Fortanix

Integration Guide

FORTANIX DATA SECURITY MANAGER WITH VERITAS NETBACKUP

VERSION 1.0

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

1.0 INTRODUCTION

1.1 OVERVIEW

This document describes how to use Fortanix Data Security Manager (DSM) to encrypt Veritas NetBackup storage.

1.2 INTENDED AUDIENCE

The intended audience of this document includes Veritas and Fortanix Sales Engineers, Field and Technical Support Engineers, and customer architects and engineers who want to learn and understand how to implement the Fortanix DSM into their Veritas environment.

2.0 FORTANIX DATA SECURITY MANAGER

Fortanix DSM is the world's first cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, and secrets, such as passwords, API keys, tokens, or any blob of data.

3.0 PREREQUISITES

- Fortanix DSM version 3.27 or later is installed and operational.

4.0 SETTING UP THE FORTANIX DATA SECURITY MANAGER

4.1 CREATE NEW VERITAS INSTANCE

1. Sign up at https://amer.smartkey.io/
2. Log in to the Fortanix DSM UI.
3. Click the **Integrations** tab in the left panel.
4. On the Integrations page, click **ADD INSTANCE** on the Veritas wizard.
5. Enter the following details:
   a. **Add Instance**: This is the name to identify the instance created.
   b. **Authentication method**:
      - **API key**: This method authenticates the application with the API Gateway.
      - **Client Certificate**: This method is used to authenticate the application with Fortanix DSM using a Client Certificate. Refer to Section 4.2.
6. Select **API key** as the authentication method.
7. Click **SAVE INSTANCE**.

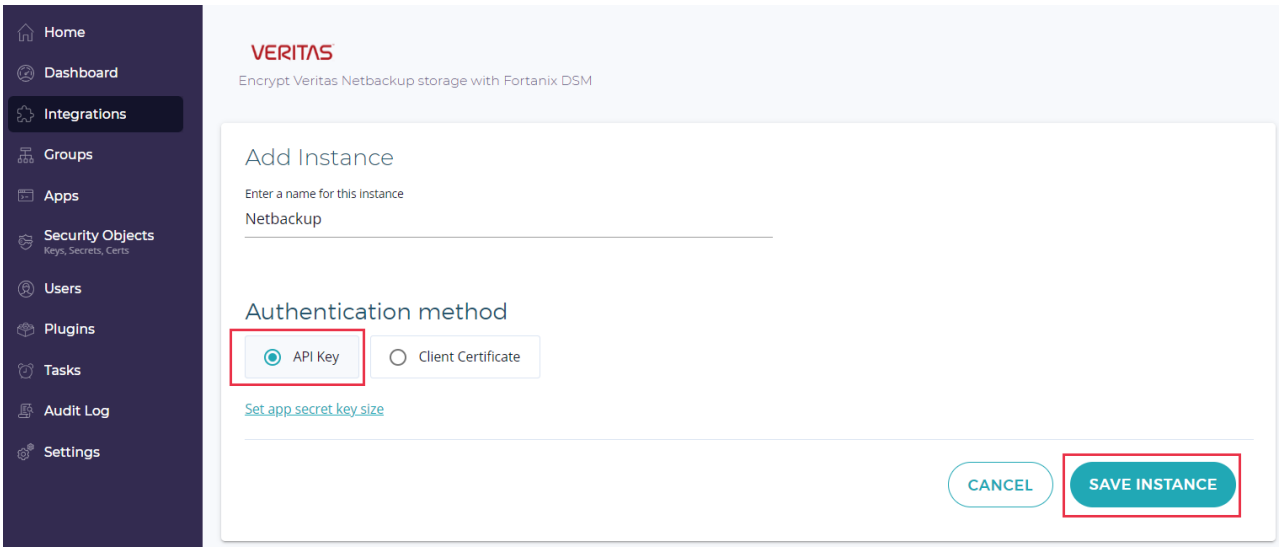

FIGURE 1: CREATE INSTANCE

With creating an instance, a new group and app are created within Fortanix DSM.

