NetBackup and Veritas Appliances Hardening Guide

Spring 2023

VERITAS™

Contents

Chapter 1

Top recommendations to improve your NetBackup and Veritas appliances security posture

This chapter includes the following topics:

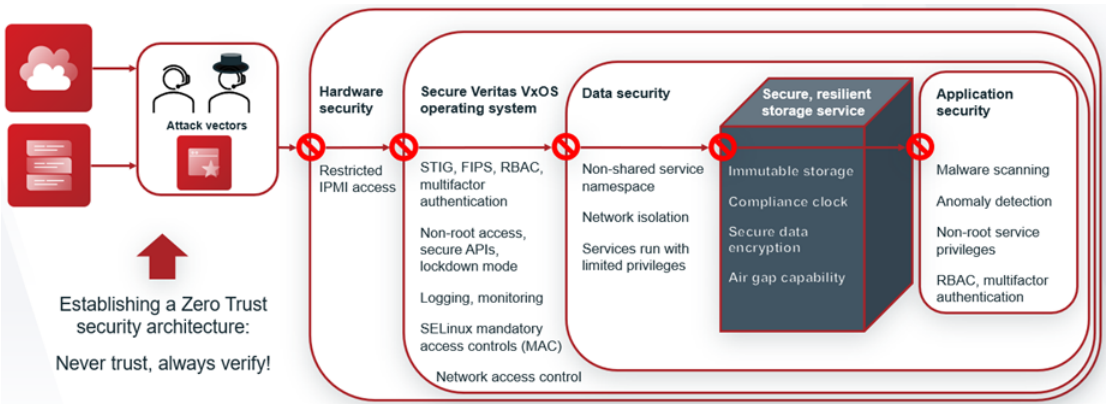
Introduction

Veritas NetBackup and Veritas appliances bring together the power of NetBackup software with state-of-the-art servers and storage technology to create enterprise-class data protection with enhanced ransomware resiliency.

Ransomware attacks are on the rise. Intelligence channels increasingly show that attackers use stolen credentials to gain unauthorized access to backup software and appliances. The likelihood of a successful attack increases dramatically in the presence of out-of-date software, poor password management practices, generic user IDs, and the lack of multifactor authentication.

Figure 1-1 shows how Veritas products use a multi-layered approach to protect against cyberattacks.

Figure 1-1 Multi-layered security



Veritas highly recommends that you take advantage of the security features in our products to bolster your cybersecurity defenses, like multifactor authentication, lockdown mode, and immutability.

Do not put your critical backup data at risk. Follow the steps in this document to improve your NetBackup and Veritas appliances security posture.

Keeping all systems and software updated

Veritas delivers new releases and patches that add security features and address vulnerabilities. Register at the Veritas NetInsight Console SaaS portal to receive proactive recommendations on product upgrades, such as security patches, hotfixes, and major or maintenance release updates.

The recommendations in this document apply to the following releases:

- Flex Appliance 3.0
- NetBackup Appliance 5.1.1
- NetBackup 10.2

Links to the latest software releases:

- Veritas NetInsight Console
- Veritas Download Center
- NetBackup Automated Upgrades

Enabling multifactor authentication

Multifactor authentication uses at least two sources of verification to gain access to a resource. It is commonly used for activities like bank sign-ins and VPN access and can help you to align with your existing Identity and Access Management (IAM) policies.

Veritas products provide multifactor authentication with the single sign-on feature or with smart cards and digital certificates.

How to enable single sign-on:

- Flex Appliance
  See “Managing single sign-on (SSO)” on page 18.
- NetBackup Appliance
  See “About single sign-on (SSO) authentication and authorization” on page 43.
- NetBackup
  See “Configure NetBackup for single sign-on (SSO)” on page 68.

How to enable smart cards or digital certificates:

- Flex Appliance
  See “Managing user authentication with smart cards or digital certificates” on page 22.
- NetBackup Appliance
  See “About authentication using smart cards and digital certificates” on page 46.
- NetBackup
  See “Configure user authentication with smart cards or digital certificates” on page 75.

Increasing the appliance security level

By default, Veritas appliances offer a hardened environment for protecting your infrastructure. Lockdown mode adds unique protection from credential compromise with its built-in One Time Password (OTP) mechanism, which prevents unauthorized access to the operating system.

NetBackup uses access codes for a similar purpose, to prevent unauthorized access to commands.

How to enable lockdown mode or access codes:

- Flex Appliance
  See “About lockdown mode” on page 24.
- NetBackup Appliance
  See “Disable user access to the NetBackup appliance operating system” on page 51.
- NetBackup
  See “Access codes” on page 77.

Implementing an immutable data vault

One of the best ways to safeguard your data is to implement immutable and indelible storage. This type of storage ensures that data cannot be changed, encrypted, or deleted for a determined length of time (or at all). Veritas appliances and NetBackup provide secure and tamper-resistant immutable and indelible storage to protect data backups from being tampered with and from unauthorized access.

Veritas also offers the ability to store immutable data in the cloud on object storage, including Veritas Alta Recovery Vault or with third-party OpenStorage Technology (OST) vendors. Veritas Alta Recovery Vault also creates a separation of duties where Veritas manages the administration of the storage and provides you another layer of isolation from attack.

These features are vital to an effective and a rapid recovery strategy.

With the addition of immutability, Veritas now recommends a new strategy for backups. In the past, the recommendation was a 3-2-1 strategy: three copies of data, two on site on different media, and one copy off site. The current rise in cyber threats calls for an extra "1," creating a 3-2-1+1 strategy: three copies of data, two on site on different media, one copy off site, and one copy that is immutable.

How to configure immutability:

- Flex Appliance
  See “Creating a NetBackup WORM storage server instance” on page 29.
- NetBackup
  See “Workflow to configure immutable and indelible data” on page 79.

This feature is not currently available for NetBackup Appliance.

Securing credentials

To avoid poor credential management practices, do not reuse or share passwords, and do not keep files of passwords on any systems. These practices create security, auditability, and compliance issues.

Veritas products support external password management solutions. You can deploy CyberArk Privileged Access Management (PAM) solutions to enforce a password rotation policy and monitor all activity in privileged sessions.

How to configure an external password management solution:

- Flex Appliance and NetBackup Appliance
  Download the appliance plug-ins from the CyberArk marketplace.

- NetBackup
  See “Add a configuration for an external CMS server” on page 81.

Reducing network exposure

You can reduce your network exposure with the following features.

Network access control

Network access control can ensure that only authorized personnel can access selected networks or network segments to access backup administrative interfaces. For example, you can use an allowed list to control which IP addresses and subnets can access your appliances through SSH and HTTPS. All IP addresses that are not on the allowed list are blocked by default. This feature is an example of network segmentation and can prevent attackers from gaining system access.

How to configure network access control:

- Flex Appliance
  See “Using network access control” on page 26.
- NetBackup Appliance
  See “About Network Access Control” on page 52.
- NetBackup
  Network access control for NetBackup is available through the isolated recovery environment (IRE) feature. See the following section.

Isolated recovery environments

Another way to isolate and protect backups is to create an isolated recovery environment (IRE). NetBackup BYO and Flex Appliance include a turnkey, pull-based IRE that creates an air-gapped network environment. This feature lets you create a vault for your data. Additionally, the proprietary compliance secure clock provides added confidence that your storage is never subject to time-based attacks that are meant to expire data prematurely.

How to configure an IRE:

- Flex Appliance
  See “Configuring an isolated recovery environment on a WORM storage server” on page 34.
- NetBackup
  See “Configuring an isolated recovery environment on a NetBackup BYO media server” on page 83.

Currently, NetBackup Appliance can be used for the production environment of an IRE but not as the target server.

Enabling encryption

Veritas recommends that you enable data encryption at rest and in transit. Encryption prevents unauthorized data access and theft. If data is encrypted with robust industry standards, attackers cannot access it even if the data is stolen.

NetBackup software provides various options to configure encryption. To ensure optimal security, NetBackup includes encryption features for data at rest and in transit. You can encrypt your data before you send it to the cloud. You can use the built-in NetBackup key manager service (KMS) or configure NetBackup with a third-party KMS during storage server configuration.

Another way that your data is protected is with certificates, which create an encrypted connection between hosts. By default, Veritas products use self-signed certificates for host communication. You can choose to configure external certificates instead. When you use external certificates, they are validated for authenticity by an external certificate authority (CA). In this way, the identity of the certificate holder is verified through a publicly known and trusted third party.

How to enable encryption:

- Flex Appliance
  Flex Appliance meets Federal Information Processing Standards (FIPS) 140-2 standards to keep data encrypted at rest and in transit. FIPS is enabled during the Flex Appliance installation process.
- NetBackup Appliance
  See “About data encryption ” on page 53.
  See “FIPS 140-2 conformance for NetBackup Appliance” on page 57.
- NetBackup
  See “About FIPS support in NetBackup” on page 90.
  See “Installing KMS” on page 96.
  See “Workflow for external KMS configuration” on page 100.
  See “Workflow to configure data-in-transit encryption” on page 104.

How to configure external certificates:

- Flex Appliance
  See “Using an external certificate” on page 27.
- NetBackup Appliance
  See “About implementing external certificates” on page 60.
- NetBackup

See "Workflow to use external certificates for NetBackup host communication" on page 130.

Enabling catalog protection

Veritas recommends that you protect NetBackup catalogs with dedicated policies for disaster recovery purposes. Failure to back up the NetBackup primary catalog may result in lengthy reconstruction activities in the event of a site disaster, hardware failure, or malicious attack. Two critical components should be protected: the NetBackup primary server catalog and the Media Server Deduplication Pool (MSDP) catalog.

For immutable storage, you can also create shadow copies of the catalog with the deduplication shell.

How to enable catalog backups:

- Flex Appliance
  For primary and media server instances, follow the same steps as NetBackup.
  See "Protecting the NetBackup catalog on a WORM storage server" on page 40.
- NetBackup Appliance
  Follow the same steps as NetBackup.
- NetBackup
  See "Guidelines for managing the primary server NetBackup catalog" on page 159.
  See "About protecting the MSDP catalog" on page 161.

Enabling malware scanning and anomaly detection

Malware and ransomware programs may go undetected on the server and the storage system for days, weeks, or months. These long durations make it possible that the malware may be backed up along with the regular backups if existing antivirus and antimalware tools miss the signature. In a ransomware event, the best practice is to scan backups before recovery to find and eliminate malware before it is restored. To plan ahead before an actual cyber event, you can implement anomaly detection and malware scanning against production backups.

Veritas NetBackup provides unique built-in anomaly detection and malware scanning to help detect malware and ransomware early. Once malware scanning is enabled, make sure that critical events are sent to a security information and event management (SIEM) system for alerts and security incident orchestration through platforms like Service Now.

How to enable malware scanning and anomaly detection:

- Flex Appliance and NetBackup Appliance
  Follow the same steps as NetBackup.
- NetBackup
  See "How to set up malware scanning" on page 167.
  See "About backup anomaly detection" on page 170.

Enabling security observability

To detect and prevent threats, organizations need to promptly spot malicious insiders, compromised accounts, malware infections, and other problems. With NetBackup and Veritas appliances, you can forward logs to an external log management server or a security information and event management (SIEM) solution. The logs include elevated shell commands for the appliances and have consistent timestamp formats, which are necessary for accurate and efficient event correlations and log analysis.

SIEM, SOAR, and XDR platforms are tools to combat unwanted trends and unsanctioned actions in IT ecosystems. NetBackup audit messages can be custom filtered and consumed by SIEM platforms, which scan the system log of the primary server and digest that information to provide reports, insights, and alerts. Automated response integration within NetBackup can automatically pause clients to stop any spread of undesired data, and SOAR integrations allow further customized actions based on scenarios in the various message categories. NetBackup adds more capability to your ransomware response plans with the insight and control of audit messaging.

How to enable log forwarding:

- Flex Appliance
  See "Forwarding logs" on page 29.
- NetBackup Appliance
  See "About forwarding logs to an external server" on page 63.
- NetBackup
  See "Send audit events to system logs" on page 175.
  See "Send audit events to log forwarding endpoints" on page 175.

Flex Appliance also includes a security meter to view and configure the security settings from one location. The security meter tracks the security settings and shows you a list of the available features with quick links to configure them. It is accessible from the Flex Appliance Console home page by a security administrator.

Figure 1-2 shows how the security meter works, or you can see it in action in the security meter demo.

Figure 1-2 Security meter

Restricting user access

Veritas products support local users and remote users from Active Directory and LDAP user domains, who you can add as individual users or as user groups. As a best practice, you should only add those users or groups who need access to the system and restrict access from those who do not.

Note: When you connect a remote user domain to a Flex Appliance application instance, all users on the domain can log in to the instance. You must perform additional steps to restrict access to specific users or groups. For details, see the topics “Connecting an Active Directory user domain to a primary or a media server instance” and “Connecting an LDAP user domain to a primary or a media server instance” in the *NetBackup Application Guide*.

Configuring a sign-in banner

A sign-in banner is a customized text banner that appears every time that a user signs in to a product. You can use a sign-in banner to communicate important

information to users. For example, a banner may include a security policy or a warning that they are on a restricted system and that all activity is logged.

How to configure a sign-in banner:

- Flex Appliance
  See “Using a sign-in banner” on page 41.
- NetBackup Appliance
  See “Creating the appliance login banner” on page 65.
- NetBackup
  See “Display a banner to users when they sign in” on page 176.

Chapter 2

Steps to protect Flex Appliance

This chapter includes the following topics:

About Flex Appliance hardening

This chapter contains information on the Flex Appliance features that can help to secure your data protection infrastructure.

The following features are enabled by default:

- Intrusion detection and prevention through Security-Enhanced Linux (SELinux)

- Conformance to the OS hardening rules of the Security Technical Implementation Guides (STIGs).
- Conformance to the Federal Information Processing Standards (FIPS) 140-2.

Use the procedures in this chapter to enable other features to protect your appliance.

For more detailed information about Flex Appliance security, see the following guides:

- *Flex Appliance Getting Started and Administration Guide*
- *NetBackup Application Guide for Flex Appliance*
- *NetBackup Flex Appliance Security* white paper

Managing single sign-on (SSO)

The Flex Appliance Console supports single sign-on (SSO). Note the following prerequisites and considerations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported.
- SSO users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with a SAML-authenticated user.
- SSO users must use the fully qualified domain name (FQDN) in the URL to access the Flex Appliance Console. For example, **https://*consoleFQDN***. The IP address option does not work for SSO.
- Single logout (SLO) is supported if an SLO POST binding URL is present in the identity provider (IDP) metadata. If it is not present, you sign out only from the appliance and not from the IDP. In this situation, Veritas recommends that you close your browser after signing out for security purposes.

Note: For some IDPs with SLO, you are not redirected to the sign-in page after you sign out of the console. Open a new session to sign back in.

Configuring SSO

Perform the following steps to configure SSO.

To configure SSO

1. Add the SSO identity provider (IDP).

   See the section called “Adding an IDP” on page 19.

2. From the **Single sign-on** page, select the check box next to **Enable single sign-on** to enable SSO.

3. Import the SSO users that you want to have access to the Flex Appliance Console.

Enabling or disabling SSO

Use the following procedure to enable or disable SSO. You must have added at least one IDP.

To disable or enable SSO

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.

2. Select or deselect the check box next to **Single sign-on**.

Managing identity providers (IDPs)

You can configure single sign-on (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol and AD or LDAP directory services. You can add up to three IDPs to the appliance but can use only one at a time.

Note: The date and time of the appliance, the IDP, and the browser must be synchronized. Veritas recommends that the date and time are set using NTP.

Use the following procedures to manage your IDPs.

Adding an IDP

To add an IDP

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.

2. Under **Appliance service provider URL**, copy or download the appliance metadata file. Upload that file to your IDP and add the appliance as a service provider. For more specific instructions, see the following articles on the Veritas Support website:

   - Active Directory Federation Services (ADFS)
   - IBM

- Microsoft Azure Active Directory
- Okta
- Ping Federate
- Shibboleth

3 From the IDP, download and save the IDP metadata XML file.

4 Gather the following information for the IDP:

- Name: A name of your choosing to identify the IDP.
- User field: The SAML attribute name that is mapped to the user attribute of the remote user domain. For example, **userPrincipalName**, **displayName**, **identifier**, **uid**, etc.
- Group field: The SAML attribute name that is mapped to the group attribute of the remote user domain. For example, **memberOf**, **role**, etc.

5 From the **Single sign-on** page on the Flex Appliance Console, click **Add**.

6 Upload the IDP metadata file. Once the file has uploaded successfully, click **View details** and verify the certificate subject values and SHA-256 fingerprints.

7 Fill in the other required fields, then click **Save**.

8 If you have added only one IDP, enable SSO to start using it. See the section called “Enabling or disabling SSO” on page 19.

If you have added more than one IDP, the first IDP is used by default. Switch to the new IDP if necessary. See the section called “Switching to a different IDP” on page 21.

Editing an IDP

To edit an IDP

1 If you need to change the IDP metadata XML file, download the file from the IDP.

2 Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.

3 Click the name of the IDP, then click **Edit**.

4 Make the required changes. If you uploaded a new IDP metadata file, click **View details** and verify the certificate subject values and SHA-256 fingerprints.

5 When you are done, click **Save**.

Switching to a different IDP

To switch to a different IDP

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. If you have not done so already, add the IDP that you want to use. See the section called “Adding an IDP” on page 19.
3. Make sure that SSO is enabled. Then select the IDP that you want to use and click **Use**.

Removing an IDP

To remove an IDP

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. Select the IDP that you want to remove and click **Remove**.

Note: If you have more than one IDP, you cannot remove the one that is in use unless you remove the others first. If you have only one IDP or have already removed the others, you must disable SSO before you can remove it. See the section called “Enabling or disabling SSO” on page 19.

Importing single sign-on (SSO) users

Use the following procedure to import single sign-on (SSO) users.

To import SSO users

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. If you have not done so already, add the SSO identity provider (IDP). See the section called “Adding an IDP” on page 19.
3. On the left, click the **User management** icon.
4. Click **Add user > Import single sign-on users**.
5. Select **User** or **User group**.
6. Depending on your selection, enter the username or the group name. Do not include the domain name.
7. Click **Import**.

After you have imported the user or the user group, you can view the details on the **User management** page.

Note: You cannot view the members of a user group from the Flex Appliance Console. Use the IDP to manage the users within a group.

Managing user authentication with smart cards or digital certificates

You can use smart cards or certificates for user validation with a remote user domain. This authentication method is not available for local users.

Prerequisites

Note the following prerequisites for smart card authentication:

- DNS must be configured on the appliance.
- The remote users who are associated with the smart cards or digital certificates must be imported to the appliance.
- Veritas recommends that the appliance date and time are set using NTP.

Configuring or editing smart card authentication

Follow these steps to configure user authentication with smart cards or digital certificates or to edit an existing configuration.

To configure or edit smart card authentication

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Smart card authentication**.
2. Click **Configure** or **Edit**.
3. Select a certificate mapping attribute and optionally enter the OCSP URI. If you do not provide the OCSP URI, the URI in the certificate is used.

4 Browse for or drag and drop the CA certificates that are associated with the user smart cards or the user digital certificates. Certificate file types must be in `.pem` format and less than 1,000 KB in size.

   To remove a certificate, click the **x** next to the file name. If the certificate is part of a certificate chain, make sure that you also remove the other certificates in the chain.

   Note: If you use Mozilla Firefox, you must also remove the certificate from the browser's certificate manager. See the browser documentation for instructions.

5 Click **Save**.

6 Open a new session to the Flex Appliance Console. The sign-in page should now display an option to sign in with a certificate or smart card.

7 Before a user can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager. See the browser documentation for instructions.

8 Once a user inserts a smart card or uploads a certificate, they are prompted to select and authenticate the certificate when they open a new session to the Flex Appliance Console. Once they do so, they can use the certificate to sign in.

   If the user does not select and authenticate the certificate when prompted, they can still sign in with their username and password.

Disabling or enabling smart card authentication

Follow these steps to disable user authentication with smart cards or digital certificates or to enable it after it has been disabled.

To disable or enable smart card authentication

1 Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Smart card authentication**.

2 Click **Disable** or **Enable**.

If you disable smart card authentication, users no longer see an option to sign in with a certificate or smart card.

About lockdown mode

Flex Appliance lockdown mode offers additional security levels to protect your appliance and data, in addition to the hardened, secure operating environment that comes out of the box.

Lockdown mode provides the following benefits:

- It prevents unauthorized access or modification to the underlying operating system (OS). Once lockdown mode is enabled, administrators cannot make changes to the OS or the internal components.
  If you need access to the OS for emergency operations, you must contact Veritas Technical Support to obtain a One-Time Password and temporarily unlock the appliance. This functionality prevents unauthorized changes even if a malicious actor gained access to stolen credentials.
- It includes the option to create WORM storage instances that prevent your data from being encrypted, modified, or deleted. WORM is the acronym for Write Once Read Many. Any data that is saved on these instances is protected with the following security measures:
  - Immutability
    This protection ensures that the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.
  - Indelibility
    This property protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

Flex Appliance includes the following lockdown modes:

- Normal mode
  This mode is the default mode of the appliance. Normal mode does not support WORM storage.
- Enterprise mode
  This mode adds additional access restrictions but retains a level of flexibility. In this mode:
  - You can create WORM storage instances and also delete them, including any existing data.
  - Any administrator can delete WORM storage instances if there is no immutable data. However, only the default **admin** user can delete them if immutable data is present.
  - When you delete a WORM storage instance as the default **admin** user, the instance can be running or stopped. When you delete a WORM instance as

any other user, the instance must be running so that the system can verify that there is no immutable data present.

- To change from enterprise mode to normal mode, you must first delete all WORM storage instances.

- Compliance mode
  This mode adds the highest level of access restrictions. In this mode:
  - You can create WORM storage instances. You can delete the instances only if there is no immutable data present.
  - Any administrator can delete WORM storage instances if there is no immutable data.
  - When you delete a WORM storage instance, the instance must be running so that the system can verify that there is no immutable data present.
  - To change from compliance mode to enterprise mode or normal mode, you must first wait for all data on the WORM storage instances to expire and then delete the instances.

In both enterprise mode and compliance mode, storage reset is disabled.

Veritas strongly recommends that you enable enterprise lockdown mode to prevent unauthorized access to the OS, even if you do not plan to create WORM storage instances.

Warning: Lockdown mode does not block access to the remote management (IPMI) port. Veritas recommends that you set up your network to restrict access and only allow security administrators or the users that manage the physical hardware to use the port.

The appliance must be in lockdown mode before you can create WORM storage instances. See “Changing the lockdown mode” on page 25.

For more information on creating and managing WORM storage instances, see the *NetBackup Application Guide for Flex Appliance*.

Changing the lockdown mode

You can use the Flex Appliance Console to change the lockdown mode on a Flex appliance. Note the following restrictions:

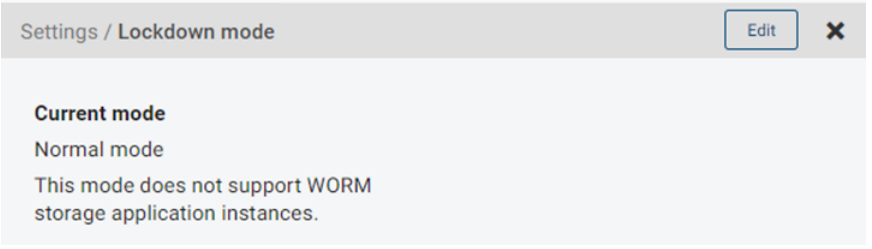
- Lockdown mode does not block access to the remote management (IPMI) port. Veritas recommends that you set up your network to restrict access and only allow security administrators or the users that manage the physical hardware to use the port.

- Only the default **admin** user can change the lockdown mode.
- To change from enterprise mode to normal mode, you must first delete all WORM storage instances.
- To change from compliance mode to enterprise mode or normal mode, you must first expire all data on the WORM storage instances, and then delete the instances.

Note: If you have a multi-node appliance, make sure that all nodes are configured before you enable lockdown mode.

