local Computer > Trusted Root Certification Authorities > Certificates.

Enable a CA certificate with the SnapCenter Server

You should configure the CA certificates and enable the CA certificate validation for the SnapCenter Server.

You can enable or disable the CA certificates using the `Set-SmCertificateSettings` cmdlet.

You can display the certificate status for the SnapCenter Server using the `Get-SmCertificateSettings` cmdlet.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name`. Alternatively, you can refer to the [SnapCenter Software Cmdlet Reference Guide](#).

Steps

1. In the Settings page, navigate to Settings > Global Settings > CA Certificate Settings.
2. Select Enable Certificate Validation.
3. Click Apply.

After you finish

The Managed Hosts tab displays a padlock and the color of the padlock indicates the status of the connection between the SnapCenter Server and the plug-in host.



indicates that there is no CA certificate enabled or assigned to the plug-in host.



indicates that the CA certificate is successfully validated.



indicates that the CA certificate could not be validated.



indicates that the connection information could not be retrieved.

Note: When the status is yellow or green, the data protection operations complete successfully.

Configure SnapCenter Server CA certificate in BlueXP Connector for hybrid protection

You should configure SnapCenter server CA signed certificate in BlueXP Connector so that the Connector can verify the SnapCenter's certificate. ([Learn about Connectors](#)).

Steps:

1. Log in to the BlueXP Connector host as a non-root user.
2. You should run the following command in the BlueXP Connector to get the `<base_mount_path>`:

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

3. Navigate to the certificate folder in the connector

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

4. Copy the root CA and intermediate CA files to the <base_mount_path>/server/certificate directory. The CA files should be in .pem format.
5. If you have CRL files, perform the following steps:
 - a. cd <base_mount_path>; mkdir -p server/crl
 - b. Copy the CRL files to the <base_mount_path>/server/crl directory.
6. Connect to the cloudmanager_snapcenter and modify the enableCACert in config.yml to true.

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

7. Restart cloudmanager_snapcenter container.

```
sudo docker restart cloudmanager_snapcenter
```

In addition, the following shall be validated as part of the SSL communication.

1. Certificate expiry
2. Certificate key strength
 - a. The Certificate should have RSA, DSA, or DH keys greater than or equal to 3072 bits and ECC keys greater than or equal to 224 bits or stronger algorithm.
3. CRL
 - a. CRL file(s) is issued by the CA authority who has issued the CA certificate. SnapCenter Agent validates CA certificate against CA issued CRL file(s) to check whether CA certificate is revoked or not.

Note: The Online Certificate Status Protocol (OCSP) based certificate revocation status verification is currently absent in Cloud Backup for Applications. It could be added in a future version of the product.

Configure CA signed certificate for BlueXP Connector for hybrid protection

If two way SSL is enabled in SnapCenter, you should perform the following steps on the Connector to use the CA certificate as the client certificate when the Connector is connecting with the SnapCenter.

Steps

1. Log in to the Connector.
2. You should run the following command to get the <base_mount_path>:

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

3. Create the client certificate folder if it is not present

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

4. Copy the CA signed certificate and key file to the `<base_mount_path>/client/certificate` in the Connector. The file name should be `certificate.pem` and `key.pem`. The `certificate.pem` should have the entire chain of the certificates like intermediate CA and root CA.
5. Create the PKCS12 format of the certificate with the name `certificate.p12` and keep at `<base_mount_path>/client/certificate`.

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

6. Connect to the `cloudmanager_snapcenter` and modify the `sendCACert` in `config.yml` to true.

```
sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert: false/sendCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml
```

7. Restart `cloudmanager_snapcenter` container.

```
sudo docker restart cloudmanager_snapcenter
```

8. Perform the following steps on the SnapCenter to validate the certificate sent by the Connector.
 - a. Login to the SnapCenter Sever host.
 - b. Click **Start > Start Search**.
 - c. Type `mmc` and press **Enter**.
 - d. Click **Yes**.
 - e. In File menu, click **Add/Remove Snap-in**.
 - f. Click **Certificates > Add > Computer account > Next**.
 - g. Click **Local computer > Finish**.
 - h. If you have no more snap-ins to add to the console, click **OK**.
 - i. In the console tree, double-click **Certificates**.
 - j. Right-click the **Trusted Root Certification Authorities store**.
 - k. Click **Import** to import the certificates and follow the steps in the **Certificate Import Wizard**.

Ciphers supported by SPL

SPL supports AES128 and AES256 ciphers only to communicate between the server and Linux client.

```
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
```

Bi-directional SSL

Two-way SSL between a BlueXP Connector and Linux plug-in communications (through SPL) is enabled by default, and the steps mentioned above need to be performed for the mutual SSL validation to be successful.