4.2 AUTHENTICATE USING A CLIENT CERTIFICATE

1. In the Veritas instance table, under the **Credentials** column, for the instance created, click **VIEW CREDENTIALS**.
2. In the "View credentials" dialog box, select the **USERNAME/PASSWORD** tab and copy the Username (**app UUID**).

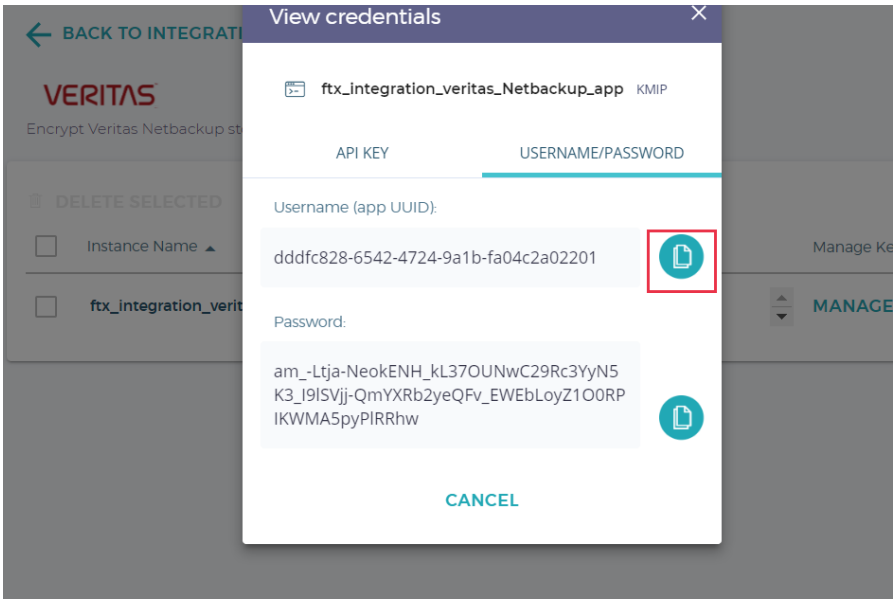

FIGURE 2: COPY UUID

3. To generate a client certificate and private key, use OpenSSL, and create a new key+cert with `CN=FORTANIX_APP_UUID`.

```
$ export FORTANIX_APP_UUID= dddfc828-6542-4724-9a1b-fa04c2a02201

openssl req -newkey rsa:2048 -nodes -keyout netbackup.key -x509 -
days 365 -out netbackup.crt -subj \
  "/C=US/ST=California/L=Mountain View/O=Fortanix,
Inc./OU=SE/CN=$FORTANIX_APP_UUID"
```

4. Now, go to the detailed view of the app that the instance automatically created.
5. In the app's detailed view, click **Change the authentication method** and select **Certificate** to change the authentication method to Certificate.
6. Click **SAVE.**
7. In the **Add certificate** dialog box, copy or upload the Certificate generated in *Step 3* above in the **Upload certificate** text box and update the authentication method.