To change the lockdown mode

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Lockdown mode**.



2. On the **Lockdown mode** page, click **Edit**.
3. Select the mode that you want to enable and click **Save**.

Using network access control

You can use the network access control feature to control which IP addresses are allowed to access the appliance. Use HTTPS access control to control which IP addresses can access the Flex Appliance Console or the APIs through HTTPS. Use SSH access control to control which IP addresses can access the Flex Appliance Shell through SSH.

To configure or edit network access control

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Depending on which service you want to configure, click **Configure** or **Edit** under **HTTPS access control** or **SSH access control**.
3. Follow the prompts to add the IP addresses or subnets that you want to have access to the appliance. Any IP addresses that are not included in the allowed list cannot access the appliance.

   Note the following information:

   - The IP protocol of the addresses in the allowed list must match the protocol of the appliance.
   - Subnets must be entered in CIDR notation. For example, 1.1.1.0/24.
   - If you use the Dynamic Host Configuration Protocol (DHCP), add subnets instead of IP addresses.
   - For HTTPS access control, you must include your current IP address in the allowed list. It can be entered by itself or as part of a subnet.
   - For SSH access control, you can leave the allowed list empty to block all SSH access.

To disable or enable network access control

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Depending on which service you want to disable or enable, click **Edit** under **HTTPS access control** or **SSH access control**.
3. Deselect or select the check box next to **Enable HTTPS access control** or **Enable SSH access control**.

Using an external certificate

By default, the appliance uses a Flex Appliance self-signed certificate for host communication. You can configure the appliance to use an external certificate instead.

Importing an external certificate

To use an external certificate, you must have the following:

- Host certificate: An X.509 certificate for the appliance, in PEM format. This certificate is different from the certificate for your NetBackup primary and media servers.
- Private key: The PKCS #8 private key of the host certificate.
- Passphrase: The passphrase of the private key if the key is encrypted.

To prevent errors while importing certificates, ensure that the external certificate files meet the following requirements.

- All certificate files must have a suffix of .pem or .cer and include `-----BEGIN CERTIFICATE-----` at the beginning of the certificate.
- All certificate files must contain the Flex Appliance Console FQDN in the common name or the subject alternative name (SAN) field of the certificate.
- The subject name and common name fields must not be left empty.
- Only ASCII 7 characters can be used in the subject and SAN fields of the certificate.
- The private key must be in the PKCS #8 PEM format, and it must begin with a header line of `-----BEGIN ENCRYPTED PRIVATE KEY-----`, `-----BEGIN PRIVATE KEY-----`, or `-----BEGIN RSA PRIVATE KEY-----`.
- Flex Appliance's web service uses the PKCS #12 standard and requires certificate files to be in the X.509 (.pem) format. If you obtained the certificate and private key in any other format you must first convert them to the X.509 (.pem) format.

To import an external certificate

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **External certificate**.
2. Upload the required files and click **Next**.
3. Confirm the details and click **Import**.

Removing an external certificate

Use the following procedure to remove an external certificate that you imported. Note that if you remove an external certificate, the appliance reverts to use the default Flex Appliance self-signed certificate for host communication.

To remove an external certificate

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **External certificate**.
2. Click **Remove**.

Forwarding logs

You can forward the appliance system logs (syslogs) and the audit logs to an external log management server. Your log management server must support the Rsyslog client.

Flex Appliance supports the following:

- TLS Anonymous Authentication for log forwarding
- X.509 file format for certificate files

To configure or edit log forwarding:

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Log forwarding**.
2. Click **Configure** or **Edit**.
3. Enter the log forwarding settings. If you want to secure the log transmissions from the appliance to the log server, select **Enable TLS log transmission** and upload the required certificate files. Veritas recommends that you enable TLS for security purposes.
4. When you are finished, click **Save**.

To stop forwarding logs

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Log forwarding**.
2. Click **Remove**.

Creating a NetBackup WORM storage server instance

NetBackup WORM (Write Once Read Many) storage server instances prevent your data from being encrypted, modified, or deleted. Any data that is saved on these instances is protected with the following security measures:

- Immutability
  This protection ensures that the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.
- Indelibility
  This property protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

See the *NetBackup Administrator's Guide, Volume I* for more information about WORM storage.

Use the following procedure to create a NetBackup WORM storage server instance on Flex Appliance.

Note: Your appliance must be in lockdown mode before you can create a WORM storage instance.

See the topic "Changing the lockdown mode" in the *Flex Appliance Getting Started and Administration Guide* for the steps to enable lockdown mode.

To create a NetBackup WORM storage server instance

1. Make sure that the NetBackup WORM storage server application you want to use is located in the repository.
2. Perform the following tasks if you have not already:
   - Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
   - Add at least one tenant.
   - Verify that the appliance is in lockdown mode. You can check or change the lockdown mode from the **Lockdown mode** page on the Flex Appliance Console. See the topic "Changing the lockdown mode" in the *Flex Appliance Getting Started and Administration Guide* for details.
3. Gather the following information for the new instance:

   Note: The hostname and IP address must not be in use anywhere else in your domain.

   - Tenant that you want to assign it to
   - Hostname (maximum of 63 characters including the domain name)
   - IP address
   - Network interface
   - Domain name
   - Name servers
   - Search domains
   - Primary server hostname (must be version 8.3.0.1 or later)
   - Media server hostname if applicable (must be version 8.3.0.1 or later)
   - Username for storage

NetBackup requires this username to connect to the deduplication storage. The username must be between 4 and 30 characters and can include uppercase letters, lowercase letters, and numbers.

- Password for storage
  NetBackup requires this password to connect to the deduplication storage. The password must be between 15 and 32 characters and must include at least one uppercase letter, one lowercase letter, one number, and one special character (_.+~={}?!).
- KMS key group
- KMS passphrase
- Certificate Authority (CA) information for one of the following:

  For a NetBackup CA:

  - CA SHA-1 or SHA-256 certificate fingerprint
    If the primary server is a Flex instance, you can locate this information from the instance details page of the primary server instance. Click on the instance name under **Application instances** on the **System topology** page.
    If the primary server is not a Flex instance, see the *NetBackup Security and Encryption Guide* for the steps to locate this information from NetBackup.
  - (Optional) Token for host ID-based certificate
    Depending on the primary server security level, the host may require an authorization or a reissue token. If you do not specify a token when you create the instance, the wizard attempts to automatically obtain the certificate.

  For an external CA:

  - Trust store, in PEM format
  - Host certificate, in PEM format
  - Private key, in PEM format
  - (Optional) Passphrase of the private key
    A passphrase is required if the key is encrypted.
- (Optional) Password for host name-based certificate
  A host name-based certificate is mandatory if Enhanced Auditing is enabled on the primary server. You can specify the password when you create the instance, or you can deploy the certificate from the primary server later.

4 On the primary server, use the `nbsetconfig` command or manually edit the NetBackup backup configuration file (`bp.conf` on Linux and UNIX, or the Windows registry) to add the following entry:

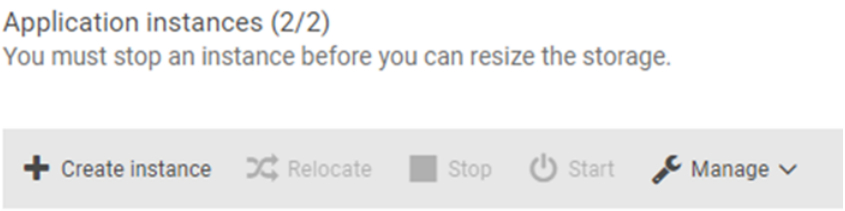
`MSDP_SERVER=<MSDP hostname>`

Where *<MSDP hostname>* is the hostname of the new WORM storage server instance.

5 If a firewall exists between the primary server and the new instance, open the following ports on the primary server to allow communication:

- `vnetd: 13724`
- `bprd: 13720`
- `PBX: 1556`
- If the primary server is a NetBackup appliance that uses TCP, open the following ports:
  443, 5900, and 7578.

6 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.



7 Click **Create instance**.

8 Select the appropriate storage server application from the repository list that appears, making sure to verify the version number. Click **Next**.

9 Follow the prompts to create the instance. When you are done, you can view the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

Note: If you use DNS and the DNS server includes both IPv4 and IPv6 addresses, the instance must be configured with both as well.

If you do not want to use DNS or want to bypass DNS for certain hosts, verify that the hostname resolution information is included in the **Hosts file entries** field. You must include entries for the primary server and any other NetBackup hosts that you want to communicate with the instance.

---

10 Once the instance has been created successfully, you must change the password from the known default password. To change the password, open an SSH session to the instance and log in with the following credentials:

- Username: **msdpadm**
- Password: **P@ssw0rd**

Follow the prompt to enter a new password. When the password change is complete, you are logged out. You can log back in with the new password.

11 If you plan to create or already have multiple instances with deduplication storage, Veritas recommends that you tune the `MaxCacheSize` according to the following guidelines:

- On each instance, allocate .75 GB to 1 GB of RAM for each TiB of storage that is allocated to deduplication on the instance. For example, if the storage pool has 80 TiB allocated, the `MaxCacheSize` should be 60 GB to 80 GB of RAM.
- The sum of the `MaxCacheSize` for all instances with deduplication storage should not exceed 70% of the physical RAM on the appliance.

To tune the deduplication `MaxCacheSize` on this instance:

- From the SSH session, run the following command on the instance:
  `setting set-MSDP-param max-fp-cache-size value=<percent%>`
  Where *<percent%>* is the percentage of the appliance RAM to use for the cache on the instance.
- Restart the `dedupe` process with the following commands:
  `dedupe MSDP stop`
  `dedupe MSDP start`

12 The appliance automatically creates a **PureDisk** storage server for the WORM storage instance that has the same name as the instance. Use the following steps to create a disk pool on that storage server:

   From the NetBackup web UI, click **Storage**, click the **Disk pools** tab, and then click **Add**. Follow the prompts to configure the disk pool.

13 Use the following steps to create a deduplication storage unit for your instance:

   From the NetBackup web UI, click **Storage**, navigate to the **Storage Units** tab, and then click **Add**. Follow the prompts and make sure that the **Enable WORM** option is activated.

You are ready to create a backup policy and start using your WORM storage instance. See the NetBackup documentation for more information.

Configuring an isolated recovery environment on a WORM storage server

You can configure an isolated recovery environment (IRE) on a WORM storage server to create an air gap between your production environment and a copy of the protected data. The air gap restricts network access to the data except during the timeframe when data replication occurs. This feature helps to protect against ransomware and malware.

To configure an IRE, you need a production NetBackup environment and a target Flex Appliance with a WORM storage server instance.

The production environment does not require any additional steps for this feature. Use the following procedure to configure an IRE on the target WORM storage server from the deduplication shell.

To configure an IRE

1 If Auto Image Replication (AIR) is not configured on the production domain, continue to the next step.

   If AIR is already configured on the production domain, log in to the deduplication shell as the **msdpadm** user. Run the following command to show the SLP windows for replication from the primary server to the WORM server.

   ```
   setting ire-network-control show-slp-windows
   production_primary_server=<production domain>
   production_primary_server_username=<production username>
   ire_primary_server=<IRE domain> ire_primary_server_username=<IRE
   username>
   ```

   Where:

- *<production domain>* is the fully qualified domain name (FQDN) of the primary server in your production environment.
- *<production username>* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.
- *<IRE domain>* is the FQDN of the primary server in the IRE. Use the same hostname that you used for the target primary server when you configured the SLPs in the production environment.
- *<IRE username>* is the username of a NetBackup user with permission to list SLPs and storage units in the IRE. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.

For example:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

The following is an example output of the command:

```
EveryDayAtNoon:
SLPs: SLP1
Sunday start: 12:00:00 duration: 00:59:59
Monday start: 12:00:00 duration: 00:59:59
Tuesday start: 12:00:00 duration: 00:59:59
Wednesday start: 12:00:00 duration: 00:59:59
Thursday start: 12:00:00 duration: 00:59:59
Friday start: 12:00:00 duration: 00:59:59
Saturday start: 12:00:00 duration: 00:59:59

WeeklyWindow:
SLPs: SLP2
Sunday start: 10:00:00 duration: 01:59:59
Monday NONE
Tuesday NONE
Wednesday NONE
Thursday NONE
Friday NONE
Saturday start: 10:00:00 duration: 01:59:59
```

This example shows two SLP windows:

- A daily window for one hour starting at noon.
- A weekly window for two hours starting at 10:00 A.M.

2 Based on the requirements for your environment, determine a schedule and take note of it. For an existing AIR environment, the schedule must accommodate the SLP windows that you viewed in the previous step.

You can set a daily schedule that is open at the same time each day, or you can set a different schedule for each day of the week.

In the previous example, you can accommodate both SLP windows with either of the following:

- A daily schedule from 10:00 A.M. to 1:00 P.M.
- A schedule from 12:00 P.M. to 1:00 P.M. on Monday through Friday and a schedule from 10:00 A.M. to 1:00 P.M. on Saturday and Sunday

---

Note: If the production environment and the IRE are in different time zones, the schedule must begin only once per day in both time zones. For example, if one environment is in the Asia/Kolkata time zone and the other is in the America/New_York time zone, the following schedule in Kolkata is not supported: Tuesday start time 22:00:00 and Wednesday start time 03:00:00. When these start times get converted to the New York time zone, they become Tuesday start time 12:30:00 and Tuesday start time 17:30:00, which is not supported.

---

3 Run the following command to configure which subnets and IP addresses are allowed to access the WORM storage server:

```
setting ire-network-control allow-subnets subnets=<CIDR subnets
or IP addresses>
```

Where <*CIDR subnets or IP addresses*> is a comma-separated list of the allowed IP addresses and subnets, in CIDR notation.

For example:

```
setting ire-network-control allow-subnets
subnets=10.80.120.208,10.84.48.0/20
```

Note: The IRE primary server, the IRE media servers, and the DNS server for the IRE must be included in the allowed list. If all of these servers are in the same subnet, only the subnet is required to be in the allowed list. If you have a dual stack IPv4-IPv6 network, make sure that you add both the IPv4 and the IPv6 addresses to the allowed list.

---

4 Run the following command to set the daily air gap schedule:

```
setting ire-network-control set-schedule start_time=<time>
duration=<duration> [weekday=<0-6>]
```

Where [weekday=<*0-6*>] is an optional parameter to indicate the day if you need to set different schedules for different days. 0 is Sunday, 1 is Monday, etc.

For example:

```
setting ire-network-control set-schedule start_time=10:00:00
duration=03:00:00 weekday=0
```

5 Before you can send data between the production domain and the IRE storage server, you must add MSDP reverse connections and add the replication operation. See "Configuring data transmission between a production environment and an IRE WORM storage server" on page 37.

Configuring data transmission between a production environment and an IRE WORM storage server

Once the configuration of an isolated recovery environment (IRE) is completed, the production NetBackup hosts are no longer able to access the WORM storage server. You need to add MSDP reverse connections to allow data transmission between the production MSDP storage server and the IRE WORM storage server. Then you can add the replication operation.

To configure data transmission between a production environment and an IRE

1 Open an SSH session to the IRE WORM storage server. Run the following command to determine if the external network is open:

```
setting ire-network-control external-network-status
```

If it is not, run the following command:

```
setting ire-network-control external-network-open
```

2 Depending on the type of certificate authority that you use for host communication, do one of the following:

- If you use a NetBackup Certificate Authority, run the following commands to request the certificates from the production domain:

  ```
  setting certificate get-CA-certificate
  primary_server=<production primary server>
  setting certificate get-certificate primary_server=<production
  primary server> token=<token>
  ```

- If you use an external certificate authority, run the following commands to enroll the certificates with the production domain:

  ```
  setting certificate enroll-external-certificates
  server=<production primary server>
  ```

3 Run the following command to add an MSDP reverse connection:

```
setting ire-network-control add-reverse-connection
remote_storage_server=<production MSDP server>
[remote_primary_server=<production primary server>]
[local_storage_server=<IRE network interface>]
```

Where:

- *<production MSDP server>* is the fully qualified domain name (FQDN) of the MSDP server in your production environment.
- [remote_primary_server=*<production primary server>*] is an optional parameter for the FQDN of the primary server in your production environment. This parameter is required if the IRE domain uses an alternative name to access the production primary server. This scenario usually occurs if the production primary server runs on multiple networks with multiple hostnames.
- [local_storage_server=*<IRE network interface>*] is an optional parameter for the hostname of the network interface to use for image replication on the IRE storage server. This parameter is required if the network interface for replication is different than the IRE storage server name.

4 If necessary, repeat the previous step to add additional MSDP reverse connections.

5 If Auto Image Replication (AIR) is not already configured on the production domain, run the following command to copy the IRE schedule to the production domain as a storage lifecycle policy (SLP) window:

```
setting ire-network-control sync-ire-window
production_primary_server=<production primary server>
production_primary_server_username=<production username>
[slp_window_name=<SLP window name>]
```

Where:

- *<production primary server>* is the FQDN of the primary server in your production environment.
- *<production username>* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment.

For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.

- [slp_window_name=<*SLP window name*>] is an optional parameter to give a name for the SLP window. If you do not provide this parameter, the name of the SLP window is `IRE_DEFAULT_WINDOW`.

6 If you do not have them already, create a source SLP on the production primary server and a target import SLP on the IRE primary server. See the section "Creating a storage lifecycle policy" in the *NetBackup Deduplication Guide* for details.

Note: You cannot add the replication operation from NetBackup when you create the SLPs. Continue to the next step to add the replication operation.

---

7 Run the following command to add the IRE WORM storage server as a replication target of the production NetBackup domain and to add the replication operation to the SLP:

```
setting ire-network-control add-replication-op
production_primary_server=<production primary server>
production_primary_server_username=<production username>
production_storage_server=<production storage server>
ire_primary_server_username=<IRE username>
source_slp_name=<production SLP name> target_import_slp_name=<IRE
SLP name> target_storage_server=<target storage server>
target_storage_server_username=<target storage server username>
production_storage_unit=<MSDP storage unit> [slp_window_name=<slp
window name>]
```

Where:

- *<production primary server>* is the FQDN of the primary server in your production environment.
- *<production username>* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.
- *<production storage server>* is the FQDN of the production storage server in your production environment.
- *<IRE username>* is the username for an administrator on the IRE primary server. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.

- *<source SLP name>* is the SLP name from the production primary server to add the replication operation to.
- *<target SLP name>* is the import SLP name from the IRE primary server.
- *<target storage server>* is the FQDN of the target WORM storage server in your IRE environment.
- *<target storage server username>* is the username for an administrator on the target WORM storage server.
- *<MSDP storage unit>* is the name of the MSDP storage unit that is the replication source in the source SLP.
- [slp_window_name=*<slp window name>*] is an optional parameter for the name of the SLP window that is synced with the IRE schedule. This parameter must match the SLP window name from the previous step, if applicable. If you do not provide this parameter, the default name is used.

8 If you opened the external network at the beginning of this procedure, run the following command to close it and resume the air gap schedule:

```
setting ire-network-control resume-schedule
```

Protecting the NetBackup catalog on a WORM storage server

By default, WORM storage servers store a copy of the NetBackup catalog in the directory `/mnt/msdp/vol0` in addition to the original copy that is available under the dedicated catalog volume (`/mnt/msdpcat`).

If you want extra protection for the catalog, you can configure additional copies. Use the following procedures to manage the NetBackup catalog copies from the deduplication shell.

To view the catalog copies

1 Open an SSH session to the server.

2 Run the following command:

```
cacontrol --catalog listshadowcopies
```

To configure an additional copy

1. Open an SSH session to the server.
2. Run the following command to determine which volumes exist in the `/mnt/msdp` directory:

   ```
   df -h
   ```

   Select one of the volumes other than vol0.

   Note: To configure an additional catalog copy, at least one volume other than vol0 must exist in the `/mnt/msdp` directory.

3. Run the following command:

   ```
   cacontrol --catalog addshadowcopy /mnt/msdp/<volume name>
   ```

   Where *<volume name>* is the volume that you chose in the previous step.

   For example:

   ```
   cacontrol --catalog addshadowcopy /mnt/msdp/vol1
   ```

Using a sign-in banner

You can set a text banner that appears before a user signs in to the Flex Appliance Console and the Flex Appliance Shell. Typical uses for the login banner include legal notices, warning messages, and company policy information.

To add or edit a sign-in banner

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Sign-in banner**.
2. Click **Add** or **Edit**.
3. Enter the sign-in banner details. You can click **Preview** to see how it appears in the console. When you are finished, click **Save**.

To remove a sign-in banner

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Sign-in banner**.
2. Click **Remove**.

Chapter 3

Steps to protect NetBackup Appliance

This chapter includes the following topics:

About NetBackup Appliance hardening

This chapter contains information on the NetBackup Appliance features that can help to secure your data protection infrastructure. For more detailed information about NetBackup Appliance security, see the *NetBackup Appliance Security Guide*.

About single sign-on (SSO) authentication and authorization

You can configure SSO with a supported external identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Veritas product. For example, the same IDP can be configured with NetBackup and with APTARE.

Note the following requirements and limitations:

- You must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported. ADFS (Active Directory Federation Services) is currently the only supported IDP for the NetBackup Appliance.
- IDP configuration is managed by using the `Main > Settings > Security > Authentication > SingleSignOn` command. You can configure only one IDP for SSO.
- SAML users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with SAML-authenticated users.
- SSO login is currently supported only to the NetBackup Appliance Web Console (web console).
- Global logout is not supported.

SSO configuration is supported from the NetBackup Appliance Shell Menu (shell menu). The following describes an overview on how to configure and enable SSO for an appliance.

Table 3-1 Process overview for SSO configuration

Step	Task	Description
1	Obtain the IDP metadata XML file.	The SAML metadata that is stored in XML files is used to share configuration information between the IDP and the appliance. The IDP metadata XML file is used to add the IDP configuration to the appliance. The following options are available: ■ Download the IDP metadata XML file from the service provider and upload it to the general share on the appliance. ■ Provide the URL address of the IDP metadata XML file for the appliance to download.
2	Configure SSO on the appliance.	Configure the appliance for SSO from the following shell menu view: `Main > Settings > Security > Authentication > SingleSignOn`
3	Authorize SSO users and user groups.	Configure appliance access for SSO users and user groups from the following shell menu view: `Main > Settings > Security > Authorization` You can grant administrator or AMS privileges to SSO users and user groups.

To perform the complete SSO configuration process, see the following topic:

See "Configure single sign-on (SSO) for a NetBackup Appliance" on page 44.

Configure single sign-on (SSO) for a NetBackup Appliance

The following procedure describes the complete process to configure an appliance for SSO.

To configure SSO on an appliance

1. Obtain the identity provider (IDP) metadata XML file by using one of the following methods:
   - Download
     Download and save the IDP metadata XML file from the IDP website. Then log in to the NetBackup Appliance Shell Menu (shell menu) and upload the file to the appliance by opening the general share as follows:

- Log in to the NetBackup Appliance Shell Menu (shell menu) and upload the file to the appliance by opening the general share as follows:
  `Settings > Share > General Open`

  Note: You can also upload the file into the general share directory from the **File Manager** tab in the NetBackup Appliance Web Console.

- URL
  Obtain the URL address of the IDP metadata XML file for the appliance to download. Make sure that it is a valid https address.

2 Configure SSO on the appliance as follows:

Note: You can configure only one IDP for SSO.

- Run the following command to add an IDP configuration to the appliance:
  `Settings > Security > Authentication > SingleSignOn Add`
- `idpname` - enter the name that you want to use for this IDP configuration.
- `metadata` - select how to associate the necessary metadata for the IDP configuration, as follows:
  Import: Import the IDP XML metadata file that you uploaded into the general share directory in the first step.
  URL: Enter the URL address of the IDP XML metadata file for the appliance to retrieve.
- *`userFieldName [userPrincipalName]`*
  `groupFieldName [memberOf]`
  These parameters are optional and are shown with their default values. You can change the default values as needed to retrieve the appropriate SAML assertion details.

After you have completed this step, the configuration is enabled by default.