In two-way SSL, both client and server authenticate each other to ensure that both parties involved in the communication are trusted.

For SPL, these parameters can be specified in `spl.properties` file located at `/var/opt/snapcenter/spl/etc/spl.properties`. The above values are set to true by default, which means that two-way mutual SSL validation is enabled by default for enhanced communication.

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

Auditing

All REST API invocations, including user-initiated invocations from the UI, are audited in Cloud Backup for Applications.

Cloud Backup for Applications rely on BlueXP's infrastructure for persisting the audit logs. The logs are not persisted within the Cloud Backup for Applications solution or any of its components such as the BlueXP Connector virtual machine (VM) or application hosts. Whenever an API request happens within Cloud Backup for Applications, the API call is intercepted, and the audit log content is captured and sent at both start and finish of the API execution. The audit log content is immediately sent to a BlueXP timeline directly, using its REST API, by the Cloud Backup for Applications SaaS service, without any local/temporary persistence.

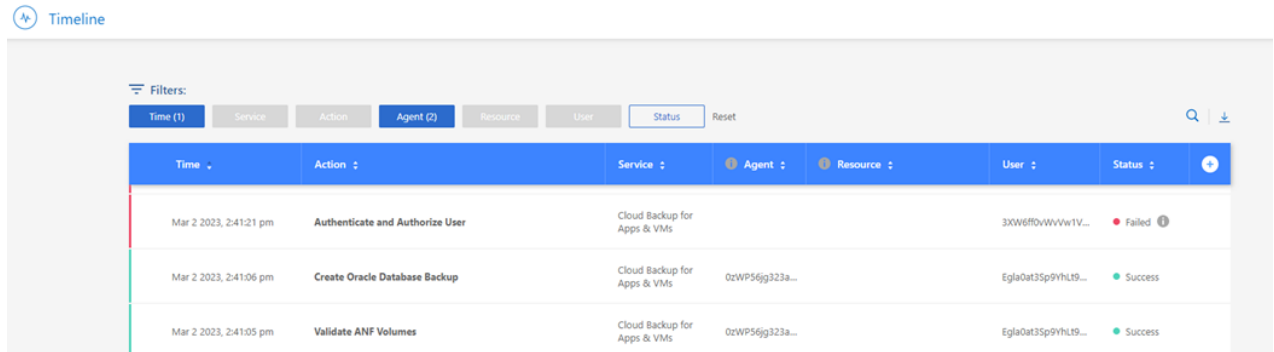
The timeline feature of BlueXP is used to persist audit logs in BlueXP. These logs are retained forever, and not purged.

The audit log consists of key information such as:

- The action name.
- Details of user/client who performed the action.
- Start and end time.
- Status of the operation such as success/failed.
- Request details such as client IP address, HTTP URI, headers, request body.
- Response details such as job ID, error, if any.

A sample audit log is shown below (Figure 1).

Figure 1) Audit log.



Time	Action	Service	Agent	Resource	User	Status
Mar 2 2023, 2:41:21 pm	Authenticate and Authorize User	Cloud Backup for Apps & VMs			3XW6ff0vWwV1V...	Failed
Mar 2 2023, 2:41:06 pm	Create Oracle Database Backup	Cloud Backup for Apps & VMs	0zWP56jg323a...		Egla0at35p9YhL19...	Success
Mar 2 2023, 2:41:05 pm	Validate ANF Volumes	Cloud Backup for Apps & VMs	0zWP56jg323a...		Egla0at35p9YhL19...	Success

The sample request payload captured for a Cloud Backup Applications operation is given below:

```
{
  "host": "stage-request-bus:9430",
  "method": "POST",
  "request_uri": "/account/account-XXXXXXX/providers/cloudmanager_scs_cloud/api/1.0/operations",
  "header": {
    "Accept": [
      "application/json"
    ],
    "Authorization": [
      "*****"
    ],
    "Content-Length": [
      "1000"
    ],
    "Content-Type": [
      "application/json"
    ],
    "Operation-Type": [
      "SmGetMetadataRequest"
    ],
    "Referer": [
      "SnapCenterService"
    ],
    "// Other request headers": ""
  },
  "body": {
    "// The request body": ""
  }
}
```

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- Cloud Backup documentation
<https://docs.netapp.com/us-en/cloud-manager-backup-restore/concept-protect-cloud-app-data-to-cloud.html#architecture>
- BlueXP documentation
<https://docs.netapp.com/us-en/cloud-manager-family/>

Version history

Version	Date	Document version history
Version 1.0	March 2023	Initial document release.
Version 1.1	July 2023	Appended content for July release

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4963-0323