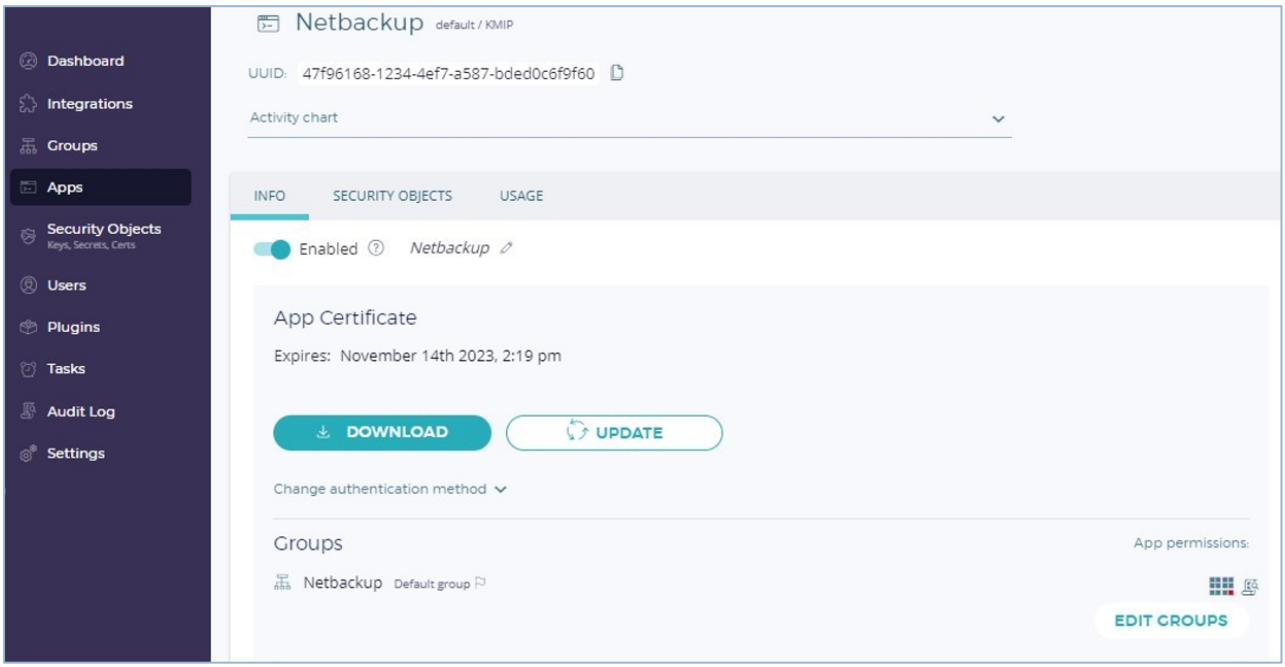

FIGURE 3: APP CERTIFICATE

5.0 CONFIGURATION ON VERITAS NETBACKUP

NOTE: In this article, Veritas NetBackup is installed on Windows. To install it on Linux, contact the Fortanix Customer Success Team.

1. Go to the installation location where NetBackup is installed on Windows.
2. In this example, NetBackup is installed in the default location, that is, `C:/Program Files/Veritas/NetBackup/bin`.
3. NetBackup comes with in-built KMS Commands. The command `nbkmscmd.exe` can be configured with Fortanix Key Management Solution.

5.1 KEY MANAGEMENT SERVICE (KMS) OPERATIONS

- `-configureKMS` - Adds an entry for the KMS configuration in the NetBackup database.
- `-deleteKMSConfig` - Deletes the KMS configuration entry from the NetBackup database.
- `-listKMSConfig` - Lists the details of the specified KMS configuration in JSON format.
- `-updateKMSConfig` - Updates the specified KMS configuration in the NetBackup database.
- `-discoverNBKMS` - Discovers whether the NetBackup KMS is configured and running and adds it to NetBackup.
- `-validateKMSConfig` - Validates the functionality with the specified KMS configuration and ensures that backup and restore functionality works.
- `-precheckKMSConfig` - Performs a dry run of KMS configuration operations to validate the required connections and setup.

5.2 CREDENTIALS MANAGEMENT OPERATIONS

- `-configureCredential` - Adds the KMS configuration credential in the NetBackup database. The credential ID and its credential name are added in the database.
- `-deleteCredential` - Deletes the specified KMS configuration credential from the NetBackup database.
- `-listCredential` - Lists the details of the specified KMS configuration credential in JSON format. If the credential name or ID is not specified, the credential details for all KMS configurations are listed.
- `-updateCredential` - Updates the specified KMS configuration credential.

5.3 KEY MANAGEMENT OPERATIONS

- `-createKey` - Creates an active NetBackup key in the KMS server that is associated with the provided configuration name.