3 Add authorized SSO user groups and users by running the `Settings > Security > Authorization` command. Use the following command options to authorize specific SSO user groups and users:

`Grant Administrator SSO_Groups` *`groups`*

`Grant Administrator SSO_Users` *`users`*

`Grant AMS SSO_Groups` *`groups`*

`Grant AMS SSO_Users` *`users`*

About authentication using smart cards and digital certificates

The following describes the supported interfaces for Smart Card Authentication.

2FA

Starting with appliance release 3.2, NetBackup supports two-factor authentication (2FA) for Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Web UI.

Starting with appliance release 5.0, NetBackup appliances support two-factor authentication (2FA) for Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Appliance Web UI.

2FA for NetBackup Web UI

- The **nbasecadmin** user or any user with the NetBackup Adminstrator role can configure 2FA for the NetBackup Web UI.
- 2FA configuration requires separate AD or LDAP configuration for NetBackup, even if AD or LDAP is already configured on the appliance.

2FA for NetBackup Appliance Web UI

Any user with the NetBackup Appliance administrator role can configure 2FA for the NetBackup Appliance Web UI. 2FA configuration requires configuring LDAP (with the directory type as OpenLDAP or ActiveDirectory) on the appliance.

For details about how to configure, enable or disable 2FA for the Appliance Web UI, see the following topic:

See “Smart card authentication for NetBackup Appliance Web UI” on page 48.

Smart card Authentication for NetBackup Web UI

The NetBackup Web UI supports authentication of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with a digital certificate or smart card, including CAC and PIV. This authentication method only supports one AD or LDAP domain for each appliance primary server domain and is not available for local domain users.

Note: Perform this configuration separately for each appliance primary server domain where you want to use this authentication method.

Ensure that you add the AD or the LDAP domain before you add access rules for domain users or configure the domain for smart card authentication. Use the `vssat` command to add AD or LDAP domains.

To add the AD or the LDAP domain for NetBackup

1. Log on to the appliance primary server as a NetBackupCLI user.
2. Run the `vssat` command.

   `vssat addldapdomain -d` *`DomainName`* `-s` *`server_URL`* `-u` *`user_base_DN`* `-g` *`group_base_DN`* `-t` *`schema_type`* `-m` *`admin_user_DN`*

   Replace the variables in the above command as per the following descriptions:

   - *`DomainName`* is a symbolic name that uniquely identifies an LDAP domain.
   - *`server_URL`* is the URL of the LDAP directory server for the given domain. The LDAP server URL must start with either `ldap://` or `ldaps://`. Starting with `ldaps://` indicates that the given LDAP server requires SSL connection. For example `ldaps://my-server.myorg.com:636`.
   - *`user_base_DN`* is the LDAP-distinguished name for the user container. For example, `ou=user,dc=mydomain,dc=myenterprise,dc=com`.
   - *`group_base_DN`* is the LDAP-distinguished name for the group container. For `example, ou=group,dc=mydomain,dc=myenterprise,dc=com`.
   - *`schema_type`* specifies which type of LDAP schema to use. The two default schema types that are supported are `rfc2307` or `msad`.
   - *`admin_user_DN`* is a string that contains the DN of the administrative user or any user that has search permission to the user container, or user subtree as specified by `UserBaseDN`. If the user container is searchable by anyone including an anonymous user, you can configure this option as an empty string. For example, `--admin_user=`. This configuration allows anyone to search the user container.
3. Verify that the specified AD or LDAP domain was successfully added using `vssat validateprpl`. Note that you can also use the `vssat` command with the following options:
   - `vssat removeldapdomain` removes an LDAP domain from the authentication broker.
   - `vssat validategroup` checks the existence of a user group in domain provided.
   - `vssat validateprpl` checks the existence of a user in domain provided.

For more details on the `vssat` command, see the *Veritas NetBackup Commands Reference Guide*

Smart card authentication for NetBackup Appliance Web UI

Ensure that you perform the following three steps before you perform authentication for the Appliance Web UI.

Note: You can perform the steps in any order.

---

1. Configure LDAP authentication with the directory type as OpenLDAP or ActiveDirectory.

   Settings > Security > Authentication > LDAP

2. Add and grant roles to LDAP users who will be authenticated by the appliance.

   Settings > Security > Authentication > LDAP > Users Add

   Settings > Security > Authorization > Grant

3. Add all the certificates in the CA chain to the appliance. Intermediate certificates on the card do not have to be added.

   Settings > Security > Certificates > AddCACertificate

The smart card command menu allows you to configure and display parameters related to the Appliance Web UI smart card authentication. You can also enable or disable this feature.

Settings > Security > Authentication > SmartCard

Table 3-2 Smart card menu commands

Command	Description
`Configure MappingAttribute`	The `Configure` command configures the appliance smart card authentication. It has one required and one optional configuration parameter. The `MappingAttribute` parameter specifies if the Common Name (CN) or the User Principal Name (UPN) of the certificate on the smart card is used to authenticate a user and determine that user's role. Enter CN or UPN. It is a required parameter. CN can be used if the CN in the certificates matches the CN field of the user records in the remote databases, OpenLDAP or ActiveDirectory. UPN can be used if the UPN in the certificates matches the UPN field of the user records in OpenLDAP or ActiveDirectory. When LDAP is, configured the `directoryType` is specified as OpenLDAP or ActiveDirectory.
`Configure OCSPURI`	The `OCSPURI` parameter (Online Certificate Status Protocol) determines if the certificate on the smart card has been revoked. It is an optional parameter. If present, this parameter overrides the OCSP URI present in the certificate. The URI is an FQDN or IPv4 address. An IPv6 address is not supported for the OCSP URI. **Note:** If authentication with smart card fails even after all the necessary steps have been performed, use the **SmartCard > Show** command and verify that the parameters, including the OCSP URI, if present, are correct. Verify that a name server which can resolve the OCSP URI is configured in the Network menu by navigating to **Network > DNS Show**
`Disable`	Disables smart card authentication.
`Enable`	Enables smart card authentication. You can enable smart card authentication only if LDAP has been configured, CA certificates have been added and smart card authentication has been configured.
`Show`	Displays a table which shows if smart card authentication is enabled, the selected mapping attribute, and the OCSP URI, if one was entered.

Smart card authentication for NetBackup Appliance Shell Menu

This topic provides the following information to configure smart card authentication for the NetBackup Appliance Shell Menu (shell menu):

- Order of steps
- Smart card SSH menu commands

Order of steps

1. Enable smart card authentication for SSH. You must first enable the feature before you can add the public key (step 3).
2. Configure the mapping attribute to determine which field in the remote database is used to search for the public key.
3. Add the public key for a local user. You can use either a public key file or a certificate file method.
4. (Optional) Choose to enable or disable password authentication for SSH login.

Table 3-3 Smart card SSH menu commands

Command	Description

`Configure MappingAttribute CN/UPN`
 	
`Configure PublicKey Add filetype <username>`
 	
`Configure PublicKey Remove <username>`
	The `Configure` command configures the appliance smart card authentication and is used to configure the following parameters:
	
	MappingAttribute is for either CN (Common Name) or UPN (User Principle Name). This attribute determines which of those fields in the remote database is used to search for the public key.
	
	`Configure PublicKey Add filetype <username>` adds a public key for a local user. Here, *filetype* is either `CertificateFile` or `PublickeyFile`. For `CertificateFile` configurations, copy and paste the certificate content directly. For `PublickeyFile` configurations, locate the public key in the certificate file and copy it, then paste it directly.
	
	Note: Before you can add a public key, you must first enable SSH smart card authentication with the `Enable` command described further below.
	
	`Configure PublicKey Remove <username>` removes a public key for a local user.

`Disable`	Disables smart card authentication for SSH user.
`Enable`	Enables smart card authentication for SSH users. If all the prerequisites for DNS and smart card configuration commands have been performed successfully, authentication with smart cards is enabled. **Note:** Before you can add a public key, you must first run this command to enable SSH smart card authentication.
`PWauth`	Enables or disables password authentication for SSH login.
`Show`	Shows the values of the mapping attribute and status of the smart card authentication.

Configure role-based access control

After adding the AD and LDAP domains for NetBackup, you can use the `nbasecadmin` user to log on to the NetBackup Web UI and configure role-based access control for the NetBackup web UI. For more information about configuring RBAC for NetBackup Appliance users, see the *NetBackup Web UI Security Administrator's Guide*.

Configure authentication for a smart card or digital certificate for the NetBackup Web UI

You can use the `nbasecadmin` user to log on to the NetBackup Web UI and configure authentication for a smart card or digital certificate. Refer to the *NetBackup Web UI Security Administrator's Guide* for steps on performing the following procedures required for the configuration:

- Configure NetBackup Web UI to authenticate users with a smart card or digital certificate.
- Edit the configuration for smart card authentication.
- Add a CA certificate that is used for smart card authentication.
- Delete a CA certificate that is used for smart card authentication.

Disable user access to the NetBackup appliance operating system

Depending on the security policies of your organization, you can choose to permanently disable user access to the NetBackup Appliance operating system (VxOS). You can disable user access to the VxOS by configuring its security level to `High`. Note that the following restrictions are permanently enforced in the appliance:

- Users cannot access the maintenance shell. The `Support > Maintenance` menu is not available in the shell menu.

Note: Only Veritas support personnel can be granted access to the maintenance shell to troubleshoot issues and manage operating system-related tasks.

To permanently disable user access to VxOS

1. To view the current security level of the VxOS, use the following command:

   ```
   Main_Menu > Settings > Security > SecurityLevel Show
   ```

   The VxOS can operate in either of the following security levels:

Security level	Description
`Optimal`	Access to VxOS is granted as per standard Veritas security policies. This is the default security configuration.
`High`	Access to VxOS is permanently disabled for all users.
`Maintenance`	Access to VxOS is temporarily granted to Veritas support personnel through the maintenance shell. The security level is automatically reverted to `High` after the maintenance activity is completed.

2. To permanently disable user access to VxOS, configure the security level to `High`. Use the following command:

   ```
   Main_Menu > Settings > Security > SecurityLevel High
   ```

   Note: After switching to the `High` security level, you cannot revert to the default (`Optimal`) security level unless you perform a factory reset of the appliance.

About Network Access Control

The Network Access Control feature lets you control which IP addresses (IPv4 or IPv6) are allowed to access the appliance. This feature is available through the NetBackup Appliance Shell Menu as follows:

```
Main > Settings > Security > NetworkAccessControl
```

The available command options are *AddIP*, *DeleteIP*, and *Show*.

Appliance access is allowed through HTTPS for the NetBackup Appliance Web Console or rest APIs, and through SSH for the shell menu. To permit access to a specific appliance, add the necessary client IP addresses to the allowed list for that appliance. Any client IP addresses that are not included in the allowed list cannot access the appliance. Any interface level restrictions are managed separately and are also appliance-specific.

For high availability (HA) setups, you must configure the `NetworkAccessControl` options on both appliance nodes and the configurations must match.

If your appliance is configured as an Appliance Management Server (AMS) or is an agent for an AMS, make sure that you add those IP addresses to the allowed list. The AMS must include the IP addresses of the agents, and the agents must include the IP address of the AMS.

For complete details, see the *NetBackup Appliance Commands Reference Guide*.

About data encryption

The NetBackup Appliance offers the following encryption methodologies to protect both data at rest and in flight:

- Transmits data in encrypted formats by using secure tunnels. These configurations can be made by client-side encryption and also replication. If these options are not used, once the data is transmitted from the appliance, the network infrastructure is used for securing data in flight.
- Starting with NetBackup Appliance version 3.0 (NetBackup version 8.0), MSDP provides AES encryption. If your environment uses encrypted MSDP, new incoming data gets encrypted with AES 128-bit (default) or AES 256-bit. For more information, see the following NetBackup documents:
  Veritas NetBackup Deduplication Guide
  Veritas NetBackup Security and Encryption Guide
- Supports encryption using NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. See "KMS support " on page 53.

KMS support

NetBackup Appliance supports encryption that is managed by NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. KMS is supported on primary and media server appliances. Regenerating the data encryption key is the only supported method of recovering KMS on an appliance primary server.

The following describes the KMS key features:

- Does not require an additional license.
- Is a primary server-based symmetric key management service.
- Can be administered as a primary server with tape devices connected to it or to another NetBackup Appliance.

- Manages symmetric cryptography keys for tape drives that conform to the T10 standard (such as LTO4 or LTO5).
- Designed to use volume pool-based tape encryption.
- Can be used with tape hardware that has built-in hardware encryption capability.
- Can be managed by a NetBackup CLI administrator using the NetBackup Appliance Shell Menu or the KMS Command Line Interface (CLI).

About the keys used under KMS

The KMS generates keys from passcodes or auto-generates keys. Table 3-4 lists the associated KMS files that hold the information about the keys.

Table 3-4 KMS files

KMS files	Description
Keystore file	The keystore file (`KMS_DATA`) contains all of the key group and key records, along with some metadata.
KPK file	The KPK file (`KMS_KPKF`) contains the KPK that is used to encrypt the ciphertext portions of the key records that are stored in the keystore file.
HMK file	The HMK file (`KMS_HMKF`) contains the HMK that is used to encrypt the entire contents of the keystore file. The keystore file header is an exception. It contains some metadata like the KPK ID and the HMK ID, which is not encrypted.

Configuring KMS

To configure KMS on an appliance primary server, you must log in as a NetBackupCLI user.

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbasecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on managing role-based access control, see the *NetBackup Web UI Administrator's Guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user,

---

The following describes how to configure and enable KMS on an appliance.

To configure and enable KMS on an appliance

1. Log in to the appliance primary server as a NetBackupCLI user.
2. Enter into a restricted shell environment by using the `Command` command as follows:

   ```
   [nb-appliance.NBCLIUSER>]# Command
   ```

3. Authenticate your CLI access using the following steps:

   - Generate an access code by running the following command:

     ```
     #bpnbat -login -logintype webui -requestApproval
     ```

     Make a note of the access code that is displayed in the command window.
   - Sign in to the NetBackup web UI as a NetBackup Command Line (CLI) Admin user and approve the CLI access request by entering the access code that you generated earlier.
     Once the request is approved, you will see a confirmation message in the restricted shell command window.

   For more information about access key and approval requests, refer to the *NetBackup Security and Encryption Guide*.
4. Create an empty database using the `nbkms` command, as follows:

   ```
   [nbucliuser-!>]# nbkms -createemptydb
   ```

5. Start `nbkms`. For example:

   ```
   [nbucliuser-!>]# nbkms
   ```

6. Create a Key group. For example:

   ```
   [nbucliuser-!>]# nbkmsutil -createkg -kgname KMSKeyGroupName
   ```

7. Create an active key. For example:

   ```
   [nbucliuser-!>]# nbkmsutil -createkey -kgname KMSKeyGroupName
   -keyname KMS KeyName
   ```

Enabling KMS encryption for MSDP

Verify that KMS is configured and running on the primary server. You can then enable KMS encryption for MSDP on all of the media servers that are associated with the primary server.

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbasecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on how to manage role-based access control, see the *NetBackup Web UI Administrator's guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user,

---

The following describes how to enable KMS encryption for MSDP on an appliance.

To enable KMS encryption for MSDP

1. Log in to the appliance media server as a NetBackupCLI user.
2. Change the following options in the order as shown:

   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSType --value=0`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSServerName --value=<primary server hostname`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSKeyGroupName --value=msdp`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KeyName --value=<KMS KeyName>`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSEnable --value=true`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=ContentRouter --option=ServerOptions --value=verify_so_references,fast,encrypt`

     Repeat this step on all media servers that are associated with the primary server.

3 Identify yourself to the system by logging on to the NetBackup web application. Run the following command:

```
sudo /usr/openv/netbackup/bin/bpnbat -login -loginType WEB

Authentication Broker: ApplianceHostname

Authentication Port: 0

Authentication Type: unixpwd

LoginName: Username

Password: Password
```

4 Ensure that the KMS is registered with NetBackup Web Service.

```
sudo /usr/openv/netbackup/bin/nbkmscmd -discoverNbkms
```

5 Stop and restart the NetBackup services with the following commands:

- `bp.kill_all`
- `bp.start_all`

6 To verify that KMS encryption for MSDP is enabled on the media server, run a backup job on the server, then run the following command:

```
crcontrol --getmode
```

FIPS 140-2 conformance for NetBackup Appliance

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for validating cryptography modules. The FIPS 140-2 standard specifies the security requirements for cryptographic modules and applies to both the hardware and the software components. It also describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

Note: For more information about the FIPS 140-2 standard and its validation program, click on the following links:

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

---

FIPS validation for Java

Starting with NetBackup Appliance 4.1, the FIPS 140-2 standard is enabled by default for all Java-based services. The FIPS validation is achieved by using SafeLogic's CryptoComply modules.

FIPS validation for MSDP, NetBackup and VxOS

Starting with NetBackup Appliance release 5.0, you can enable the FIPS 140-2 standard for MSDP, NetBackup and VxOS. The NetBackup Cryptographic Module, which is used by MSDP, NetBackup and VxOS, is FIPS validated.

Once FIPS for VxOS is enabled, the `sshd` uses the following FIPS approved ciphers:

- aes256-ctr
- aes256-gcm@openssh.com

Older SSH Clients are likely to prevent access to the appliance after FIPS for VxOS is enabled. Check to make sure that your SSH client supports the listed ciphers, and upgrade to the latest version if necessary. Default cipher settings are not typically FIPS-compliant, which means you may need to select them manually in your SSH client configuration.

You can enable the FIPS 140-2 standard for NetBackup MSDP, NetBackup and VxOS with the following commands:

- `Main Menu > Settings > Security > FIPS Enable MSDP`, followed by the maintenance password.
  Enabling or disabling the `MSDP` option terminates all jobs that are currently in progress and restarts the NetBackup services. As a best practice, it is recommended that you first stop all jobs manually before you enable or disable this feature.

  Note: If you have upgraded from a previous version of NetBackup Appliance, ensure that you enable MSDP only after your existing data has been converted to use FIPS compliant algorithms. To check the current status of the data conversion use the `crcontrol --dataconvertstate` command. Enabling MSDP before the status is set to **Finished** can cause data restoration failures.

- `Main Menu > Settings > Security > FIPS Enable NetBackup`, followed by the maintenance password.
  Enabling or disabling the `NetBackup` option terminates all jobs that are currently in progress and restarts the NetBackup services. As a best practice, it is recommended that you first stop all jobs manually before you enable or disable this feature.

- `Main Menu > Settings > Security > FIPS Enable VxOS`, followed by the maintenance password.
  Enabling or disabling the `VxOS` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable or disable this feature.
- `Main Menu > Settings > Security > FIPS Enable All`, followed by the maintenance password.
  Enabling or disabling the `All` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable or disable this feature.

Note: In a NetBackup Appliance high availability (HA) setup, you can enable the FIPS feature on both nodes only after you have completed configuration of the HA setup. The FIPS configuration must match on both the nodes. If FIPS is enabled on either node before the HA setup is completed, you must disable FIPS on that node before you complete the HA setup.

For complete information about FIPS commands, see the *NetBackup Appliance Commands Reference Guide*.

Limitations of FIPS mode

As FIPS security continues to increase, some older encryption methods can no longer be used.

When FIPS is enabled, appliance CIFS file share features work as follows: The appliance is added as a domain member in Active Directory (AD) environments with Kerberos authentication that uses AES ciphers.

CIFS shares opened by the following operations may not mount when using older authentication methods, like NTLM.

The following describes the impacted scenarios:

- For the general share:

  ```
  Settings> Share General Open
  Settings> LogForwarding > Share Open
  Manage> OpenStorage > Share Open
  Security> Certificate Import
  ```

- For incoming_patches:

  ```
  Manage> Software > Share Open
  ```

To work around these limitations, do one of the following:

- Disable the FIPS feature.
- Configure Active Directory authentication on the appliance. This adds the appliance as a domain member in Active Directory (AD) environments with Kerberos authentication that uses AES ciphers.

https://www.veritas.com/support/en_US/article.100054201

About implementing external certificates

NetBackup Appliance's web service uses the PKCS#12 standard and requires certificate files to be in the X.509 (`.pem`) format. If the certificate files are in the `.der`, `.DER`, or `.p7b` formats, NetBackup Appliance automatically converts the files to an accepted format.

Certificate requirements

To prevent errors while importing certificates, ensure that the external certificate files meet the following requirements.

- Certificate files are in the `.pem` file format and begin with "`-----BEGIN CERTIFICATE-----`".
- Certificate files contain the host name and FQDN in the subject alternative name (SAN) field of the certificate. If the certificate is used in an HA environment, the SAN field must contain VIP, host name, and FQDN.
- Subject name and common name fields are not empty.
- Subject fields are unique for each host.
- Subject fields contain a maximum of 255 characters.
- Server and client authentication attributes are set in the certificate.
- Only ASCII 7 characters are used in the subject and SAN fields of the certificate.
- The private key file is in the PKCS#8 PEM format and begins with `-----BEGIN ENCRYPTED PRIVATE KEY-----` or `-----BEGIN PRIVATE KEY-----`.

Certificate Signing Request (CSR)

Although optional, you can use the `Settings > Security > Certificate > CertificateSigningRequest > Create` command to generate a CSR. Copy the CSR content from the command line to your external certificate portal to obtain the required external certificate files.

```
Example:
Enter specified value or use the default value.
Common Name (eg, your name or your server's hostname) [Default abc123]:
Organizational Unit Name (eg, section) []:Appliance
Organization Name (eg, company) [Default Company Ltd]:YourCompanyName
Locality Name (eg, city) [Default City]:YourCity
State or Province Name (full name) []:YourStateorProvince
Country Name (2 letter code) [XX]:YourCountryName
Email Address []:email@yourcompany.com
Please enter the following 'extra' attributes
to be sent with your certificate request.
-----
A challenge password []:123456
An optional company name []:ABCD
Subject Alternative Name (DNS Names and/or IP Addresses comma separated):
abc123,def456.yourcompany.com
Subject Alternative Name (email comma separated):
Certificate Signing Request Name [Default abc123.csr]:
Validity period (in days) [Default 365 days]:
Ensure that the Distinguished Name (DN) is specified as a string consisting
of a sequence of key=value pairs separated by a comma:
Then the generated certificate signing request will be shown on the screen.
```

Register the external certificate

Starting from version 4.1, you can register an external certificate on both NetBackup Appliance and NetBackup using the `Settings > Security > Certificate > Import` command.

Perform the following steps to import the host certificate, host private key, and trust store to register the external certificate on NetBackup and NetBackup Appliance. Both NetBackup and NetBackup Appliance layers use the same host certificate, host private key, and trust store.

1. Log in to the appliance as an Administrator user.
2. From the NetBackup Appliance Shell Menu, run the `Settings > Security > Certificate > Import` command. The following NFS and CFS share locations are now accessible:
   - NFS: `/inst/share`
   - CFS: `\\<ApplianceName>\general_share`
3. Upload the certificate file, trust store file, and private key file to either of the share locations and enter the paths to the files.

4 Choose how to access the certificate revocation list (CRL). A CRL comprises a list of external certificates that have been revoked by the external certificate and should not be trusted. Select either of the following options:

- Use the CRL location provided in the certificate file.
- Provide the location of a CRL file (`.crl`) in the local network.
- Do not use a CRL.

5 Confirm the location of the certificate files you want to register on the appliance.

A detailed example of how to import the certificates is provided here.

- Identify the certificate which should be imported.
- Import the certificate.

```
Enter the certificate:
Enter the following details for external certificate configuration:
Enter the certificate file path: cert_chain.pem
Enter the trust store file path: cacerts.pem
Enter the private key path: key.pem
Enter the password for the passphrase file path or skip security
configuration (default: NONE):
Should a CRL be honored for the external certificate?
1) Use the CRL defined in the certificate.
2) Use the specific CRL directory.
3) Do not use a CRL.
q) Skip security configuration.
CRL option (1): 2
Enter the CRL location path: crl
Then confirm input information and answer the subsequent questions.
```

Adding and removing certificates

You can manage external certificates on NetBackup Appliance using the **Certificate** commands.

You can use the **Settings** > **Security** > **Certificate** > **Add CACertificate** command to add a server CA, HTTPS proxy CA, or LDAP CA certificate to the certificate authority list. Ensure that you paste the CA certificate content in the PEM or P7B format. The Appliance appends this CA certificate to the certificate authority list. Before appending the CA certificate, the appliance verifies whether the CA certificate is already being used on the appliance. If yes, the appliance quits with a message.

You can use the **Settings** > **Security** > **Certificate** > **Remove CACertificate** command to remove a server CA certificate from the certificate authority list. The

available CA certificates are listed and you can select the certificate that you want to remove.

About forwarding logs to an external server

This feature can forward NetBackup Appliance system logs (syslogs) to an external log management server.

The following types of log severs are supported:

- Splunk

NetBackup Appliance uses the Rsyslog client to forward logs. In addition to Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance. Refer to the log management server documentation to verify Rsyslog client support.

You can view, enable, and disable log forwarding from the NetBackup Appliance Shell Menu.

See "Uploading certificates for TLS" on page 63.

See "Enabling log forwarding" on page 64.

Uploading certificates for TLS

Use TLS to secure the log transmissions from the appliance to the log server. TLS is optional for log forwarding. However, Veritas recommends that you enable TLS for security purposes.

NetBackup Appliance currently only supports the following:

- TLS Anonymous Authentication for log forwarding.
- X.509 file format for certificate files.

Before you enable TLS, you must first do the following:

- Deploy the configured certificate and private key files from the Certificate Authority (CA) server onto your log server.
- Upload valid certificates to opened NFS and CIFS shares on the appliance. For log forwarding security information, see the *NetBackup Appliance Security Guide*.

Note: You can also upload certificate files from the **Manage > File Manager** menu in the appliance web console.

To upload the certificate

1. Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
2. To open NFS and CIFS shares on the appliance, enter the following command:

   `Share General Open`
3. On the server where the certificates reside, mount an NFS or a CIFS share to the appliance as follows:

   NFS: `<appliance.name>:/inst/share`

   CIFS: `\\<appliance.name>\general_share`
4. Upload two certificates and one private key file. The certificate file names are as follows:
   - `ca-server.pem`
   - `nba-rsyslog.pem`
   - `nba-rsyslog.key`
5. To close the shares on the appliance, enter the following command:

   `Share General Close`

See "About forwarding logs to an external server" on page 63.

See "Enabling log forwarding" on page 64.

Enabling log forwarding

This procedure describes how to enable the log forwarding feature.

To enable log forwarding

1. Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
2. To enable log forwarding, enter the following command:

   `Enable`

   Specify the following:
   - **Server name or IP address**: Enter the name or the IP address of the external log management server.
   - **Server port**: Enter the port number of the external log management server.
   - **Protocol**: Select either **UDP** or **TCP**. **TCP** is the default.

- **Interval**: Enter the forwarding interval in minutes. The options are **0**, **15**, **30**, **45**, or **60**. The default is **15**. If you set the interval to **0**, appliance continuously forwards syslogs to the target server.
- **TLS**: Select either **Yes** or **No**. **Yes** is the default.

Note: Enabling TLS requires that you upload two certificates and one private key to the appliance.

See "Uploading certificates for TLS" on page 63.

---

3 Verify the configuration summary, and type `yes` to complete the configuration.

See "About forwarding logs to an external server" on page 63.

See "Uploading certificates for TLS" on page 63.

Creating the appliance login banner

The following procedures describe how to set the appliance login banner using the NetBackup Appliance Web Console.

To enable and create a new login banner using the NetBackup Appliance Web Console

1 Log onto the NetBackup Appliance Web Console.

2 Click **Settings > Notifications > Login Banner**.

3 Select the **Display Login Banner** check box.

Note: The **Login Banner Heading** and **Login Banner Text** fields are only activated if **Display Login Banner** is checked.

---

4 Enter the desired text in the **Login Banner Heading** and the **Login Banner Text** fields.

5 Click **Preview** to review your changes.

6 Select the **Apply changes in NetBackup** check box if you want the same login banner to appear in the NetBackup Administration Console.

7 Click **Save**.

When the confirmation dialog window appears, click **Yes** to apply the changes, or click **No** to continue making changes.

Once the login banner is enabled, you can go back and make changes. New changes are only applied if you click **Save**.

The following procedures describe how to set the appliance login banner using the NetBackup Appliance Shell Menu.

To enable and create a new login banner using the NetBackup Appliance Shell Menu

1. Log onto the NetBackup Appliance Shell Menu.
2. Run the `Main > Settings > Notifications > LoginBanner Set` command.
3. Enter a banner heading, and then press **Enter**.
4. Enter the banner message text.

   Once you have entered the banner message, type **end** on a new line and press **Enter**.
5. A preview of the login banner appears with the following message:

   ```
   The existing login banner will be overwritten and the SSH daemon
   will be restarted. Do you want to proceed? [y, n]: (y)
   ```

   Type **y** and press **Enter** to set the login banner. Type **n** and press **Enter** to cancel any changes and exit the login banner configuration.
6. The following message appears:

   ```
   Do you want to use this banner for the NetBackup Administration
   Console as well? (Any existing Netbackup login banner will be
   overwritten.) [y, n]: (y)
   ```

   Type **y** and press **Enter** to set the login banner in the NetBackup Administration Console. Type **n** and press **Enter** to continue without changing the NetBackup login banner.

Once the login banner is enabled, you cannot make individual changes to it using the NetBackup Appliance Shell Menu. However, you can run the `LoginBanner Set` command again and overwrite the existing banner with one that contains your desired changes. Alternatively, you can use the NetBackup Appliance Web Console to make individual changes.

For more information on the login banner commands, refer to the *NetBackup Appliance Command Reference Guide*.

Chapter 4

Steps to protect NetBackup

This chapter includes the following topics:

- Send audit events to log forwarding endpoints
- Display a banner to users when they sign in

About NetBackup hardening

This chapter contains information on the NetBackup features that can help to secure your data protection infrastructure. For more detailed information about NetBackup security, see the *NetBackup Security and Encryption Guide*.

Configure NetBackup for single sign-on (SSO)

This section provides steps to set up trust and exchange configuration information between the IDP and the NetBackup primary server. Before proceeding with the steps, ensure that the following prerequisites are met in your environment:

- An IDP is set up and deployed in your environment.
- The IDP is configured to authenticate domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).

Table 4-1 Steps to configure NetBackup for single sign-on

Step	Action	Description
1.	Download the IDP metadata XML file	Download and save the IDP metadata XML file from the IDP. SAML metadata that is stored in XML files is used to share configuration information between the IDP and the NetBackup primary server. The IDP metadata XML file is used to add the IDP configuration to the NetBackup primary server.
2.	Configure the SAML keystore, and add and enable the IDP configuration on the NetBackup primary server	See "Configure the SAML KeyStore" on page 69. See "Configure the SAML keystore and add and enable the IDP configuration" on page 72.

Table 4-1 Steps to configure NetBackup for single sign-on *(continued)*

Step	Action	Description
3.	Download the service provider (SP) metadata XML file	The NetBackup primary server is the SP in the NetBackup environment. You can access the SP metadata XML file from the NetBackup primary server by entering the following URL in your browser: `https://masterserver/netbackup/sso/saml2/metadata` Where *masterserver* is the IP address or host name of the NetBackup primary server.
4.	Enroll the NetBackup primary server as a service provider (SP) with the IDP	See "Enroll the NetBackup primary server with the IDP" on page 74.
5.	Add SAML users and the SAML groups that use SSO to the necessary RBAC roles	SAML users and SAML user groups are available in RBAC only if the IDP is configured and enabled on the NetBackup primary server. For steps on adding RBAC roles, see the following topic.

After the initial setup, you can choose to enable, update, disable, or delete the IDP configuration.

After the initial setup, you can choose to update, renew, or delete the NetBackup CA SAML keystore . You can also configure and manage the ECA SAML keystore.

Configure the SAML KeyStore

To establish a trust between the NetBackup primary server and the IDP server, you must configure an SAML KeyStore on the NetBackup primary server. Depending on whether you are using the NetBackup CA or an external certificate authority (ECA), refer to either of the following sections:

Note: If you are using a combination of an ECA and NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server.

Note: The SAML KeyStore configuration using batch files, such as `configureCerts.bat`, `configureCerts`, `configureSAMLECACert.bat`, `configureSAMLECACert`and their corresponding options is deprecated.

Configure a NetBackup CA KeyStore

If you are using the NetBackup CA, create the NetBackup CA KeyStore on the NetBackup primary server.

To create a NetBackup CA KeyStore

1. Log on to the NetBackup primary server as root or administrator.
2. Run the following command:

   ```
   nbidpcmd -cCert -M master_server -f
   ```

   `-f` is optional. Use the option for the forceful update.

Once the NetBackup CA KeyStore is created, ensure that you update the NetBackup CA KeyStore every time the NetBackup CA certificate is renewed.

To renew the NetBackup CA KeyStore

1. Log on to the NetBackup primary server as root or administrator.
2. Run the following command:

   ```
   nbidpcmd -rCert -M master_server
   ```

3. Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

   https://*primaryserver*/netbackup/sso/saml2/metadata

   Where *primaryserver* is the IP address or host name of the NetBackup primary server.
4. Upload the new SP metadata XML file to the IDP.

   See "Enroll the NetBackup primary server with the IDP" on page 74.

To remove the NetBackup CA KeyStore

1. Log on to the NetBackup primary server as root or administrator.
2. Run the following command

   ```
   nbidpcmd -dCert -M master_server
   ```

3. Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

   https://*primaryserver*/netbackup/sso/saml2/metadata

   Where *primaryserver* is the IP address or host name of the NetBackup primary server.
4. Upload the new SP metadata XML file to the IDP.
5. See "Enroll the NetBackup primary server with the IDP" on page 74.

Configure an ECA KeyStore

If you are using an ECA, import the ECA KeyStore to the NetBackup primary server.

Note: If you are using a combination of an ECA and the NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server. To use the NetBackup CA, you must first remove the ECA KeyStore.

To configure an ECA KeyStore

1. Log on to the primary server as root or administrator.
2. Depending on whether you want to configure SAML ECA keystore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:
   - Run the following command to use NetBackup ECA configured KeyStore:
     `nbidpcmd -cECACert -uECA` *`existing ECA configuration`* `[-f] [-M` *`primary_server`*`]`
   - Run the following command to use ECA certificate chain and private key provided by the user:
     `nbidpcmd -cECACert -certPEM` *`certificate chain file`* `-privKeyPath` *`private key file`* `[-ksPassPath` *`Keystore Passkey File`*`] [-f] [-M <master_server>]`
   - Certificate chain file specifies the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
   - Private key file specifies the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
   - KeyStore passkey file specifies the KeyStore password file path and must be accessible to the primary server on which the configuration is being performed.
   - Primary server is the host name or IP address of primary server on which you want to perform SAML ECA KeyStore configuration. The NetBackup primary server where you run the command is selected by default.

To remove the ECA KeyStore

1. Log on to the primary server as root or administrator.
2. Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

   https://*primaryserver*/netbackup/sso/saml2/metadata

   Where *primaryserver* is the IP address or host name of the NetBackup primary server.
3. Upload the new SP metadata XML file to the IDP.

   See "Enroll the NetBackup primary server with the IDP" on page 74.

Configure the SAML keystore and add and enable the IDP configuration

Before proceeding with the following steps, ensure that you have downloaded the IDP metadata XML file and saved it on the NetBackup primary server.

To configure SAML keystore and add and enable an IDP configuration

1. Log on to the primary server as root or administrator.
2. Run the following command.

   For IDP and NetBackup CA SAML KeyStore configuration:

   ```
   nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
   [-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
   group field] [-cCert] [-f] [-M primary server]
   ```

   Alternatively for IDP and ECA SAML KeyStore configuration:

   Depending on whether you want to configure SAML ECA KeyStore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:

   - Use NetBackup ECA configured keystore:

     ```
     nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
     file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
     user group field] -cECACert -uECA existing ECA configuration
     [-f] [-M Primary Server]
     ```

   - Use ECA certificate chain and private key provided by the user:

     ```
     nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
     file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
     user group field] -cECACert -certPEM certificate chain file
     ```

`-privKeyPath` *`private key file`* `[-ksPassPath` *`KeyStore passkey file`*`] [-f] [-M primary server]`

Replace the variables as described below:

- *`IDP configuration name`* is a unique name provided to the IDP configuration.
- *`IDP XML metadata file`* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- `-e true | false` enables or disables the IDP configuration. An IDP configuration must be added and enabled, otherwise users cannot sign in with the single sign-on (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.
- *`IDP user field`* and *`IDP user group field`* are the SAML attribute names, which are mapped to the `userPrincipalName` and the `memberOf` attributes of the AD or LDAP.

  Note: Ensure that the SAML attribute names are defined in the format of ***username@domainname*** and **(CN=*group name*, DC=*domainname*)** respectively.

- *`primary Server`* is the host name or IP address of primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.
- *`Certificate Chain File`* is the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
  `Private Key File` is the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
  `KeyStore Passkey File` is the KeyStore passkey file path and must be accessible to the primary server on which the configuration is being performed.

Fore example: `nbidpcmd -ac -n veritas_configuration -mxp file.xml -t SAML2 -e true -u username -g group-name -cCert -M primary_server.abc.com`

Enroll the NetBackup primary server with the IDP

The NetBackup primary server must be enrolled with the IDP as a service provider (SP). For step-by-step procedures that are specific to a particular IDP, see the following table:

Table 4-2 IDP-specific steps for enrolling the NetBackup primary server

IDP name	Link to steps
ADFS	https://www.veritas.com/docs/100047744
Okta	https://www.veritas.com/docs/100047745
PingFederate	https://www.veritas.com/docs/100047746
Azure	https://www.veritas.com/docs/100047748
Shibboleth	https://www.veritas.com/docs/00047747

Enrolling an SP with an IDP typically involves the following operations:

Uploading the SP metadata XML file to the IDP

The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). The SP metadata XML file is required by the IDP to establish trust, and exchange authentication and authorization information with the SP.

Mapping the SAML attributes to their AD or LDAP attributes

Attribute mappings are used to map SAML attributes in the SSO with its corresponding attributes in the AD or LDAP directory. The SAML attribute mappings are used for generating SAML responses, which are sent to the NetBackup primary server. Ensure that you define SAML attributes that map to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP directory. The SAML attributes must adhere to the following formats:

Table 4-3

Corresponding AD or LDAP attribute	SAML attribute format
`userPrincipalName`	***username@domainname***
`memberOf`	**(CN=*group name*, DC=*domainname*)**

Note: While adding the IDP configuration to the NetBackup primary server, the values entered for the user (`-u`) and user group (`-g`) options must match the SAML attribute names that are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

See "Configure the SAML keystore and add and enable the IDP configuration" on page 72.

Configure user authentication with smart cards or digital certificates

You can map a smart card or certificate with an AD or an LDAP domain for user validation. Alternatively, you can configure a smart card or certificate without an AD or an LDAP domain.

See "Configure smart card authentication with a domain" on page 75.

See "Configure smart card authentication without a domain" on page 76.

Configure smart card authentication with a domain

You can configure NetBackup to validate users with smart cards or certificates with an AD or an LDAP domain.

Note the following prerequisites:

- Before you add the authentication method you must add the domain that is associated with your NetBackup users. See the NetBackup Security & Encryption Guide.
- Ensure that you complete the role-based access control (RBAC) configuration for the NetBackup users before you configure smart card or certificate authentication.

To configure smart card authentication with a domain

1. At the top right, select **Settings > Smart card authentication**.
2. Turn on **Smart card authentication**.
3. Select the required AD or LDAP domain from the **Select the domain** option.
4. Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
5. Optionally, enter the **OCSP URI**.

   If you do not provide the OCSP URI, the URI in the user certificate is used.

6 Click **Save**.

7 To the right of **CA certificates**, click **Add**.

8 Browse for or drag and drop the **CA certificates** and click **Add**.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be `.crt`, `.cer`, `.der`, `.pem`, or `PKCS #7` format and less than 64KB in size.

9 On the **Smart card authentication** page, verify the configuration information.

10 Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.

See the browser documentation for instructions or contact your certificate administrator for more information.

11 When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

For such users, the domain name and domain type are smart card.

Configure smart card authentication without a domain

You can configure NetBackup to validate users with smart cards or certificates without an associated AD or LDAP domain. Only users are supported for this configuration. User groups are not supported.

To configure smart card authentication without a domain

1 At the top right, select **Settings > Smart card authentication**.

2 Turn on **Smart card authentication**.

3 (Conditional step) If AD or LDAP domain is configured in your environment, select **Continue without the domain** option.

4 Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).

5 Optionally, enter the **OCSP URI**.

If you do not provide the OCSP URI, the URI in the user certificate is used.

6. Click **Save**.
7. To the right of **CA certificates**, click **Add**.
8. Browse for or drag and drop the **CA certificates** and click **Add**.
9. Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

   Certificate file types must be `.crt`, `.cer`, `.der`, `.pem`, or `PKCS #7` format and less than 64KB in size.
10. On the **Smart card authentication** page, verify the configuration information.

    Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.
11. When users sign in, they now see an option to **Sign in with certificate or smart card**.

    If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

Access codes

To run certain NetBackup administrator commands, for example `bperror`, you need to authenticate through the web UI. You need to generate an access code through the command-line interface, get the access request approved from the administrator, and then access the command.

With the web UI authentication for CLI access, NetBackup administrators can delegate the associated privileges to other users. By default, only a root administrator or an administrator can perform NetBackup operations through the command-line interface. The web UI authentication support allows non-root users to administer NetBackup who have CLI access that the Security Administrator has granted. You can also administer NetBackup with a non-RBAC user role (such as Operating System Administrator) even though you are not registered as a NetBackup user. Each time you need to generate a new access code to access CLIs.

Get CLI access through web UI authentication

To get CLI access

1. Run the following command:

   ```
   bpnbat -login -logintype webui
   ```

   An access code is generated.

2. (Optional) Run the following command if you want to get the code approved from your security administrator:

   ```
   bpnbat -login -logintype webui -requestApproval
   ```

3. If you have the Command Line (CLI) Administrator role, you can use the web UI to approve the CLI access request using the access code.

   See “Approve your CLI access request” on page 78.

   If you do not have the Command Line (CLI) Administrator role, request the administrator to approve the CLI access request.

   See “Approve CLI access requests of other users” on page 78.

4. Once the CLI access request is approved, go to the command-line interface and run the required command.

   By default, the CLI access session is valid for 24 hours.

Approve your CLI access request

You can approve your CLI access request using the web UI.

To approve your CLI access request

1. On the right, click your user profile icon.
2. Click **Approve Access Request**.
3. Enter the CLI access code that you have received from the user, who requires CLI access and click **Review**.
4. Review the access request details.
5. Click **Approve**.

Approve CLI access requests of other users

If you have the Command Line (CLI) Administrator role, you can approve access requests of other users using the web UI.

To approve CLI access request of other user

1. On the left, select **Security > Access keys > Access codes**.
2. Enter the CLI access code that you have received from the user, who requires CLI access and click **Review**.
3. Review the access request details.
4. Provide comments, if any.
5. Click **Approve**.

Workflow to configure immutable and indelible data

Carry out the following steps in the given order to protect your data by configuring immutability and indelibility.

Table 4-4 Workflow to configure immutable and indelible data

Step	Description
1	Configure the following WORM settings on the storage server. The storage administrator configures these settings outside of NetBackup. ■ **WORM capable** - If the storage unit and the associated disk pool are enabled to use the WORM property at the time of backup image creation, the backup images are set to be immutable and indelible. ■ **Lock Minimum Duration** - Specifies the minimum allowed duration for which the data for a backup image is indelible. The storage administrator sets this duration on the Logical Storage Unit (LSU) or the Domain Volume (DV), which NetBackup discovers. ■ **Lock Maximum Duration** - Specifies the maximum allowed duration for which the data for a backup image is indelible. The storage administrator sets this duration on the Logical Storage Unit (LSU) or the Domain Volume, which NetBackup discovers. Refer to the OST vendor plug-in documentation.
2	Configure a disk pool using WORM-capable volumes. See “About configuring disk pool storage” on page 80.
3	Configure a storage unit with the **Use WORM** option enabled. See “Use WORM setting” on page 80.
4	Configure a backup policy using the WORM-enabled storage unit. See “Creating a backup policy” on page 80.

Note: In case of storage changes or third-party OST vendor software upgrades, you need to manually update the storage servers and the disk pools. See the 'Completing your system update after an upgrade' section from the NetBackup Upgrade Guide.

About configuring disk pool storage

You can configure disk pools if you license a NetBackup feature that uses disk pools.

For more information, see the NetBackup online help or the following guides:

- The *NetBackup AdvancedDisk Storage Solutions Guide*.
- The *NetBackup Cloud Administrator's Guide*.
- The *NetBackup Deduplication Guide*.
- The *NetBackup OpenStorage Solutions Guide for Disk*.
- The *NetBackup Replication Director Solutions Guide*.

Use WORM setting

The **Use WORM** option is enabled for storage units that are WORM capable. Select this option if you want the backup images on this storage unit to be immutable and indelible until the WORM Unlock Time.

Note: You must also select the **On Demand Only** option whenever the **Use WORM** option is selected.

WORM is the acronym for Write Once Read Many.

Creating a backup policy

Use the following procedure to create a backup policy.

To create a policy

1. In **NetBackup web UI**, select **Protections > Policies**.
2. Click **Add**.
3. Enter the policy name.
4. Configure the attributes, the schedules, the clients, and the backup selections for the new policy.

Add a configuration for an external CMS server

This section provides you the procedure for adding a configuration for an external CMS server.

To add a configuration for an external CMS server

1. On the left, click **Credential management**.
2. On the **External CMS servers** tab, click **Add** and provide the following properties:
   - Configuration name
   - Description (for example: This configuration is used to access the external CMS.)
   - External CMS provider
   - Host name
   - Port number: Default port number 443 would be considered (if not provided by the user).

   Note: While configuring the external CMS server for CyberArk server, user can use the DNS hostname or IPV4 address. However it is recommended to use the DNS hostname for connecting to the host. CyberArk configuration fails if IPV6 address is used.
3. Click **Next**.
4. On the Associate credentials page, **Select existing credential** or **Add a new credential**.

   More information is available on how to add a new credential.

   See "Add a credential for CyberArk" on page 81.
5. Click **Next** and follow the prompts to complete the wizard.

Add a credential for CyberArk

This type of credential allows you to access an external CMS server.

To add a credential for an external CMS server

1. On the left, click **Credential management**.
2. On the **Named credentials** tab, click **Add**.
3. Select **NetBackup** and click **Start**.

On **Add a credential** page, provide the following properties:

- Credential name
- Tag
- Description (for example: This credential is used to access the external CMS.)

4 Click **Next**.

5 Select **CyberArk** as the category.

6 Provide the credential details for CyberArk server:

These details are used to authenticate the communication between the NetBackup primary server and the external CMS server:

- Certificate - Specify the certificate file contents.
- Private key - Specify the private key file contents.
- CA Certificate - Specify the CA certificate file contents.
- Passphrase - Enter the passphrase of the private key file.
- CRL check level - Select the revocation check level for the external CMS server certificate.
  CHAIN - The revocation status of all the certificates from the certificate chain are validated against the CRL.
  DISABLE - Revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication.
  LEAF - The revocation status of the leaf certificate is validated against the CRL.

7 Click **Next**.

8 Add a role that you want to have access to the credential.

- Click **Add**.
- Select the role.
- Select the credential permissions that you want the role to have.

9 Click **Next** and follow the prompts to complete the wizard.

Configuring an isolated recovery environment on a NetBackup BYO media server

You can configure an isolated recovery environment (IRE) on a NetBackup BYO media server to create an air gap between your production environment and a copy of the protected data. The air gap restricts network access to the IRE environment all the time. This feature helps to protect against ransomware and malware. To configure an IRE, you need a production NetBackup environment and a NetBackup IRE environment with MSDP server configured in a BYO Media server. The production environment does not require any additional steps for this feature.

Use the following procedure to configure an IRE on a BYO media server.