  To create a key, the KMS server should allow NetBackup to create a key and set NetBackup attributes on that key.

  For NetBackup KMS, If the specified key-group name does not exist, the key-group is created with the specified algorithm.

- `-listKeys` - Lists the NetBackup keys from the specified KMS configuration in JSON format.

5.4 CONFIGURATION STEPS ON VERITAS NETBACKUP

1. Create the API Key in Veritas NetBackup Security Access Keys as shown above.

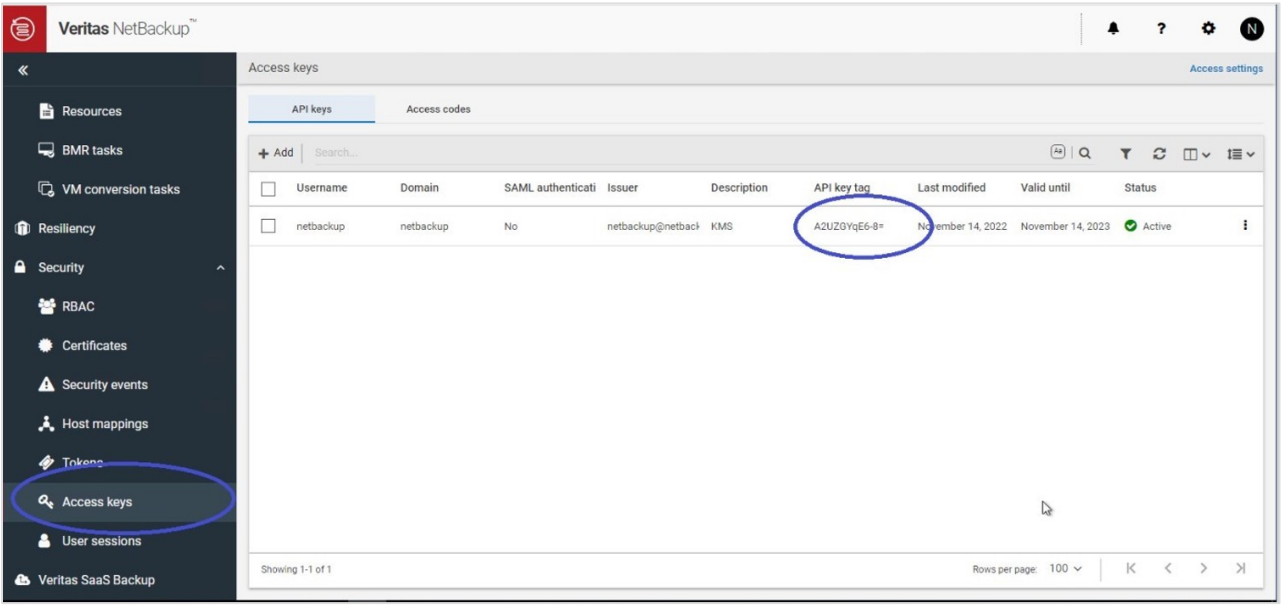

FIGURE 4: CREATE API KEY IN VERITAS

2. Log in to `NBKMSCMD.EXE` from the command prompt.

```
C:\Program Files\Veritas\NetBackup\bin>bpnbat.exe -login -loginType APIKEY
Master server: netbackup
Login Name: netbackup
API key: ************************************************************
Operation completed successfully.

C:\Program Files\Veritas\NetBackup\bin>_
```

FIGURE 5: LOG IN TO NBKMSCMD

NOTE: The API Key can be retrieved from NetBackup WebUI.

3. For creating the credentials in NetBackup you need the following:
    a. OpenSSL self-signed certificate created with App UUID uploaded in Fortanix DSM App UI.
    b. The private key associated with the certificate.
    c. Fortanix DSM certificate chain (which can be downloaded from the browser).
4. Configure the KMS in Fortanix as shown in the following screenshot.