To configure an IRE on a BYO media server

1. Note that this procedure applies only to NetBackup 10.1 and later.

   Log in to the media server.

2. This step is optional. Use this step in any of the following conditions:

   - You want to enable IRE on an existing system.
   - AIR SLP is already configured.
   - You want to configure the IRE schedule in step 4 based on the existing SLP window.

   Run the following command to show the SLP windows for replication from the primary server to the MSDP storage on the media server:

   ```
   /usr/openv/pdde/shell/bin/show_slp_windows
   --production_primary_server production primary server name
   --production_primary_server_username production primary server
   username --ire_primary_server target primary server name
   --ire_primary_server_username target primary server username
   ```

   Where:

   - The *production primary server name* is the fully qualified domain name (FQDN) of the primary server in your production environment.
   - The *production primary server username* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment.
     The *production primary server username* must be in `domain_name\user_name` format on Windows.

- The *target primary server name* is the FQDN of the primary server in the IRE. Use the same hostname that you used to configure the SLPs in the production environment.
- The *target primary server username* is the username of a NetBackup user with permission to list the SLPs and storage units in the IRE environment. The *target primary server username* must be in `domain_name\user_name` format on Windows.

For example:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=appadmin
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=appadmin
```

The following is an example output of the command:

```
EveryDayAtNoon: SLPs: SLP1 Sunday start: 12:00:00 duration: 00:59:59
Monday start: 12:00:00 duration: 00:59:59 Tuesday start: 12:00:00
duration: 00:59:59 Wednesday start: 12:00:00 duration: 00:59:59
Thursday start: 12:00:00 duration: 00:59:59 Friday start: 12:00:00
duration: 00:59:59 Saturday start: 12:00:00 duration: 00:59:59
WeeklyWindow: SLPs: SLP2 Sunday start: 10:00:00 duration: 01:59:59
Monday NONE Tuesday NONE Wednesday NONE Thursday NONE Friday NONE
Saturday start: 10:00:00 duration: 01:59:59
```

This example shows two SLP windows:

- A daily window for one hour starting at noon.
- A weekly window for 2 hours starting at 10 A.M.

Note: If an SLP window is greater than 24 hours, the `show-slp-windows` may display the duration incorrectly.

---

3 Based on the output for your environment, determine a daily schedule that accommodates the SLP windows and take note of it. In the previous example, a daily schedule from 10 A.M. to 12:00 P.M. accommodates both SLP windows.

The start times in the output of this command are in the IRE server's time zone.

Note: If the time zone of the production primary server is changed, you must restart the NetBackup services.

---

4 Run the following command to configure the subnets and IP addresses that are allowed to access the media server:

```
/usr/openv/pdde/shell/bin/ire_network_control allow-subnets
--subnets CIDR subnets or IP addresses
```

Where the *CIDR subnets or IP addresses* field is a comma-separated list of the allowed IP addresses and subnets in CIDR notation.

For example:

```
/usr/openv/pdde/shell/bin/ire_network_control allow-subnets
--subnets 10.10.100.200,10.80.40.0/20
```

Note: The IRE primary server, the IRE media servers, and the DNS server for the IRE environment must be included in the allowed list. If all these servers are in the same subnet, only the subnet is required to be in the allowed list.

Note: If your network environment is dual stack, ensure that both IPv4 and IPv6 subnets and IP addresses of the IRE domain are configured in allowed subnets. For example, if you specify only IPv6 subnets in the allowed subnet, all the IPv4 addresses are not allowed to access the IRE storage server.

---

5 Run the following command to set the daily air gap schedule:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time time --duration duration [--weekday 0-6]
```

`weekday` is optional. It starts from Sunday. You can configure different network and open or close window for a specific weekday. If it is not specified, the IRE schedule is the same on each day.

For example:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time 10:00:00 --duration 03:00:00
```

Note: The SLP replication window on the production domain must be configured to be open at the same time as the IRE schedule. The IRE schedule window can be different for weekdays. You can configure a window for a specific weekday.

For example:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time 11:00:00 --duration 10:00:00 --weekday 0
```

Note: If the production and the IRE environments are in different time zones, the schedule must begin only once per day in both time zones.

For example, if one environment is in the Asia/Kolkata time zone and the other is in the America/New_York time zone, the following schedule in Kolkata is not supported: Tuesday start time 22:00:00 and Wednesday start time 03:00:00. When these start times are converted to the New York time zone, they become Tuesday start time 12:30:00 and Tuesday start time 17:30:00, which is not supported.

Note: If you want to open air gap network for 24 hours on all days, you do not need to configure IRE schedule. However, the IRE media server restricts the network access from the hosts that are not configured in the subnets that the air gap allows.

Configuring AIR for replicating backup images from production environment to IRE BYO environment

Once IRE configuration is completed, the production NetBackup hosts are no longer able to access the IRE MSDP storage server. You need to enable MSDP reverse connection to allow the data transmission between the production MSDP server and the IRE MSDP server.

Note: AIR configuration operations can be performed when the external network is open by IRE air gap. All the given operations are performed on the IRE MSDP server.

Prerequisites

Before you configure AIR for replicating backup images from production environment to IRE BYO environment, ensure the following:

- In case of NetBackup certificate authority (CA), get the CA certificate and host certificate for the IRE MSDP storage server from the production primary server.
- Create a token on the production primary server.

To configure AIR for replicating backup images from production environment to IRE BYO environment

1. Run the following commands:
   - NetBackup certificate:

     ```
     /usr/openv/netbackup/bin/nbcertcmd -getCACertificate -server
     <production primary server>
     /usr/openv/netbackup/bin/nbcertcmd -getCertificate -server
     <production primary server> -token <token>
     ```

   - External certificate:

     ```
     /usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -server
     <production primary server>
     ```

2. Run the following command to enable MSDP reverse connection.

   ```
   /usr/openv/pdde/shell/bin/ire_network_control reverse_connection
   --add production msdp server
   ```

3 This step is not required if you have not configured any IRE schedule. That is because if the IRE schedule is not configured, MSDP reverse connection is enabled for 24 hours on all days. The production primary server can configure the SLP replication operation with any SLP window.

Once the MSDP reverse connection is configured, copy the IRE schedule to the NetBackup production domain as an SLP window. Use the following command:

```
/usr/openv/pdde/shell/bin/sync_ire_window
--production_primary_server production primary server name
--production_primary_server_username production primary server
username [--slp_window_name slp_window_name ]
```

Where:

The *production primary server name* is the fully qualified domain name (FQDN) of the primary server in your production environment.

The *production primary server username* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment.

The *production primary server username* must be in `domain_name\user_name` format on Windows.

The *slp_window_name* is the name of the SLP window to be synced with the IRE window. It is an optional parameter. If the SLP window is not specified, an SLP window with the name `IRE_DEFAULT_WINDOW` is created on the production primary server.

4 You can then add the IRE WORM storage server as a replication target of the production NetBackup domain. Then add the replication operation to an existing SLP to replicate from production NetBackup domain to IRE WORM storage server using the following command:

```
/usr/openv/pdde/shell/bin/add_replication_op
--production_primary_server production primary server name
--production_primary_server_username production primary server
username --source_slp_name source slp name
--target_import_slp_name target import slp name
--production_storage_server production storage server name
--ire_primary_server_username ire primary server username
--target_storage_server target storage server name
--target_storage_server_username target storage server username
--production_storage_unit msdp storage unit name used in source
SLP [--slp_window_name slp window name]
```

Where:

The *production primary server name* is the fully qualified domain name (FQDN) of the primary server in your production environment.

The *production primary server username* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment.

The *production primary server username* must be in `domain_name\user_name` format on Windows.

The *production storage server name* is the fully qualified domain name (FQDN) of the production storage server in your production environment.

The *ire primary server username* is the username for administrator user of IRE primary server.

The *ire primary server username* must be in `domain_name\user_name` format on Windows.

The *source slp name* is the SLP name on the production primary server against which a replication operation is added.

The *target import slp name* is the import SLP name from IRE primary server.

The *target storage server name* is the fully qualified domain name (FQDN) of the target WORM storage server.

The *target storage server username* is the username of the target WORM storage server.

The *slp_window_name* is the name of the SLP window that is synced with the IRE window. Alternatively, it is created on the production primary server before

the operation. It is an optional parameter. If the SLP window is not specified, an SLP window with the name `IRE_DEFAULT_WINDOW` is used that must be created using the `sync_ire_window` command before the operation.

The *production_storage_unit* is the storage unit name of type PureDisk used in source SLP.

Note: The source SLP and target import SLP need to be created before the operation.

About FIPS support in NetBackup

By default, FIPS mode is disabled in NetBackup.

The following workloads are supported in FIPS-compliant mode:

- Oracle, MS-SQL, SAP HANA, DB2, VMware, Hyper-V, RHV, Nutanix, DynamicNAS, MongoDB, Hadoop, HBase, MySQL, PostgreSQL, SQLite, MariaDB, SharePoint
- Cassandra, Sybase, Informix, MS-Exchange, Enterprise Vault, BMR, Universal Shares, OpenStack (cloud-based solution)

The following operating system-level support is available in FIPS mode:

- Once you enable FIPS mode on RHEL 8, the operating system requires that each RPM package has a SHA-256 digest. RPMs that do not have this digest will fail to install. The RPMs that are built using the native toolchain present on RHEL 6 or RHEL 7 platforms do not include a SHA-256 digest and therefore can fail to install on RHEL 8 when FIPS mode is enabled. This issue affects NetBackup 9.1 and earlier setups as packages for these versions are built using the OS native toolchain on RHEL 7 or earlier.
  Starting with NetBackup 10.0, the packages are built using a toolchain that adds the SHA-256 digest and these can be installed on RHEL 8 with FIPS mode enabled.

The following components, configurations, or operations are not supported in FIPS mode:

- Client-side encryption

Note: To perform a backup with client-side encryption, you need to disable FIPS mode on the client host.

- NDMP backups
- Scripts (Perl, batch, shell, python) that are executed within NetBackup
- Binaries or utilities: `restore_spec_utility`, `nbcallhomeproxyconfig`, `nbbsdtar`, `nbrepo`
- NetBackup domain with NBAC enabled
  If NBAC is configured in the NetBackup domain, it is recommended that you do not enable FIPS mode.
- The MQBROKER processes do not support NetBackup-level FIPS configuration on Windows.
- MIT Kerberos used by Hadoop and HBase does not operate with a FIPS-enabled OpenSSL. To perform backup with Kerberos authentication, you need to disable FIPS on the backup host.
- NetBackup CloudPoint does not support the CloudPoint host that is configured in FIPS mode.
- SharePoint internally uses encryption algorithms that do not comply with FIPS standards. The Windows FIPS policy blocks the MD5 hashing algorithms that SharePoint uses. Therefore, the OS-level FIPS policy should be disabled for the SharePoint restores for successful operation.
  Note that NetBackup-FIPS is supported for protecting SharePoint.
  See the following articles for more details:
  FIPS and SharePoint Server
  SharePoint 2016 and FIPS

Enable FIPS mode on NetBackup during installation

NetBackup lets you enable FIPS mode during installation. For more information, refer to the NetBackup Installation Guide.

After you enable FIPS mode on NetBackup during installation, enable FIPS mode for the **NetBackup Administration Console**.

See “Enable FIPS mode for the NetBackup Administration Console” on page 94.

Enable FIPS mode on a NetBackup host after installation

This section provides steps to enable FIPS mode on a primary server, a media server, or a client in a NetBackup domain. You should do the following configurations on each host to enable FIPS.

If the host is a primary server, enable FIPS mode for the NetBackup Authentication Broker (AT) by updating the `VRTSatlocal.conf` configuration file on the primary server.

See "Enable FIPS mode for the NetBackup Authentication Broker service" on page 93.

To enable FIPS mode on a NetBackup host

1. Enable the `NB_FIPS_MODE` flag in the NetBackup configuration file.

   See "NB_FIPS_MODE option for NetBackup servers and clients" on page 95.

2. Restart the NetBackup services.

To verify if a certain daemon or a command runs in FIPS mode, check the respective logs. The log lines are available only for the daemons and commands that use cryptography.

Example 1: To verify if the `nbcertcmd` command runs in FIPS mode

1. Run the following command:

   ```
   nbcertcmd -ping
   ```

   Location of the command:

   Windows: *`install_path`*`\NetBackup\bin\nbcertcmd`

   UNIX: `/usr/openv/netbackup/bin/nbcertcmd`

2. Check the `nbcertcmd` logs.

   Location of the log directory:

   Windows: *`install_path`*`\NetBackup\logs\nbcert`

   UNIX: `/usr/openv/netbackup/logs/nbcert`

   The following log lines should be present:

```
<2> nbcertcmd: ./nbcertcmd -ping ProcessContext: ProcessName:[nbcertcmd],
FipsMode:[ENABLED], Username:[root], IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

Example 2: To verify if the NetBackup Web Management Console runs in FIPS mode

- By default, FIPS mode is disabled when the **NetBackup Web Management Console** (`nbwmc`) service runs. FIPS mode is enabled for the `nbwmc` service after you enable it for the NetBackup host.

  Check the `catalina` log file on the NetBackup primary server host to verify if the `nbwmc` service runs in FIPS mode.

  Location of the log file:

  Windows:
  `install_path``\NetBackup\wmc\webserver\logs\catalina-`*`date`*`.log`

  UNIX: `/usr/openv/wmc/webserver/logs/catalina-`*`date`*`.log`

  The following log lines should be present:

  ```
  The nbwmc service is running in FIPS approved mode
  ```

Enable FIPS mode for the NetBackup Authentication Broker service

The NetBackup Authentication Broker (`nbatd`) service runs only on the NetBackup primary server, therefore you need to enable FIPS mode on the primary server to enable it for the `nbatd` service.

FIPS mode is disabled by default.

To enable FIPS mode for the `nbatd` service

1. Open the following directory on the primary server:

   On UNIX: `/usr/openv/netbackup/sec/at/bin/`

   On Windows: *`install_path`*`\NetBackup\sec\at\bin\`

2. Run the following command:

   On UNIX:
   ```
   run vssregctl -s -f
   /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
   -b "Security\Authentication\Client" -k FipsMode -t int -v 1
   ```

   On Windows:
   ```
   run vssregctl -s -f
   "install_path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"
   -b "Security\Authentication\Client" -k FipsMode -t int -v 1
   ```

   For example:

   If the *install_path* is `"C:\Program Files\VERITAS"` location, run the following command on Windows:

   ```
   vssregctl -s -f "C:\Program
   Files\VERITAS\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"
   -b "Security\Authentication\Client" -k FipsMode -t int -v 1 3
   ```

   Check the `nbatd` logs.

   Location of the `nbatd` logs:

   On UNIX:

   ```
   /usr/openv/logs/nbatd
   ```

   On Windows:

   ```
   install_path\NetBackup\logs\nbatd
   ```

   The following log lines should be present:

   ```
   *** Trying to start Broker In FIPS mode ***

   *** Broker In FIPS mode already ***
   ```

3. Restart the NetBackup services.

Enable FIPS mode for the NetBackup Administration Console

By default, FIPS mode for the **NetBackup Administration Console** is disabled.

To enable FIPS mode for the NetBackup Administration Console (on local or remote host)

1. Open the **NetBackup Administration Console** configuration file.
   - On Windows computers, the file containing configuration options for the **NetBackup Administration Console** is: `install_path\java\nbj.conf`
   - On UNIX computers, the file containing configuration options for the **NetBackup Administration Console** is: `/usr/openv/java/nbj.conf`
2. In the configuration file, enable the `NB_FIPS_MODE` option. Use the following format:

   ```
   NB_FIPS_MODE = true
   ```
3. Save the changes.
4. Restart the **NetBackup Administration Console**.

To verify if the NetBackup Administration Console runs in FIPS mode

- Check the **NetBackup Administration Console** logs.

  Log location:

  On Windows:
  `install_path\logs\user_ops\nbjlogs\jbp.root.jnbSA.`*`pid`*`.log`

  On UNIX: `/usr/openv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA.`*`pid`*`.log`

  On a standalone console, create a directory structure and check the logs.

  If the log file contains the following log lines, it means the console runs in FIPS mode:

  ```
  com.safelogic.cryptocomply.fips.approved_only: true
  ```

  It should have the following log lines:

  ```
  JavaPresentationLayer- FIPS mode enforced. Reconfiguring SunJSSE.
  JavaPresentationLayer- Administration console is running in FIPS approved
  ```

  Note: This FIPS mode configuration does not affect the NetBackup KMS FIPS mode. NetBackup KMS continues to run in FIPS mode by default.

NB_FIPS_MODE option for NetBackup servers and clients

Use the `NB_FIPS_MODE` option to enable the FIPS mode in your NetBackup domain.

Table 4-5 NB_FIPS_MODE information

Usage	Description
Where to use	On NetBackup servers or clients.

How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	By default, the `NB_FIPS_MODE` option is disabled.
	To enable the option, use the following format:
	`NB_FIPS_MODE = ENABLE`
	To disable the option, use the following format:
	`NB_FIPS_MODE = DISABLE`

Equivalent Administration Console	No equivalent exists in the **NetBackup Administration Console** host properties.

Installing KMS

The following procedure describes how to install KMS.

Note: For more information about configuring KMS in a Cloud storage environment refer to the NetBackup Cloud Administrator's Guide.

The KMS service is called `nbkms`.

The service does not run until the data file has been set up, which minimizes the effect on environments not using KMS.

To install KMS

1. Run the `nbkms -createemptydb` command.
2. Enter a pass phrase for the host master key (HMK). You can also press **Enter** to create a randomly generated key.
3. Enter an ID for the HMK. This ID can be anything descriptive that you want to use to identify the HMK.
4. Enter a pass phrase for the key protection key (KPK).

5 Enter an ID for the KPK. The ID can be anything descriptive that you want to use to identify the KPK.

The KMS service starts when after you enter the ID and press Enter.

6 Start the KMS service as follows:

On UNIX, run the following command:

```
/usr/openv/netbackup/bin/nbkms
```

On Windows, do the following:

```
Start > Run > Services.msc > Start the NetBackup Key Management
Service
```

7 Use the `grep` command to ensure that the service has started, as follows: `ps -ef | grep nbkms`

8 Run the following command to register the `nbkms` service with NetBackup web services:

```
nbkmscmd -discovernbkms
```

9 Create the key group. The key group name must be an identical match to the volume pool name. All key group names must have a prefix `ENCR_`.

Note: When using key management with Cloud storage and PureDisk, the `ENCR_` prefix is not required for the key group name.

To create a (non-Cloud storage) key group use the following command syntax.
`nbkmsutil -createkg -kgname ENCR_`*`volumepoolname`*

The `ENCR_` prefix is essential. When BPTM receives a volume pool request that includes the `ENCR_` prefix, it provides that volume pool name to KMS. KMS identifies it as an exact match of the volume pool and then picks the active key record for backups out of that group.

To create a Cloud storage key group use the following command syntax.

```
nbkmsutil -createkg -kgname storage_server_name:volume_name
```

10 Create a key record by using the `-createkey` option.

```
nbkmsutil -createkey -kgname ENCR_volumepool -keyname keyname
-activate -desc "message"
```

The key name and message are optional; they can help you identify this key when you display the key.

The `-activate` option skips the prelive state and creates this key as active.

11 Provide the pass phrase again when the script prompts you.

In the following example the key group is called `ENCR_pool1` and the key name is `Q1_2008_key`. The description explains that this key is for the months January, February, and March.

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q1_2008_key
-activate -desc "key for Jan, Feb, & Mar"
```

12 You can create another key record using the same command; a different key name and description help you distinguish they key records: `nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q2_2008_key -activate -desc "key for Apr, May, & Jun"`

Note: If you create more than one key record by using the command `nbkmsutil -kgname` *`name`* `-activate`, only the last key remains active.

---

13 To list all of the keys that belong to a key group name, use the following command:

`nbkmsutil -listkeys -kgname` *keyname*

Note: You need the passphrase, salt (if applicable), key group name, and key tag to recover this key if it is lost. You must store all this information at a secure place. Salt, key group name, and key tag can be found in the output of the `nbkmsutil -listkeys` command execution.

The following command and output use the examples in this procedure.

```
# nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name        : ENCR_pool1
Supported Cipher      : AES_256
Number of Keys        : 2
Has Active Key        : Yes
Creation Time         : Thu Aug  8 16:23:06 2013
Last Modification Time: Thu Aug  8 16:23:06 2013
Description           : -
 Key Tag    : 825784185f87145c368c54e919908905a45f79927cb733337a53e9b174bbe046
 Key Name              : Q2_2013_key
 Current State         : ACTIVE
 Creation Time         : Thu Aug  8 16:25:19 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Apr, May, & Jun
 FIPS Approved Key     : No

 Key Tag    : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
 Key Name              : Q1_2013_key
 Current State         : INACTIVE
 Creation Time         : Thu Aug  8 16:25:03 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Jan, Feb, & March
 FIPS Approved Key     : No
Number of Keys: 2
```

Workflow for external KMS configuration

For external KMS integration, centralized configuration on the NetBackup primary server is used. The primary server should establish an outbound connection with the KMIP port on the external KMS server. Configure the communication channel with external KMS on the primary server with certificate credentials. The primary server then sends all the requests to the external KMS servers on behalf of other servers such as media servers.

Table 4-6 Workflow to configure a KMS

Step number	Step	Reference topic
Step 1	Validate KMS credentials	See "Validating KMS credentials" on page 100.
Step 2	Configure KMS credentials	See "Configuring KMS credentials" on page 102.
Step 3	Configure KMS	See "Configuring KMS" on page 103.
Step 4	Create keys	See "Creating keys in an external KMS" on page 103.
Step 5	Configure storage	Refer to the NetBackup Administrator's Guide, Volume I.
Step 6	Configure policy	Refer to the NetBackup Administrator's Guide, Volume I.

Validating KMS credentials

If incorrect credentials are configured in NetBackup, communication with external KMS server may fail. To avoid such failures, you can carry out certain validations before a credential can be configured for the KMS use. If a validation check is not passed, the credential cannot be configured.

The following validations are carried out while you configure a new credential or updating an existing one and it is not recommended to configure credentials if any of the checks fail:

- The certificate path is valid
- The trust store path is valid
- The private key path is valid
- The certificate(s) in certificate chain are readable

- The certificate(s) in trust store are readable
- The private key is readable
- The Common Name field is not empty
- The certificate is not expired
- The certificate is currently valid
- The private key matches the certificate
- The certificates are in the appropriate order
- The following CRL validation checks are performed, if the `ECA_CRL_PATH` is configured and the CRL check level is other than DISABLE:
  - The CRL directory consists of CRL files
  - The CRL check level is valid
  - The CRL path is valid
  - The available CRLs are readable

To validate KMS credentials and KMS compatibility

1 Run the following command:

```
nbkmiputil -kmsServer kms_server_name -port port
-certPathcert_path -privateKeyPath private_key_path
-trustStorePathtrust_store_path -validate
```

The `nbkmiputil` command validates the KMS functionality including connection to the KMS server.

It also tests operations like list keys, fetch keys, set attributes, and fetch attributes. For set attributes, you must have the 'write' permission for the KMS server. The `nbkmiputil` command also validates CA fingerprint on the server certificate that is exchanged through TLS handshake. `nbkmiputil` uses TLS 1.2 and later protocol for secure communication with external KMS server.

2 (This step is conditional). If the KMS vendor is not listed as a supported KMS vendor in the NetBackup hardware compatibility list and you want to verify the compatibility of the vendor with NetBackup, use the following command:

The command requires you to have the 'write' privileges for the external KMS server. The command creates eight Symmetric keys on the external KMS server and performs various KMIP operations to check the compatibility. After the compatibility check, you need to explicitly delete the keys that are created.

3 Check if the NetBackup primary server is compatible with the KMS vendor and it can communicate with the KMS vendor using the KMIP protocol. Run the following command:

```
nbkmiputil -kmsServer kms_server_name -port port
-certPathcert_path -privateKeyPath private_key_path
-truststorepathtrust_store_path -ekmsCheckCompat
```

It is recommended that you run the `-ekmsCheckCompat` option to check whether you can successfully configure KMS in your environment.

This option creates eight test keys on the specified KMS server that you can manually delete later.

4 If a check fails, contact Veritas Technical Support.

Configuring KMS credentials

To configure external KMS in NetBackup, you need to first configure the credentials that NetBackup uses to authenticate with the external KMS server. As part of this step, you need to specify the path for public key Infrastructure (PKI) artifacts that are required for certificate-based authentication. The following information is required:

- Certificate file path
- Keystore file path
- Trust store file path
- Passphrase or passphrase file path

Note: After external KMS configuration or keys are updated, NetBackup may take several minutes to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 minutes (for external KMS). To immediately consume a key, cache can be cleared by executing the following command on the respective media server:

```
bpclntcmd -clear_host_cache
```

To configure KMS credentials

- Run the following command:

```
nbkmscmd -configureCredential -credName credential_name -certPath
certificate_file_path -privateKeyPath private_key_file_path
-trustStorePath CA_certificate_file_path [-passphrasePath
private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN |
DISABLE] [-server master_server_name] [-description description]
```

Configuring KMS

To configure NetBackup KMS (NBKMS)

- Run the following command:

```
nbkmscmd -configureKMS -name configuration_name -type NBKMS -hmkId
host_master_key_ID_to_identify_HMK_passphrase -kpkId
key_protection_key_ID_to_identify_KPK_passphrase
[-useRandomPassphrase 0 | 1] [-enabledForBackup 0 | 1] [-priority
priority_of_KMS_server] [-server master_server_name] [-description
description]
```

To configure external KMS

- Run the following command:

```
nbkmscmd -configureKMS -name configuration_name -type KMIP -port
port_to_connect_to_external_KMS_server -kmsServerName
network_name_of_external_KMS_server -credId credential_ID |
-credName credential_name [-enabledForBackup 0 | 1] [-priority
priority_of_KMS_server] [-server master_server_name] [-description
description]
```

Creating keys in an external KMS

You can use NetBackup to create keys in an external KMS. NetBackup must have the required permissions to create keys in the external KMS.

To create keys in an external KMS

- Run the following command:

  ```
  nbkmscmd -createkey -name configuration_name -keyGroupName
  keygroup_name -keyName key_name -comment comments
  ```

  The `createKey` command creates a key in active state. For external KMS, you can have multiple active keys in a key group. NetBackup uses the latest active key. The command also sets all the required attributes for the key.

  Note: After any update in external KMS configuration or key related changes, NetBackup may take some time to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 min (for external KMS). To consume the key immediately, run the following command on the respective media server to clear the cache:

  ```
  bpclntcmd -clear_host_cache.
  ```

Workflow to configure data-in-transit encryption

This topic provides the steps to carry out data-in-transit encryption (DTE) in your NetBackup environment. The DTE configuration comprises the following two primary options:

- Global DTE mode
- Client DTE mode

Table 4-7 Workflow of DTE configuration

Step number	Step	Reference topic
Step 1	Review the configuration settings of the global DTE mode option and configure the option as per your DTE requirements	See "Configure the global data-in-transit encryption setting" on page 105.
Step 2	Review the configuration settings of the client DTE mode option and configure the option as per your DTE requirements	See "Configure the DTE mode on a client" on page 106.

Table 4-7 Workflow of DTE configuration *(continued)*

Step number	Step	Reference topic
Step 3	Review how the decision about data encryption is made based on the NetBackup operation that you want to perform and the DTE configuration settings.	See "How DTE configuration settings work in various NetBackup operations" on page 107. **Note:** If you plan to modify any existing DTE configuration settings, you must review this topic to understand the impact on the NetBackup operations.

Apart from the primary DTE configuration settings, the following settings are used in certain scenarios:

- Media server DTE mode
  See "Configure the DTE mode on the media server" on page 128.
- Backup image DTE mode
  See "Modify the DTE mode on a backup image" on page 128.
  See "DTE_IGNORE_IMAGE_MODE for NetBackup servers" on page 129.

Configure the global data-in-transit encryption setting

To configure the data-in-transit encryption (DTE) in your NetBackup environment, you need to first set the global DTE configuration setting (or global DTE mode) and then the client DTE mode.

Data-in-transit encryption decision for various NetBackup operations is carried out based on the global DTE mode, the client DTE mode, and the image DTE mode.

The supported values for the global DTE mode are as follows:

- `Preferred Off` (default): Specifies that the data-in-transit encryption is disabled in the NetBackup domain. This setting can be overridden by the NetBackup client setting.
- `Preferred On`: Specifies that the data-in-transit encryption is enabled only for NetBackup 9.1 and later clients.
  This setting can be overridden by the NetBackup client setting.
- `Enforced`: Specifies that the data-in-transit encryption is enforced if the NetBackup client setting is either 'Automatic' or 'On'. With this option selected, jobs fail for the NetBackup clients that have the data-in-transit encryption set to 'Off' and for the hosts earlier than 9.1.

Note: By default, the DTE mode for 9.1 clients is set to `Off` and for 10.0 and later clients, it is set to `Automatic`.

See "DTE_CLIENT_MODE for clients" on page 106.

RESTful API to be used for the global DTE configuration:

- GET - /security/properties
- POST - /security/properties

To set or view the global DTE mode using the NetBackup web UI

1. At the top right, select **Security > Global security**.
2. On the **Secure communication** tab, select one of the following global DTE settings:
   - `Preferred Off`
   - `Preferred On`
   - `Enforced`

Configure the DTE mode on a client

The `DTE_CLIENT_MODE` configuration option specifies the data-in-transit encryption (DTE) mode that is set on the NetBackup client.

See "DTE_CLIENT_MODE for clients" on page 106.

You can update and view the client DTE mode using the following commands:

`bpsetconfig`/`nbsetconfig` and `bpgetconfig`/`nbgetconfig`

DTE_CLIENT_MODE for clients

The `DTE_CLIENT_MODE` option specifies the data-in-transit encryption (DTE) mode that is set on the NetBackup client.

Table 4-8 DTE_CLIENT_MODE information

Usage	Description
Where to use	On NetBackup clients.

Table 4-8 DTE_CLIENT_MODE information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `DTE_CLIENT_MODE = AUTOMATIC | ON | OFF` By default, the DTE mode for 9.1 clients is set to `OFF` and for 10.0 and later clients, it is set to `AUTOMATIC`. ■ If the `DTE_CLIENT_MODE` option is set to `AUTOMATIC`, the client follows the DTE mode that is set at the global level: `Enforced`, `Preferred On`, or `Preferred Off`. ■ If the option is set to `ON`, data-in-transit encryption is enabled for the client. ■ If the option is set to `OFF`, data-in-transit encryption is disabled for the client. This setting can be used to exclude a client for encryption if the global DTE mode is set to `Preferred On`. **Note:** If the global DTE mode is set to `Enforced`, jobs fail for the NetBackup clients that have the `DTE_CLIENT_MODE` option set to 'OFF' and also for the hosts earlier than 9.1.
Equivalent UI property	No equivalent exists.

How DTE configuration settings work in various NetBackup operations

This topic provides information on how you can change the DTE configuration settings to achieve the required data-in-transit encryption with respect to various NetBackup operations.

Review the following reference topics before you modify any DTE configuration settings.

The following tables show how DTE setting (unencrypted or encrypted) is decided for a certain NetBackup workflow under different NetBackup configurations along with DTE configuration settings.

Backup

In the backup workflow, data is transferred between a media server and a client as part of a backup job.

Figure 4-1 Backup workflow

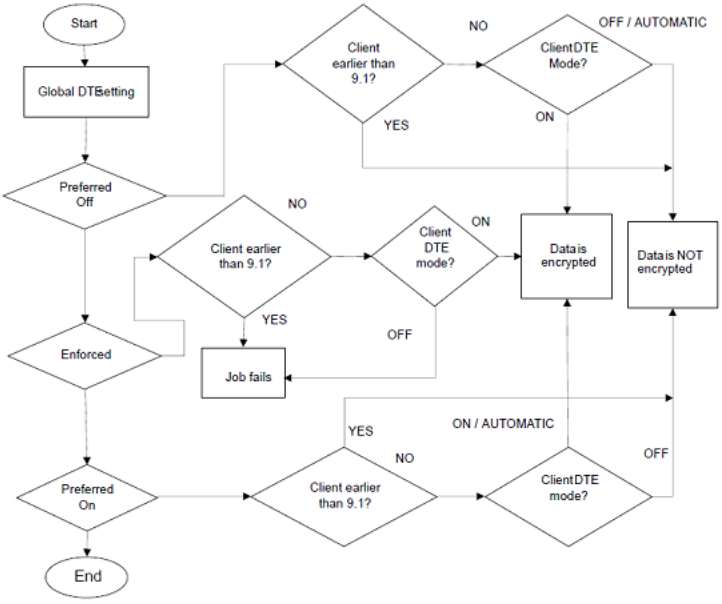


Table 4-9 The media server DTE mode is On (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted	Operation fails

Table 4-10 The media server DTE mode is Off (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails	Operation fails

Restore

In the restore workflow, there can be two DTE scenarios:

- When the image DTE mode is Off
- When the image DTE mode is On

In either of the scenarios, there can be one or more media servers involved (if multiple images are selected) while restoring data on a client for single NetBackup job.

Image DTE mode is Off

Table 4-11 Media server DTE mode is On (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted	Operation fails

Table 4-12 Media server DTE mode is Off

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted

Table 4-12 Media server DTE mode is Off *(continued)*

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred On	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails	Operation fails

Table 4-13 Mixed media servers (9.1 and 10.0 or later) - Media1: DTE mode On, Media2: DTE mode Off

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Media1 - Data is encrypted Media2 - Operation fails Job state - Partial Success Job DTE mode - On	Media1- Data is not encrypted Media2 - Data is not encrypted	Media1- Data is not encrypted Media2 - Data is not encrypted	Media1- Data is not encrypted Media2 - Data is not encrypted
Preferred On	Media1- Data is encrypted Media2- Operation fails Job state - Partial Success Job DTE mode - On	Media1- Data is not encrypted Media2 - Data is not encrypted	Media1 - Data is encrypted Media2 - Data is not encrypted Job DTE mode - Off	Media1- Data is not encrypted Media2 - Data is not encrypted
Enforced	Media1 - Data is encrypted Media2 - Operation fails Job state - Partial Success Job DTE mode - On	Media1 - Operation fails Media2 - Operation fails Job state - Fail	Media1 - Data is encrypted Media2 - Operation fails Job state - Partial Success Job DTE mode - On	Media1 - Operation fails Media2 - Operation fails Job state - Operation fails

Image DTE mode is On

If the image DTE mode is On, the default behavior is to restore with data-in-transit encryption for 9.1 and later hosts and to fail the job if any DTE unsupported host involves in the workflow . However, you can still restore by ignoring the image DTE mode.

Use the `DTE_IGNORE_IMAGE_MODE` configuration option that is to be set on the primary server. Possible values: `NEVER` (default) | `ALWAYS` | `WHERE_UNSUPPORTED`

Table 4-14 When the image DTE mode is On and the media server DTE mode is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred Off	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted

Table 4-14 When the image DTE mode is On and the media server DTE mode is On *(continued)*

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Enforced	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Operation fails
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Operation fails	Operation fails

Table 4-15 When the image DTE mode is On and the DTE setting on 10.0 and later media server is Off

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred Off	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted

Table 4-15 When the image DTE mode is On and the DTE setting on 10.0 and later media server is Off *(continued)*

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred On	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Operation fails
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Operation fails	Operation fails

Note: If the `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-12.

MSDP backup, restore, and optimized duplication

Data-in-transit encryption (DTE) feature is now integrated with MSDP storage server for backup and restore workflows.

For backup on MSDP disk pool, the encryption of data path from client to media server is controlled by the NetBackup DTE settings (global and client DTE modes).

If the MSDP storage server has multiple load balancing media servers attached to it and if the selected media server is 10.0.0.1 or later, the storage server must be 10.0.0.1 or later. Else, backup job fails. You must upgrade the 10.0 storage server

to 10.0.0.1. If the load balancing media server is 10.0 or earlier, the data may be transferred in plain text and job is always successful, even if DTE was to be honored.

Ideally, you must have load balancing media servers and storage servers with 10.0.0.1 or later when DTE is enabled.

These given conditions are also valid for the optimized duplication workflow.

In case of mixed environment, where either storage server or one of the load balancing media servers is earlier than 10.0, the following configuration will be required in order to honor an end-to-end encryption:

- DTE should be enabled from NetBackup side based on DTE configurations i.e. Global/Media Server/Client Settings
- Encryption should be enabled from MSDP side using ENCRYPTION flag in pd.conf
  See the *NetBackup Deduplication Guide* for details on enabling the encryption using MSDP.

Note: If data-in-transit encryption is enabled in NetBackup and the `ENCRYPTION` flag in `pd.conf` is also enabled, MSDP encryption takes the precedence over NetBackup DTE. It results into data-at-rest encryption and not in data-in-transit encryption.

Universal-Share policy backup

For Universal-Share policy type, client selection can either be storage server name where the Universal Share resides or the host name where the Universal Share is mounted. So the client for this policy type can be a host where the NetBackup client software is not installed.

Because of this limitation, NetBackup cannot check the client DTE mode. It checks for the global and media server DTE modes for Universal-Share policy backup and works as per the following table:

Table 4-16 DTE for Universal-Share policy backup

Global DTE mode	DTE mode of media server 9.1 or later		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Catalog backup and recovery

Media server should be of the same NetBackup version as the primary server for catalog backup and recovery workflow.

Review the following points:

- DTE mode for catalog backup jobs is similar to the file system workflow and DTE decision is similar to the backup workflow described above.
- DTE mode in catalog backup jobs:
  - Parent catalog backup job does not have DTE mode set.
  - Database staging child job does not have DTE mode set.
  - Other two child jobs have DTE mode set as per the configured DTE settings.
- DTE mode in catalog recovery jobs:
  - First 2 jobs have the DTE mode set as per the following tables depending on the image DTE mode.
  - The first two jobs replace the global DTE setting and primary server's bp.conf values, so the 3rd job DTE mode is set as per the recovered global DTE setting and primary server's bp.conf values.

The image DTE mode is Off

Table 4-17 When the image DTE mode is Off and the media server DTE setting is On

Global DTE mode	NetBackup Primary server 9.1 and later with DTE mode		
	On	**Off**	**Automatic**
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted
Enforced	Data is encrypted	Data is encrypted	Data is encrypted

Note: When the global DTE setting is set to `ENFORCED` and the `DTE_CLIENT_MODE` is Off, DTE is preferred over failure in case of catalog recovery.

Table 4-18 When the image DTE mode is Off and the media server DTE setting is Off

Global DTE mode	NetBackup Primary server 9.1 and later with DTE mode		
	On	**Off**	**Automatic**
Preferred Off	Data is encrypted *	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted *	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted *	Data is encrypted *	Data is encrypted *

* signifies that DTE is preferred over failure during catalog recovery. It ignores the DTE setting on the media server, that is Off unless the client DTE mode is set to Automatic.

The image DTE mode is On

Table 4-19 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred Off	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is not encrypted

Table 4-19 When the image DTE mode is On and the media server DTE setting is On *(continued)*

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred On	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
Enforced	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-17.

Table 4-20 When the image DTE mode is On and the media server DTE setting is Off

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is not encrypted
Preferred On	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is not encrypted
Enforced	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is encrypted *

* signifies that DTE is preferred over failure during catalog recovery. It ignores the DTE setting on the media server, that is Off unless the client DTE mode is set to Automatic.

Duplication

In the duplication workflow, a backup copy is copied from one storage unit to another storage unit, so there is no client that comes into picture. The hosts that participate are source media server and target media server from the same domain.

Table 4-21 The image DTE mode is Off

Global DTE mode	Both media servers are 9.1 or later with DTE mode		One of the media servers is earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-22 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Both NetBackup media servers 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	Both NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	Both NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-21.

Table 4-23 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Synthetic backup

A synthetic backup can be a synthetic full or a synthetic cumulative backup. The images that are used to create the synthetic image are known as component images. For instance, the component images in a synthetic full backup are the previous full image and the subsequent incremental images. A typical NetBackup backup process accesses the client to create a backup. A synthetic backup is a backup image created without using the client. Instead, a synthetic backup process creates a full or a cumulative incremental image by using previously created backup images called component images. In the synthetic backup workflow, images are fetched from different source storage units, synthesized, and copied to a target storage unit.

The hosts that come into the picture are source media servers and target media server from the same domain.

Table 4-24 DTE mode is OFF in the image

Global DTE mode	All NetBackup media server 9.1 and later with DTE mode		Any NetBackup media server earlier than 9.1
	On	**Off**	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-25 When DTE mode is On for any one of the images and media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-24.

Table 4-26 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-24.

Note:

Verify

In the verification workflow, backup image header is read, and its integrity is checked with the catalog. Therefore, a client does not come into picture. The hosts that participate are media server and primary server from the same domain.

Table 4-27 The image DTE mode is Off

Global DTE mode	NetBackup media server 9.1 and later with DTE mode		NetBackup media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-28 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	DTE mode of NetBackup client 9.1 or later	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Table 4-29 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Import

In the import workflow, backup image is read from the storage unit and the NetBackup catalog is created. Therefore, a client does not come into picture. The hosts that participate are the media server and the primary server from the same domain.

Note: If you want to retain the DTE controls based on the image, you must upgrade the media servers that are to be used for the import operations to NetBackup 10.0 before you perform the import operation.

The following table is applicable for all import workflows such as phase-1 import, phase-2 import and Storage Lifecycle Policy (SLP) import.

Table 4-30 DTE mode is OFF in the image

Global DTE mode	Media server 9.1 or later with DTE mode		Media server earlier than 9.1
	On	**Off**	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-31 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup media server earlier than 9.1	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: For phase-1 import, you need to set `DTE_IGNORE_IMAGE_MODE` on the media server to ignore the DTE mode of the image for 9.1 and later media servers.

For phase-1 import scenario, NetBackup media server earlier than 9.1 is not aware of the DTE mode in the image. If the image was created with the DTE mode set to On, for phase-1 import, the job does not fail for media servers with version earlier than 9.1 and the image DTE mode is set to Off in the catalog.

Note: When `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, DTE decision is as per Table 4-30.

Table 4-32 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted

Table 4-32 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off *(continued)*

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-30.

MSDP SLP import at target domain

In this case, the image is already replicated in the target disk pool and now the intention is to create a catalog out of that image through SLP import policy. As this operation happens in the target domain and no cross-domain operation happens, the target DTE global setting comes into the picture.

If the replicated image has the DTE mode On, then irrespective of other DTE configurations, the import operation is carried out with DTE mode On.

If the replicated image has the DTE mode Off, the DTE mode is derived based on the target domain global DTE setting and import is carried out based on the derived DTE mode.

Review the following MSDP limitations that need to be considered for this workflow:

- If the MSDP storage server has multiple load balancing media servers attached to it and if the selected media server is 10.0.0.1 or later, the storage server must be 10.0.0.1 or later. Else, backup job fails. You must upgrade the 10.0 storage server to 10.0.0.1.
  If the load balancing media server is 10.0 or earlier, the data may be transferred in plain text and job is always successful, even if DTE was to be honored.
  Ideally, you must have load balancing media servers and storage servers with 10.0.0.1 or later when DTE is enabled.
- In case of mixed environment, where either storage server or even one of the load balancing media servers is of version earlier than 10.0, the following configuration is required in order to honor end-to-end encryption:
  - DTE should be enabled from NetBackup side based on the DTE configuration settings - global / media server / client DTE mode
  - Encryption should be enabled from MSDP side using the `ENCRYPTION` flag in pd.conf

Refer to the NetBackup Deduplication Guide for details on enabling encryption using MSDP.

Note: If you set DTE On for NetBackup, but the ENCRYPTION flag in pd.conf is not enabled, the data path from the load balancing media server to the storage server is not encrypted. However, the job DTE mode and the image DTE mode may be On.

If DTE is enabled at the NetBackup side and encryption is enabled from MSDP side (`ENCRYPTION` flag in pd.conf), MSDP encryption takes the precedence over NetBackup DTE. It results in data-at-rest encryption and not data-in-transit encryption.

Replication

If the MSDP storage server is used for replication, the following considerations need to be reviewed:

- The Data-in-transit (DTE) encryption feature is not integrated with MSDP storage for replication workflows and it is controlled by the `OPTDUP_ENCRYPTION` flag in pd.conf.
- The job DTE mode depends on the image DTE mode or the global DTE setting of the source domain.
- The correct values must be set for the DTE configuration settings and the `OPTDUP_ENCRYPTION` flag for the source and target domains.

For details on enabling encryption using MSDP, see the *NetBackup Deduplication Guide*.

Table 4-33 The image DTE mode is Off

Global DTE mode	Media server 9.1 or later with DTE mode		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted

Table 4-34 When the image DTE mode is On and media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is not encrypted
Preferred On	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is encrypted
Enforced	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is encrypted

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-33.

Table 4-35 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-33.

Configure the DTE mode on the media server

The media server setting can be used only to turn off data-in-transit encryption (DTE) for NetBackup operations.

In a NetBackup configuration where a media server is slow because of the old hardware, you can turn off the media server DTE mode so that there is no performance issue. However, it is recommended that you upgrade the old media server hardware. This setting is available for media servers with NetBackup 10.0 and later.

RESTful API to be used for the global DTE configuration:

- GET - /config/media-servers/{hostName}
- PATCH - /config/media-servers/{hostName}

To set or view the media server DTE mode

1. Ensure that you have an RBAC role with the following permissions on the media server resource:
   - View
   - Update
   - Manage access
2. Run the following command to set the media server DTE mode:

   ```
   nbseccmd -setsecurityconfig -dtemediamode off|on -mediaserver
   media_server_name
   ```
3. Run the following command to view the media server DTE mode:

   ```
   nbseccmd -getsecurityconfig -dtemediamode -mediaserver
   media_server_name
   ```

   Note: For 9.1 media servers, you can only view the DTE mode as `On`, but you cannot set it.

Modify the DTE mode on a backup image

The data-in-transit (DTE) feature of NetBackup introduces an additional image attribute (DTE mode) when a backup image is created.

Primarily, the global DTE mode and the client DTE mode decide whether the data-in-transit encryption takes place or not for a NetBackup operation. If the data

is encrypted during backup, the DTE mode attribute of the associated NetBackup image is set to `On`.

If based on the global DTE mode and the client DTE mode, the data cannot be encrypted during backup, the DTE mode attribute of the image is set to `Off`.

The image DTE mode should be honored and retained for all subsequent operations on that image. For example, restore and secondary operations like duplication, replication, import and so on. If the image DTE mode is set to On, subsequent operations always encrypt the data for DTE supported hosts.

If the host does not support DTE, then the job fails. If the image DTE mode is set to Off, the DTE for subsequent operations is decided based on the global and client DTE modes at that point of time. This is the default behavior.

In certain cases, you may want to modify the image DTE mode that was set at the time of its creation.

RESTful API to be used to modify the image DTE mode:

- PATCH - /catalog/images/{backupId}

To modify the image DTE mode

- Run the following command:

  ```
  bpimage -update -image_dtemode Off|On
  ```

  You can also change the image DTE mode using the **NetBackup Web UI > Catalog** node.

See "DTE_IGNORE_IMAGE_MODE for NetBackup servers" on page 129.

DTE_IGNORE_IMAGE_MODE for NetBackup servers

Use the `DTE_IGNORE_IMAGE_MODE` option if you do not want the data to be encrypted even if the data-in-transit encryption (DTE) mode of the backup image is enabled.

The `DTE_IGNORE_IMAGE_MODE` option is applicable for all backup images.

Table 4-36 DTE_IGNORE_IMAGE_MODE information

Usage	Description
Where to use	On NetBackup servers.