FIGURE 6: CONFIGURE KMS

5. Verify if the KMS has been configured.

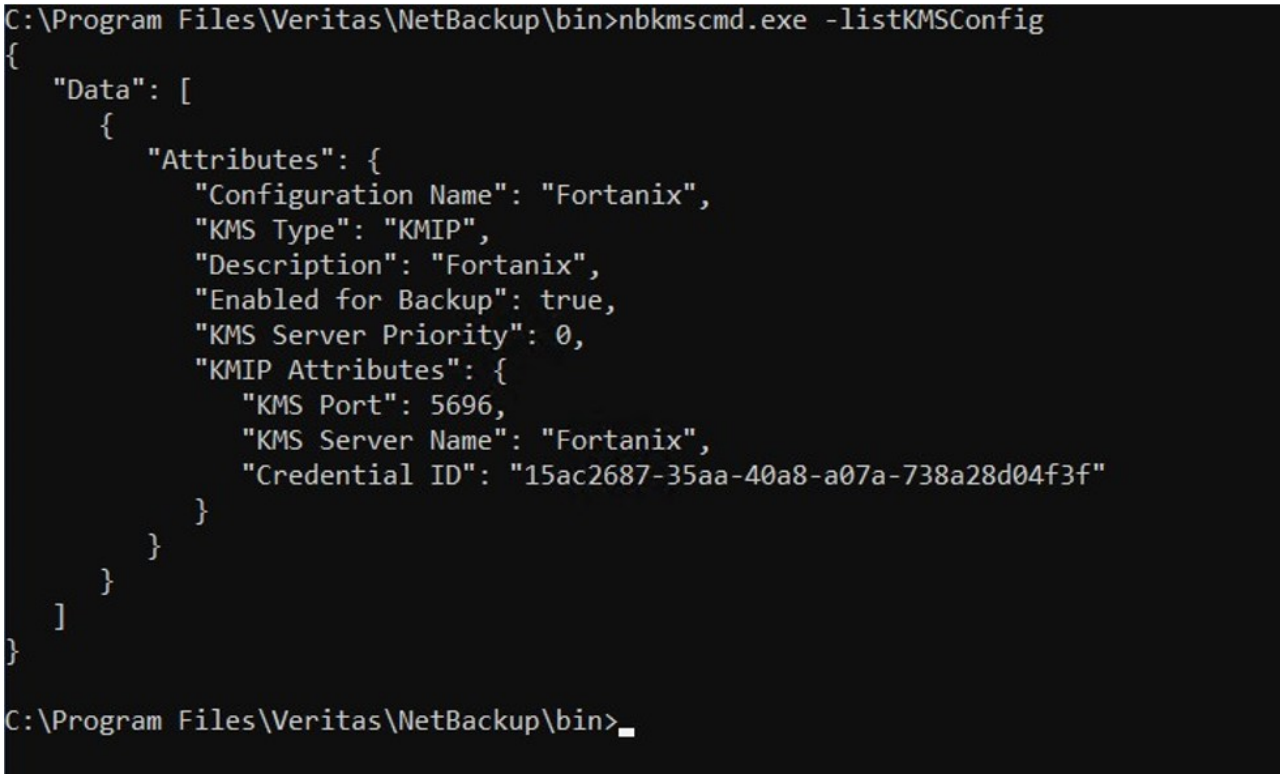

FIGURE 7: VERIFY KMS

6. Create a key with NetBackup CLI in Fortanix DSM.

```
nbkmscmd.exe -configureKMS -name Fortanix -type KMIP -kmsServerName
Fortanix -port 5696 -credId 15ac2687-35aa-40a8-a07a-738a28d04f3f -
enabledForBackup 1 -description Fortanix
```

7. After the command runs successfully, You can run the following command to list the keys.

```
nbkmscmd.exe -listKeys -name Fortanix
```

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/12883881039508-Using-Fortanix-Data-Security-Manager-with-Veritas-NetBackup

6.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com