Table 4-36 DTE_IGNORE_IMAGE_MODE information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `DTE_IGNORE_IMAGE_MODE = NEVER | ALWAYS | WHERE_UNSUPPORTED` The default value of the `DTE_IGNORE_IMAGE_MODE` option is `NEVER`. ■ `NEVER` - Use this option to specify that the data-in-transit encryption takes place based on the DTE mode of the image. ■ `ALWAYS` - Use this option to specify that the DTE mode of the image is always ignored during data-in-transit encryption irrespective of whether the NetBackup host supports the encryption or not. Data-in-transit encryption takes place based on the global DTE mode and client DTE mode. ■ `WHERE_UNSUPPORTED` - Use this option if you have NetBackup hosts earlier than 9.1 in your environment and you do not want the jobs to fail for these hosts when the DTE mode is enabled for the image. With this configuration, data-in-transit encryption happens based on the global and client DTE mode settings. The image DTE mode is ignored.
Equivalent UI property	No equivalent exists.

Workflow to use external certificates for NetBackup host communication

To configure NetBackup to use external CA-signed certificates for secure communication, you should carry out the following steps in the given order:

Table 4-37 Workflow to use external certificates for NetBackup host communication

Step	Description
Step 1	Ensure the following: ■ The external certificates for the web server, primary server, and all hosts are placed at the appropriate locations. ■ In case of file-based certificates, the private key files for the external certificates are placed at the appropriate locations. See "ECA_PRIVATE_KEY_PATH for NetBackup servers and clients" on page 150. If the private keys are encrypted, passphrase files should be placed at the appropriate locations. See "ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients" on page 151. ■ The CRLs are placed at the required locations on the hosts as per their CRL configuration options and they are accessible. See "About certificate revocation lists for external CA" on page 132.
Step 2	Install the NetBackup software on the primary server (or upgrade the primary server).
Step 3	Enable the NetBackup domain to use external certificates by configuring the NetBackup web server. See "Configuring an external certificate for the NetBackup web server" on page 135.
Step 4	Configure an external certificate for the NetBackup primary server host. See "Configuring the primary server to use an external CA-signed certificate" on page 136.
Step 5	Install the NetBackup software on the media server and clients (or upgrade the media server and clients). If the primary server is configured to use external certificates, the Installer prompts you to provide external certificate information for the host.

Table 4-37 Workflow to use external certificates for NetBackup host communication *(continued)*

Step	Description
Step 6	**Note:** This step is required for the hosts (media server and clients) that have the current NetBackup software, but are not configured to use external certificate. NetBackup hosts may not have external certificate configuration because of the following reasons: ■ You did not provide the external certificate information during installation or upgrade of the host. ■ The NetBackup primary server was not configured to use external certificates during installation or upgrade of the host. Configure an external certificate for a NetBackup host (media server or client) after installation. See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 142.

About certificate revocation lists for external CA

Certificate revocation list (CRL) for an external certificate authority (CA) contains a list of digital certificates that the external CA has revoked before the scheduled expiration date and should no longer be trusted.

NetBackup supports PEM and DER formats for CRLs for external CA.

CRLs for all CRL issuers or external CAs are stored in the NetBackup CRL cache that resides on each host.

During secure communication, each NetBackup host verifies the revocation status of the peer host's external certificate with the CRL that is available in the NetBackup CRL cache, based on the `ECA_CRL_CHECK` configuration option.

See "ECA_CRL_CHECK for NetBackup servers and clients" on page 152.

The NetBackup CRL cache is updated with the required CRLs using one of the following CRL sources:

`ECA_CRL_PATH` configuration option
: A NetBackup configuration option (from `bp.conf` file on UNIX or Windows registry) that specifies the directory path where the CRLs exist.

  See "ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients" on page 154.

  See "How CRLs from ECA_CRL_PATH are used" on page 133.

CRL distribution point (CDP)	If you have not specified `ECA_CRL_PATH`, NetBackup downloads the CRLs from the URLs that are specified in the peer host certificate's CDP and caches them in the NetBackup CRL cache. See "How CRLs from CDP URLs are used" on page 134. NetBackup supports downloading CRLs from HTTP and HTTPS URLs that are specified in CDP.

The NetBackup CRL cache contains only the latest copy of a CRL for each CA (including root and intermediate CAs).

The `bpclntcmd -crl_download` service updates the CRL cache during host communication in the following scenarios irrespective of the time interval set for the `ECA_CRL_PATH_SYNC_HOURS` or `ECA_CRL_REFRESH_HOURS` options:

- When CRLs in the CRL cache are expired
- If CRLs are available in the CRL source (`ECA_CRL_PATH` or CDP), but they are missing from the CRL cache

---

Note: Once the `bpclntcmd -crl_download` service updates the CRLs in the CRL cache, it does not download the CRLs for the same CA for the next 15 min even though a valid download scenario has occurred. If you want to update the CRL within 15 min, terminate the `bpclntcmd -crl_download` service.

How CRLs from ECA_CRL_PATH are used

Use this section if you want to use `ECA_CRL_PATH` as the CRL source for the NetBackup CRL cache.

To use CRLs from ECA_CRL_PATH

1 Ensure that the CRLs for external CAs are stored in a directory and the directory path is accessible by the host.

If you have a Flex Appliance application instance, the files must be stored in the following directory on the instance: `/mnt/nbdata/hostcert/crl`

You can specify the CRL details that are required for external CA configuration during NetBackup installation or upgrade on the host.

Select one of the following certificate revocation list (CRL) options during installation or upgrade:

- **Use the CRL defined in the certificate** - No additional information is required.

- **Use the CRL at the following path** - You are prompted to provide a path to the CRL.

  If you choose to use the **Do not use a CRL** option, peer host's certificate is not verified with the CRL during host communication.

For more information, refer to the NetBackup Installation Guide.

2. Specify the CRL directory path for the `ECA_CRL_PATH` configuration option.
3. Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

   During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from `ECA_CRL_PATH`.

   By default, CRLs from the cache are updated every one hour. To change the time interval, set the `ECA_CRL_PATH_SYNC_HOURS` option to a different value.

   To manually update the CRL cache with the `ECA_CRL_PATH` CRLs, run the `nbcertcmd -updateCRLCache` command.

   To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

How CRLs from CDP URLs are used

Use this section if you want to use CRL Distribution Point (CDP) as the CRL source for the NetBackup CRL cache.

To use CRLs from CDP

1. Ensure that the `ECA_CRL_PATH` configuration option is not specified.
2. Ensure that the host can access the URLs that are specified in the peer host's CDP.
3. Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

   During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from CDP URLs.

   By default, CRLs are downloaded from the CDP after every 24 hours and updated in the CRL cache. To change the time interval, set the `ECA_CRL_REFRESH_HOURS` configuration option to a different value.

   To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

Configuring an external certificate for the NetBackup web server

Note: Before enrolling the certificate for the primary server, ensure that you complete the prerequisite steps as described in the following topic.

See "Workflow to use external certificates for NetBackup host communication" on page 130.

By default, NetBackup uses the security certificates that the NetBackup CA has issued. If you have a certificate that an external CA has issued, you can configure the NetBackup web server to use it for secure communication.

Note: Windows certificate store is not supported as certificate source for the NetBackup web server.

To configure an external certificate for the web server

1. Ensure that you have valid certificate, private key of the certificate, and trusted CA bundle.
2. Run the following command:

   `configureWebServerCerts -addExternalCert -nbHost -certPath` *`certificate path`* `-privateKeyPath` *`private key path`* `-trustStorePath` *`CA bundle path`* `[-passphrasePath` *`passphrase file path`*`]`

   The `configureWebServerCerts` command does not support use of Windows certificate store paths.

   Refer to the NetBackup Commands Reference Guide for more details on the command-line options.

   - In a clustered setup, to avoid a failover run the following command on the active node:

     `install_path``/netbackup/bin/bpclusterutil -freeze`
3. Restart the NetBackup Web Management Console service to reflect the changes.

   On UNIX, run the following commands:

   - *`install_path`*`/netbackup/bin/nbwmc -terminate`
   - *`install_path`*`/netbackup/bin/nbwmc start`

   On Windows, use the **Services** application in the **Windows Control Panel**.

   Location of the commands:

Windows	*install_path*\NetBackup\wmc\bin\install\
UNIX	*install_path*/wmc/bin/install

- In a clustered setup, unfreeze the cluster using the following command on the active node:
  install_path/netbackup/bin/bpclusterutil -unfreeze

4. Restart the NetBackup Messaging Queue Broker (`nbmqbroker`) service as follows:

   On Windows:

   Go to the **Services** application in the **Windows Control Panel** and manually restart the NetBackup Messaging Queue Broker service.

   On UNIX:

   Run the following command:

   ```
   nbmqbroker stop; nbmqbroker start
   ```

5. Verify that you can access the NetBackup web user interface using a browser, without a certificate warning message.

Configuring the primary server to use an external CA-signed certificate

A NetBackup host ID-based certificate is deployed on the primary server during installation or upgrade. You can configure the primary server to use an external CA-signed certificate after installation. It includes:

- Defining the external certificate configuration options
  See "Configuration options for external CA-signed certificates" on page 145.
- Enrolling the external certificate for the primary server host
  The enrolled certificate is used for communication between the host and the primary server domain that is listed in the `SERVER` configuration option on the host.

See "Configuring an external certificate for a clustered primary server" on page 138.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configuring an external certificate for the NetBackup web server" on page 135.

- External certificates for the NetBackup web server and the primary server must be issued by the same root certificate authority.
  If the two certificate authorities do not match, communication between the **NetBackup Administration Console** and the NetBackup Web Management Console service (`nbwmc` service) fails.
- Ensure that the certificate revocation lists (CRLs) for the external CA are stored at the required location.
  If CRL distribution point (CDP) is used, ensure that the URLs that are specified in the CDP are accessible.
  See "About certificate revocation lists for external CA" on page 132.
- When NetBackup primary server is configured to use the service user (non-privileged user on UNIX and Local Service on Windows) to start most of the daemons or services, you must ensure that the following ECA paths are accessible to the service user:
  - ECA_CERT_PATH
  - ECA_PRIVATE_KEY_PATH
  - ECA_TRUST_STORE_PATH
  - ECA_KEY_PASSPHRASEFILE (optional)
  - ECA_CRL_PATH (optional)

  To grant access to the service user, do the following:
  On Unix, use the `chmod` or the `chown` command.
  On Windows run the following command:
  install_path`\NetBackup\bin\goodies\nbserviceusercmd.exe -addAcl` *ECA path* `-reason` *reason*

To configure the primary server to use an external certificate

1 Update the NetBackup configuration file (`bp.conf` file on UNIX or Windows registry) on the primary server with the external certificate-specific parameters.

See "Configuration options for external CA-signed certificates" on page 145.

For Windows certificate store	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) ■ ECA_DR_BKUP_WIN_CERT_STORE (optional)

For file-based certificates	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_PRIVATE_KEY_PATH ■ ECA_TRUST_STORE_PATH ■ ECA_KEY_PASSPHRASEFILE (optional) ■ ECA_CRL_CHECK (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) **Note:** If you have a Flex Appliance application instance, the certificate files must be stored in the following directories on the instance: ECA_CERT_PATH, ECA_PRIVATE_KEY PATH, and ECA_TRUST_STORE_PATH: `/mnt/nbdata/hostcert/` ECA_CRL_PATH: `/mnt/nbdata/hostcert/crl`

2 Run the following command on the primary server to enroll an external certificate with the primary server domain that is defined in the `SERVER` option:

```
nbcertcmd -enrollCertificate
```

For more details on the command, refer to the NetBackup Commands Reference Guide.

Configuring an external certificate for a clustered primary server

Use this section to configure an external CA-signed certificate for a clustered primary server. The enrolled certificate is used for host communication.

Requirements

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configuring an external certificate for the NetBackup web server" on page 135.
- Ensure that external certificates for the NetBackup web server and the virtual name are issued by the same certificate authority.
  If the two certificate authorities do not match, communication between the **NetBackup Administration Console** and the NetBackup Web Management Console service (`nbwmc` service) fails.

To enroll an external certificate for a clustered primary server

1. Update the NetBackup configuration file that is present on the shared disk (`nbcl.conf`) with the external certificate configuration options.

   See "Configuration options for external CA-signed certificates for a virtual name" on page 139.

   Use the `nbsetconfig` command to configure the following options:

   - `CLUSTER_ECA_CERT_PATH`
   - `CLUSTER_ECA_TRUST_STORE_PATH`
   - `CLUSTER_ECA_PRIVATE_KEY_PATH`
   - `CLUSTER_ECA_KEY_PASSPHRASEFILE` (optional)

   You need to configure the certificate revocation list (CRL) configuration options for each node.

   See "About certificate revocation lists for external CA" on page 132.

2. Run the following command on the primary server:

   ```
   nbcertcmd -enrollCertificate -cluster
   ```

   The enrolled certificate is used for communication between the active node and the primary server domain that is listed in the `SERVER` configuration option on the host.

   For more details on the command, refer to the *NetBackup Commands Reference Guide*.

3. Configure an external certificate on each cluster node.

   See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 142.

Configuration options for external CA-signed certificates for a virtual name

To configure a clustered NetBackup primary server to use external CA-signed certificate for host communication, you must define certain configuration options in the `nbcl.conf` file.

CLUSTER_ECA_CERT_PATH for clustered primary server

The `CLUSTER_ECA_CERT_PATH` option is specific to clustered primary server. It specifies the path to the external CA-signed certificate of the virtual name.

Table 4-38 CLUSTER_ECA_CERT_PATH information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `CLUSTER_ECA_CERT_PATH = Path to the certificate of the virtual identity`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

CLUSTER_ECA_TRUST_STORE_PATH for clustered primary server

The `CLUSTER_ECA_TRUST_STORE_PATH` option is specific to clustered primary server. It specifies the path to the certificate bundle file that contains all trusted root CA certificates in PEM format.

Table 4-39 CLUSTER_ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `CLUSTER_ECA_TRUST_STORE_PATH = Path to the external CA certificate`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

CLUSTER_ECA_PRIVATE_KEY_PATH for clustered primary server

The `CLUSTER_ECA_PRIVATE_KEY_PATH` option is specific to clustered primary server. It specifies the path to the private key for the external CA-signed certificate of the virtual name.

If the virtual name certificate's private key is encrypted, you should define the `CLUSTER_ECA_KEY_PASSPHRASEFILE` option.

See "CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered primary server" on page 141.

Table 4-40 CLUSTER_ECA_PRIVATE_KEY_PATH information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `CLUSTER_ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered primary server

The `CLUSTER_ECA_KEY_PASSPHRASEFILE` option is specific to clustered primary server. It specifies the path to the text file where the passphrase for the virtual name certificate's private key is stored.

`CLUSTER_ECA_KEY_PASSPHRASEFILE` is optional. You should define this option if the virtual name certificate's private key is encrypted.

See "CLUSTER_ECA_PRIVATE_KEY_PATH for clustered primary server" on page 140.

Table 4-41 CLUSTER_ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On clustered primary server.

Table 4-41 CLUSTER_ECA_KEY_PASSPHRASEFILE information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `CLUSTER_ECA_KEY_PASSPHRASE_FILE = Path to the passphrase file`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation

A NetBackup host (media server or client) is configured to use an external certificate during installation or upgrade. You may choose to do the configuration after installation.

Use this section to configure a host to use an external certificate.

You can use this section to configure an external certificate for a cluster node.

The configuration steps include:

- Defining the external certificate configuration options
  See "Configuration options for external CA-signed certificates" on page 145.
- Ensuring that automatic enrollment is enabled - `ECA_DISABLE_AUTO_ENROLLMENT` is set to `TRUE` - or enrolling the external certificate manually for the host
  See "Enrolling an external certificate for a remote host" on page 144.
  The enrolled certificate is used for communication between the host and the primary server domain that is listed in the `SERVER` configuration option on the host.

The enrolled certificate is used for host communication.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configuring an external certificate for the NetBackup web server" on page 135.

- It is recommended that you enroll an external certificate for the primary server host before you enroll one for other hosts.
  See "Configuring the primary server to use an external CA-signed certificate" on page 136.
- Ensure that the certificate revocation lists (CRLs) for the external CA are stored at the required location.
  If CRL distribution point (CDP) is used, ensure that the URLs that are specified in the CDP are accessible.
  See "About certificate revocation lists for external CA" on page 132.

To configure a host (media server or client) to use an external certificate

1. Update the configuration file (`bp.conf` file or Windows registry) with the required external certificate-specific parameters on the host:

   See "Configuration options for external CA-signed certificates" on page 145.

For Windows certificate store	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) ■ ECA_DR_BKUP_WIN_CERT_STORE (optional)

For file-based certificates	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_PRIVATE_KEY_PATH ■ ECA_TRUST_STORE_PATH ■ ECA_KEY_PASSPHRASEFILE (optional) ■ ECA_CRL_CHECK_LEVEL (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) **Note:** If you have a Flex Appliance application instance, the certificate files must be stored in the following directories on the instance: ECA_CERT_PATH, ECA_PRIVATE_KEY PATH, and ECA_TRUST_STORE_PATH: `/mnt/nbdata/hostcert/` ECA_CRL_PATH: `/mnt/nbdata/hostcert/crl`

2 Ensure that the `ECA_DISABLE_AUTO_ENROLLMENT` option is set to `TRUE` using the `nbgetconfig` command. This ensures that automatic enrollment is enabled.

If the option is disabled and you want to manually enroll the certificate, run the following command on the host to enroll an external certificate with the primary server domain that is defined in the `SERVER` configuration option on the host:

```
nbcertcmd -enrollCertificate
```

For more details on the command, refer to the *NetBackup Commands Reference Guide*.

Enrolling an external certificate for a remote host

Use this section to enroll an external certificate for a NetBackup host remotely. This lets the security administrator to enroll external certificate for multiple remote hosts from the same host.

To enroll an external certificate for a remote host (or to perform an enrollment sync operation on a remote host), ensure that the server from which you want to enroll the certificate is listed in the `SERVER` configuration option on the remote host.

To enroll certificate for a remote host

◆ Run the following command on the local host:

```
nbcertcmd -enrollCertificate -remoteHost remote_host_name -server
primary_server_name
```

An external certificate is enrolled for the specified remote host with the primary server that you provide with the `-server` option. This primary server must be available in the remote host's `SERVER` configuration option.

See "Configuration options for external CA-signed certificates" on page 145.

For more details on the commands, refer to the *NetBackup Commands Reference Guide*.

Configuration options for external CA-signed certificates

To configure a NetBackup primary server, media server, or client to use external CA-signed certificate for host communication, you must define certain configuration options in the NetBackup configuration file (`bp.conf` on UNIX platform or Windows registry).

About the mandatory and optional configuration options

- For external certificate configuration, for file-based certificates, the following configuration options are mandatory:
  - `ECA_CERT_PATH`
  - `ECA_TRUST_STORE_PATH`
  - `ECA_PRIVATE_KEY_PATH`
    If the private key of the external certificate is encrypted, `ECA_KEY_PASSPHRASEFILE` is also mandatory:
- For Windows certificate store, the following configuration options are mandatory:
  - `ECA_CERT_PATH`
- The following options are optional:
  - `ECA_CRL_CHECK`
    If the option is set to `DISABLE` (or `0`) the `ECA_CRL_PATH` option is ignored and revocation status of a peer host's certificate is not verified.
    If the option is set to a value other than `DISABLE` and `0`, revocation status of a peer host's certificate is verified based on `ECA_CRL_PATH`.
  - `ECA_DR_BKUP_WIN_CERT_STORE`
    For Windows certificate store, specify this option if you want to backup the external certificates during catalog backup.
  - `ECA_CRL_PATH_SYNC_HOURS`
    This option is used when `ECA_CRL_CHECK` is enabled and `ECA_CRL_PATH` is defined.

- ECA_CRL_REFRESH_HOURS

  This option is used when ECA_CRL_CHECK is enabled, but ECA_CRL_PATH is not defined (when CDP is used as a CRL source).

See "About certificate revocation lists for external CA" on page 132.

ECA_CERT_PATH for NetBackup servers and clients

The ECA_CERT_PATH option specifies the path to the external CA-signed certificate of the host. This option is mandatory.

NetBackup supports the following certificate sources for host certificates:

- Windows certificate store

  Note: The Windows certificate store is not supported for clustered primary servers.

- File-based certificates

Certificate order in the certificate file

A certificate file must have a certificate chain with certificates in the correct order. The chain starts with the server certificate (also known as the leaf certificate) and is followed by zero or more intermediate certificates. The chain must contain all intermediate certificates up to the Root CA certificate but should not contain the Root CA certificate itself. The chain is created such that each certificate in the chain signs the previous certificate in the chain.

The certificate file should be in one of the following formats:

- PKCS #7 or P7B file that is either DER or PEM encoded that has certificates in the specified order
- A file with the PEM certificates that are concatenated together in the specified order

Table 4-42 ECA_CERT_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-42 ECA_CERT_PATH information *(continued)*

Usage	Description

How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	For file-based certificates, use the following format:
	`ECA_CERT_PATH = Path to the external certificate of the host`
	For example: `c:\server.pem`
	If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/`.
	For Windows certificate store, use the following format:
	`ECA_CERT_PATH = Certificate store name\Issuer name\Subject name`
	You can specify multiple certificate selection queries in a comma-separated format.
	`ECA_CERT_PATH = Store name1\Issuer name1\Subject name1,Store name2\Issuer name2\Subject name2`
	See "Specifying Windows certificate store for ECA_CERT_PATH" on page 147.

Equivalent UI property	No equivalent exists.

Specifying Windows certificate store for ECA_CERT_PATH

NetBackup selects a certificate from any of the local machine certificate stores on a Windows host.

In case of Windows certificate store, `ECA_CERT_PATH` is a list of comma-separated clauses.

Each clause is of the form *Store name**Issuer**Subject*. Each clause element contains a query.

`$hostname` is a keyword that is replaced with the fully qualified domain name of the host. Use double quotes when a `\` is present in the actual path. For example, `MY\Veritas\"NetBackup\$hostname"`.

`$shorthostname` is a keyword that is replaced with the short name of the host. Use double quotes when a `\` is present in the actual path. For example, `MY\Veritas\"NetBackup\$shorthostname"`.

The 'Store name' should be the exact name of the store where the certificate resides. For example: 'MY'

The 'Issuer' is optional. If this is provided, NetBackup picks the certificates for which the Issuer DN contains the provided substring.

The 'Subject' is mandatory. NetBackup picks the certificate for which the Subject DN contains the provided substring.

You must ensure to:

- Add the root certificate to Trusted Root Certification Authorities or Third-Party Root Certification Authorities in the Windows certificate store.
- If you have any intermediate CAs, add their certificates to the Intermediate Certification Authorities in the Windows certificate store.

Example - Certificate locations with WHERE CLAUSE:

- `My\Veritas\$hostname, My\ExampleCompany\$hostname`
  Where (certificate store is MY, Issuer DN contains `Veritas`, Subject DN contains `$hostname`) OR (certificate store name is `MY`, Issuer DN contains `ExampleCompany`, Subject DN contains `$hostname`)
- `MY\Veritas\"NetBackup\$hostname"`
  Where certificate store name is `MY`, Issuer DN contains `Veritas`, Subject DN contains `NetBackup\$hostname`
- `MY\\$hostname`
  Where certificate store name is `MY`, any Issuer DN, Subject DN contains `$hostname`
- `MY\\$shorthostname`
  Where certificate store name is `MY`, any Issuer DN, Subject DN contains `$shorthostname`
- `MY\Veritas\NetBackup $hostname`
  Where certificate store name is `MY`, Issuer DN contains `Veritas`, Subject DN contains `NetBackup $hostname`

If you provide a space between words, it is considered as a valid character.

Example - Certificate locations with invalid data:

- `MY\\`
  The Subject DN should have some value.
- `My\$hostname`
  The Subject DN should have some value.

- `\\$hostname`

  The certificate store name should have exact value of the store in which the certificate resides.

- `MY\CN=Veritas\CN=$hostname`

  The Subject DN and issuer DN cannot contain =, and also specific tags like CN=.

ECA_TRUST_STORE_PATH for NetBackup servers and clients

The `ECA_TRUST_STORE_PATH` option specifies the file path to the certificate bundle file that contains all trusted root CA certificates.

This certificate file should have one or more certificates in PEM format.

Do not specify the `ECA_TRUST_STORE_PATH` option if you use the Windows certificate store.

The trust store supports certificates in the following formats:

- PKCS #7 or P7B file having certificates of the trusted root certificate authorities that are bundled together. This file may either be PEM or DER encoded.
- A file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.

This option is mandatory for file-based certificates.

The root CA certificate in Cloudera distribution can be obtained from the Cloudera administrator. It may have a manual TLS configuration or an Auto-TLS enabled for the Hadoop cluster. For both cases, NetBackup needs a root CA certificate from the administrator.

The root CA certificate from the Hadoop cluster can validate the certificates for all nodes and allow NetBackup to run the backup and restore process in case of the secure (SSL) cluster. This root CA certificate is a bundle of certificates that has been issued to all such nodes.

Certificate from root CA must be configured under `ECA_TRUST_STORE_PATH` in case of self-signed, third party CA or Local/Intermediate CA environments. For example: In case of AUTO-TLS enabled Cloudera environments, you can typically find the root CA file named with `cm-auto-global_cacerts.pem` at path `/var/lib/cloudera-scm-agent/agent-cert`. For more details, refer Cloudera documentation.

Table 4-43 ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, Red Hat Virtualization servers, or Nutanix AHV, this option must be set on the NetBackup primary server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_TRUST_STORE_PATH = Path to the external CA certificate` For example: `c:\rootCA.pem` If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/`.
Equivalent UI property	No equivalent exists.

ECA_PRIVATE_KEY_PATH for NetBackup servers and clients

The `ECA_PRIVATE_KEY_PATH` option specifies the file path to the private key for the external CA-signed certificate of the host.

This option is mandatory for file-based certificates.

If the private key of the certificate is encrypted, you should specify the `ECA_KEY_PASSPHRASEFILE` option.

See "ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients" on page 151.

NetBackup supports PKCS #1 and PKCS #8 formatted private keys that are either plain text or encrypted. These may either be PEM or DER encoded. However, if it is PKCS #1 encrypted, it must be PEM encoded.

For encrypted private keys, NetBackup supports the following encryption algorithms:

- DES, 3DES, and AES if the private key is in the PKCS #1 format
- DES, 3DES, AES, RC2, and RC4 if the private key is in the PKCS #8 format

Note: You should not specify the `ECA_PRIVATE_KEY_PATH` option if Windows certificate store is specified for the `ECA_CERT_PATH` option.

See "ECA_CERT_PATH for NetBackup servers and clients" on page 146.

Table 4-44 ECA_PRIVATE_KEY_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate` For example: `c:\key.pem` If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/`.
Equivalent UI property	No equivalent exists.

ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients

The `ECA_KEY_PASSPHRASEFILE` option specifies the path to the text file where the passphrase for the external certificate's private key is stored.

You should specify the `ECA_KEY_PASSPHRASEFILE` option only if the certificate's private key is encrypted.

See "ECA_PRIVATE_KEY_PATH for NetBackup servers and clients" on page 150.

Note: You should not specify the `ECA_KEY_PASSPHRASEFILE` option if you use Windows certificate store.

See "ECA_CERT_PATH for NetBackup servers and clients" on page 146.

Note: Do not use the ECA_KEY_PASSPHRASEFILE on the MSDP servers that are used for MSDP direct cloud tiering as it is not supported with MSDP direct cloud tiering.

Table 4-45 ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_KEY_PASSPHRASEFILE = Path to the passphrase file`
Equivalent UI property	No equivalent exists.

ECA_CRL_CHECK for NetBackup servers and clients

The `ECA_CRL_CHECK` option lets you specify the revocation check level for external certificates of the host. It also lets you disable the revocation check for the external certificates. Based on the check, revocation status of the certificate is validated against the Certificate Revocation List (CRL) during host communication.

You can choose to use the CRLs from the directory that is specified for the `ECA_CRL_PATH` configuration option in the configuration file (`bp.conf` on UNIX or Windows registry) or the CRL Distribution Point (CDP).

See "ECA_CRL_PATH for NetBackup servers and clients" on page 153.

Table 4-46 ECA_CRL_CHECK information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-46 ECA_CRL_CHECK information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_CRL_CHECK = CRL check` You can specify one of the following: ■ DISABLE (or 0) - Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication. ■ LEAF (or 1) - Revocation status of the leaf certificate is validated against the CRL. This is the default value. ■ CHAIN (or 2) - Revocation status of all certificates from the certificate chain are validated against the CRL.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_PATH for NetBackup servers and clients

The `ECA_CRL_PATH` option specifies the path to the directory where the Certificate Revocation Lists (CRL) of the external certificate authority (CA) are located.

These CRLs are copied to NetBackup CRL cache. Revocation status of the external certificate is validated against the CRLs from the CRL cache.

CRLs in the CRL cache are periodically updated with the CRLs in the directory that is specified for `ECA_CRL_PATH` based on the `ECA_CRL_PATH_SYNC_HOURS` option.

If the `ECA_CRL_CHECK` or `HADOOP_CRL_CHECK` option is not set to `DISABLE` (or 0) and the `ECA_CRL_PATH` option is not specified, NetBackup downloads the CRLs from the URLs that are specified in the CRL distribution point (CDP) and uses them to verify revocation status of the peer host's certificate.

Note: For validating the revocation status of a virtualization server certificate, the `VIRTUALIZATION_CRL_CHECK` option is used.

For validating the revocation status of a Hadoop server certificate, the `HADOOP_CRL_CHECK` option is used.

Table 4-47 ECA_CRL_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, Red Hat Virtualization servers, Nutanix AHV, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA). If certificate validation is required for VMware, Red Hat Virtualization servers, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format to specify a path to the CRL directory: `ECA_CRL_PATH = Path to the CRL directory` If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/crl`.
Equivalent UI property	No equivalent exists.

ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients

The `ECA_CRL_PATH_SYNC_HOURS` option specifies the time interval in hours to update the Certificate revocation lists (CRL) in the NetBackup CRL cache with the CRLs in the directory specified for the `ECA_CRL_PATH` configuration option.

See "ECA_CRL_PATH for NetBackup servers and clients" on page 153.

The `ECA_CRL_PATH_SYNC_HOURS` option is not applicable if CDP is used for CRLs.

By default, CRLs in the cache are updated every one hour.

During host communication, revocation status of the external certificate is validated against the CRLs from the CRL cache.

Table 4-48 ECA_CRL_PATH_SYNC_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_CRL_PATH_SYNC_HOURS = Number of hours` Minimum number of hours that you can specify - 1 hour Maximum number of hours that you can specify - 720 hour The default value is one hour.
Equivalent UI property	No equivalent exists.

ECA_CRL_REFRESH_HOURS for NetBackup servers and clients

The `ECA_CRL_REFRESH_HOURS` option specifies the time interval in hours to download the CRLs from the URLs that are specified in the peer host certificate's CRL distribution points (CDP).

The `ECA_CRL_REFRESH_HOURS` option is applicable when you use CDP for CRLs.

See "ECA_CRL_PATH for NetBackup servers and clients" on page 153.

After the specified time interval, CRLs of the certificate authority are downloaded from the URLs that are available in CDP.

By default, the CRLs are downloaded from the CDP after every 24 hours.

Table 4-49 ECA_CRL_REFRESH_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-49 ECA_CRL_REFRESH_HOURS information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_CRL_REFRESH_HOURS = Number of hours` Minimum number of hours that you can specify - 0 hour, which indicates that CRLs from the CDP are not periodically downloaded. Maximum number of hours that you can specify - 4380 hours The default value for the option is 24 hours. **Note:** CRLs are also downloaded from the CDP during host communication if they are expired or not available in the CRL cache, irrespective of the time interval set for the `ECA_CRL_REFRESH_HOURS` option.
Equivalent UI property	No equivalent exists.

ECA_DISABLE_AUTO_ENROLLMENT for NetBackup servers and clients

When NetBackup is configured to use the certificates that an external CA has signed, such certificates are automatically enrolled with the primary server during host communication. If you want to disable automatic enrollment of such certificates, set the `ECA_DISABLE_AUTO_ENROLLMENT` to '1'.

When automatic enrollment is disabled, you can enroll the external certificates manually using the `nbcertcmd -enrollCertificate` command.

A certificate must be enrolled with the primary server before it can be used for host communication.

By default, automatic certificate enrollment is enabled.

Table 4-50 ECA_DISABLE_AUTO_ENROLLMENT information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-50 ECA_DISABLE_AUTO_ENROLLMENT information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_DISABLE_AUTO_ENROLLMENT = 1`
Equivalent UI property	No equivalent exists.

ECA_DR_BKUP_WIN_CERT_STORE for NetBackup servers and clients

The `ECA_DR_BKUP_WIN_CERT_STORE` option specifies whether you want to take a backup of the Windows certificate store information during catalog backup or not.

By default, Windows certificate store information is backed up during catalog backup.

Note: If the Windows certificate store information is not exportable, it cannot be backed up during catalog backup.

Table 4-51 ECA_DR_BKUP_WIN_CERT_STORE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. If you do not want the catalog backup operation to take a backup of the Windows certificate store information, use the following format: `ECA_DR_BKUP_WIN_CERT_STORE = NO`
Equivalent UI property	No equivalent exists.

MANAGE_WIN_CERT_STORE_PRIVATE_KEY option for NetBackup primary servers

The MANAGE_WIN_CERT_STORE_PRIVATE_KEY option lets you disable the automatic permission management of the private key of the certificate in Windows Certificate Store.

This option is applicable for Windows Certificate Store and only when the NetBackup services are running in the Local Service account context.

When NetBackup services are running in the Local Service account context, the services need to have permissions to read the private key for certificate in Windows Certificate Store.

When the MANAGE_WIN_CERT_STORE_PRIVATE_KEY option is set to Automatic, the NetBackup service that is running in the privileged user account context grants access to all other NetBackup services for reading the private key whenever required.

By default, permissions for the private key are automatically managed. When the MANAGE_WIN_CERT_STORE_PRIVATE_KEY option is set to Disabled, the permissions of the private key need to be managed manually.

Note: It is not recommended to set the MANAGE_WIN_CERT_STORE_PRIVATE_KEY option to Disabled.

To manually update the permissions when this option is Disabled, run the following command:

```
nbcertcmd -setWinCertPrivKeyPermissions -reason audit reason -force
```

Refer to the NetBackup Commands Reference Guide for more details on the command-line options.

Table 4-52 MANAGE_WIN_CERT_STORE_PRIVATE_KEY information

Usage	Description
Where to use	On NetBackup primary server.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: MANAGE_WIN_CERT_STORE_PRIVATE_KEY = Automatic

Table 4-52 MANAGE_WIN_CERT_STORE_PRIVATE_KEY information *(continued)*

Usage	Description
Equivalent UI property	No equivalent exists.

Guidelines for managing the primary server NetBackup catalog

Consider the following:

- Back up the catalog.
  Catalog backup can be performed while regular backup activity takes place. It is a policy-based backup. It also allows for incremental backups, which can significantly reduce catalog backup times for large catalogs.

  Warning: Failure to backup the primary server NetBackup catalog may result in data loss if a catastrophic failure occurs to the file systems housing the various parts of the catalog.

  Note: Veritas recommends schedule-based, incremental catalog backups with periodic full backups.

  Be cautious in using Accelerator full backups daily as a replacement for daily incremental backups. While Accelerator full backups are quick to run, the catalog size will be a full catalog backup instead of an incremental and can grow quickly in size. Backups of client data that contain millions of small files in combination with the use of Accelerator and frequent full backups can also cause the catalog to bloat.

- Store the catalog on a separate file system.
  The primary server NetBackup catalog can grow quickly depending on backup frequency, retention periods, and the number of files being backed up. With the catalog data on its own file system, catalog growth does not affect other disk resources, root file systems, or the operating system.
  Information is available on how to move the catalog.
  The following directories and files that are related to the catalog can also be moved. Using an SSD device also improves performance:

  On a Linux/UNIX host:

- `/usr/openv/netbackup/db/error` (directory)
- `/usr/openv/netbackup/db/images` (directory)
- `/usr/openv/netbackup/db/jobs` (directory)
- `/usr/openv/netbackup/db/rb.db` (file)

On a Windows host:

- `C:\Program Files\VERITAS\NetBackup\db\error` (directory)
- `C:\Program Files\VERITAS\NetBackup\db\images` (directory)
- `C:\Program Files\VERITAS\NetBackup\db\jobs` (directory)
- `C:\Program Files\VERITAS\NetBackup\db\rb.db` (file)

- Change the location of the NetBackup relational database files.
  The location of the NetBackup relational database files can be changed or split into multiple directories, for better performance. For example, by placing the transaction log file (`NBDB.log`) on a physically separate drive, you gain better protection against disk failure and increased efficiency in writing to the log file. The following directories and files that are related to the catalog can also be moved. Using an SSD device also improves performance:

  On a Linux/UNIX host:

  - `/usr/openv/tmp` (directory)
  - `/usr/openv/var` (directory)
  - `/usr/openv/db/data` (directory)
  - `/usr/openv/db/staging` (directory)

  On a Windows host:

  - `C:\Program Files\VERITAS\NetBackup\Temp` (directory)
  - `C:\Program Files\VERITAS\NetBackup\var` (directory)
  - `C:\Program Files\VERITAS\NetBackupDB\data` (directory)
  - `C:\Program Files\VERITAS\NetBackupDB\staging` (directory)

  Refer to the procedure in the "NetBackup relational database" appendix of the *NetBackup Administrator's Guide, Volume I*.

- Set a delay to compress the catalog.
  The default value for this parameter is 0, which means that NetBackup does not compress the catalog. As your catalog increases in size, you may want to use a value between 10 days and 30 days for this parameter. When you restore old backups, NetBackup automatically uncompresses the files as needed, with minimal performance effect.

- Adjust the batch size for sending metadata to the catalog.
  This setting affects overall backup performance, not the performance of catalog backups.
- Best practices for primary server NetBackup catalog layout:
  https://www.veritas.com/content/support/en_US/article.100003918

About protecting the MSDP catalog

To increase availability, NetBackup provides a two-tier approach to protect the MSDP catalog, as follows:

Daily shadow copies	NetBackup automatically creates copies of the MSDP catalog. See "About the MSDP shadow catalog" on page 161.
Catalog backup policy	Veritas provides a utility that you can use to configure a NetBackup policy that backs up the MSDP catalog. See "About the MSDP catalog backup policy" on page 165.

About the MSDP shadow catalog

The NetBackup Deduplication Manager automatically creates a *shadow copy* of the catalog daily. The Deduplication Manager also builds a transaction log for each shadow copy. If NetBackup detects corruption in the MSDP catalog, the Deduplication Manager restores the catalog automatically from the most recent shadow copy. That restore process also plays the transaction log so that the recovered MSDP catalog is current.

By default, the NetBackup Deduplication Manager stores the shadow copies on the same volume as the catalog itself. Veritas recommends that you store the shadow copies on a different volume.

Warning: You can change the path only during initial MSDP configuration only. If you change it after MSDP backups exist, data loss may occur.

See "Changing the MSDP shadow catalog path" on page 162.

The NetBackup Deduplication Manager creates a shadow copy at 0340 hours daily, host time. To change the schedule, you must change the scheduler definition file.

See "Changing the MSDP shadow catalog schedule" on page 163.

By default, the NetBackup Deduplication Manager keeps five shadow copies of the catalog. You can change the number of copies.

See "Changing the number of MSDP catalog shadow copies" on page 164.

Changing the MSDP shadow catalog path

You can change the location of the catalog shadow copies. It is recommended that you store the copies on a different volume than both the *storage_path* and the *database_path*. (If you configured a separate path for the deduplication database, the paths are different.)

NetBackup stores the MSDP catalog shadow copies in the following location:

UNIX: */database_path*/databases/catalogshadow

Windows: *database_path*\databases\catalogshadow

Warning: You can change the shadow catalog path during initial MSDP configuration only. If you change it after MSDP backups exist, data loss may occur.

See "About protecting the MSDP catalog" on page 161.

To change the MSDP catalog shadow path

1. Open the following file in a text editor:

   UNIX: */storage_path*/etc/puredisk/spa.cfg

   Windows: *storage_path*\etc\puredisk\spa.cfg

2. Find the `CatalogShadowPath` parameter and change the value to the wanted path.

   The volume must be mounted and available.

3. After your changes, save the file.

4. Create the `.catalog_shadow_identity` file in the catalog shadow path that you have specified in step 1.

   Note: There is a period (`.`) in front of the file name that denotes a hidden file.

   ---

5. Restart the NetBackup Deduplication Manager (`spad`).

6 Create the shadow catalog directories by invoking the following command on the MSDP storage server:

UNIX: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog backup all`

Windows: *`install_path`*`\Veritas\pdde\cacontrol --catalog backup all`

7 If an MSDP catalog backup policy exists, update the policy with the new shadow catalog directories. To do so, invoke the following command on the MSDP storage server:

UNIX: `/usr/openv/pdde/pdcr/bin/drcontrol --update_policy --policy` *`policy_name`*

Windows: *`install_path`*`\Veritas\pdde\drcontrol --update_policy --policy` *`policy_name`*

Changing the MSDP shadow catalog schedule

NetBackup automatically creates a copy of the MSDP catalog at 0340 hours daily, host time. You can change the default schedule.

See "About protecting the MSDP catalog" on page 161.

To change the MSDP shadow catalog schedule

1. Open the following file in a text editor:

   UNIX: `/database_path/databases/spa/database/scheduler/5`

   Windows: `database_path\databases\spa\database\scheduler\5`

   By default, NetBackup uses the same path for the storage and the catalog; the *database_path* and the *storage_path* are the same. If you configure a separate path for the deduplication database, the paths are different.

   The contents of the file are similar to the following line. The second section of the line (`40 3 * * *`) configures the schedule.

   ```
   CatalogBackup|40 3 * * *|21600|32400|
   ```

2. Edit the second section of the file (`40 3 * * *`). The schedule section conforms to the UNIX `crontab` file convention, as follows:

   ```
   40 3 * * *
   ┬  ┬ ┬ ┬ ┬
   │  │ │ │ │
   │  │ │ │ │
   │  │ │ │ └──── Day of week (0 - 7, Sunday is both 0 and 7, or use
   │  │ │ │       sun, mon, tue, wed, thu, fri, sat; asterisk (*) is
   │  │ │ │       every day)
   │  │ │ └─────────── Month (1 - 12; asterisk (*) is every month)
   │  │ └──────────────── Day of month (1 - 31; asterisk (*) is every
   │  │                   day of the month)
   │  └────────────────────── Hour (0 - 23; asterisk (*) is every hour)
   └──────────────────────────── Minute (0 - 59; asterisk (*) is every
                                 minute of the hour)
   ```

3. After your changes, save the file.

4. Restart the NetBackup Deduplication Manager (`spad`).

Changing the number of MSDP catalog shadow copies

NetBackup keeps five shadow copies of the MSDP catalog. You can change the number of copies.

See "About protecting the MSDP catalog" on page 161.

To change the number of MSDP catalog shadow copies

1. Open the following file in a text editor:

   UNIX: `/storage_path/etc/puredisk/spa.cfg`

   Windows: `storage_path\etc\puredisk\spa.cfg`

2. Find the `CatalogBackupVersions` parameter and change the value to the wanted number of shadow copies. The valid values are 1 to 256, inclusive.
3. After your changes, save the file.
4. Restart the NetBackup Deduplication Manager (`spad`).

About the MSDP catalog backup policy

Veritas recommends that you protect the MSDP catalog by backing it up. A NetBackup catalog backup does not include the MSDP catalog. The NetBackup Deduplication Catalog Policy Administration and the Catalog disaster recovery utility (the `drcontrol` utility) configure a backup policy for the MSDP catalog. The policy also includes other important MSDP configuration information.

The MSDP catalog backups provide the second tier of catalog protection. The catalog backups are available if the shadow copies are not available or corrupt.

The following are the attributes for the catalog backup policy that the `drcontrol` utility creates:

Schedule	Weekly **Full Backup** and daily **Differential Incremental Backup**.
Backup window	6:00 A.M. to 6:00 P.M.
Retention	2 weeks

Backup selection

The following are the default catalog paths.

UNIX:

```
/database_path/databases/catalogshadow
/storage_path/etc
/database_path/databases/spa
/storage_path/var
/usr/openv/lib/ost-plugins/pd.conf
/usr/openv/lib/ost-plugins/mtstrm.conf
/database_path/databases/datacheck
```

Windows:

```
database_path\databases\catalogshadow
storage_path\etc
storage_path\var
install_path\Veritas\NetBackup\bin\ost-plugins\pd.conf
install_path\Veritas\NetBackup\bin\ost-plugins\mtstrm.conf
database_path\databases\spa
database_path\databases\datacheck
```

By default, NetBackup uses the same path for the storage and the catalog; the *database_path* and the *storage_path* are the same. If you configure a separate path for the deduplication database, the paths are different. Regardless, the `drcontrol` utility captures the correct paths for the catalog backup selections.

You should consider the following items carefully before you configure an MSDP catalog backup:

- Do not use the **Media Server Deduplication Pool** as the destination for the catalog backups. Recovery of the MSDP catalog from its **Media Server Deduplication Pool** is impossible.
- Use a storage unit that is attached to a NetBackup host other than the MSDP storage server.
- Use a separate MSDP catalog backup policy for each MSDP storage server. The `drcontrol` utility does not verify that the backup selections are the same for multiple storage servers. If the backup policy includes more than one MSDP storage server, the backup selection is the union of the backup selections for each host.
- You cannot use one policy to protect MSDP storage servers on both UNIX hosts and Windows hosts.

UNIX MSDP storage servers require a Standard backup policy and Windows MSDP storage servers require an MS-Windows policy.

How to set up malware scanning

Table 4-53 Steps for setting up malware scanning

Step description	Link
Install or upgrade NetBackup software on the primary server, the media server, and MSDP storage server to version 10.0 or later.	NetBackup Installation or Upgrade Guide
For BYO setup, Instant access must be configured on MSDP storage server.	See the "Configuring Universal share" section in Veritas NetBackup™ Deduplication Guide
Configure the required share type such as NFS or SMB. Notes: ■ Perform the following steps on MSDP storage server: ■ Configure NFS and SMB configurations. Also, NFS or SMB client must be on scan host. ■ For SMB share, ensure to obtain an active directory domain details and a valid user credentials. ■ Ensure that user specified in the share type has required permission to mount.	See the "Configuring Universal share" section in Veritas NetBackup™ Deduplication Guide
On the scan host, configure any of the following malware tool: ■ NetBackup Malware Scanner ■ Symantec Protection Engine ■ Microsoft Defender Antivirus **Note:** Ensure that the host user has required permission to scan with configured malware tool and is able to access the mount on the storage server.	See "Prerequisites for a scan host" on page 168.
On the NetBackup Web UI, configure the malware detection settings.	See "Configuring a new scan host pool" on page 169.

Prerequisites for a scan host

A scan host is a host machine that has the required malware tool configured. Once it is integrated with NetBackup, NetBackup initiates scanning on the scan host.

Ensure that you meet the following prerequisites:

- The malware tool must be installed and configured.
- The scan host must have a share type configured, that is, an NFS or SMB client.
- The scan host must be reachable from the media server over SSH.

  Note: SSH connection to scan host from the media server must be successful.

- `OpenSSH` must be configured on windows scan host.

  Note the following:

  - For Windows 2016, get OpenSSH from GIT hub repository and for Windows 2019, enable OpenSSH server feature. For more details, refer to Microsoft documentation.
  - Microsoft Visual C/C++ Redistributable is an additional dependency if media server is updated to 10.1.1.
    Visual C/C++ run-time library DLL is required to execute `nbmalwareutil` utility on windows scan host. The runtime DLL can be obtained from Microsoft Visual C++ Redistributable latest supported downloads.
- The minimum required configuration for the scan host is 8 CPU and 32-GB RAM.
- NetBackup footprint is not required on the scan host. The existing systems with the NetBackup client or media server can be used as scan host, too.
- For the supported operating systems of the scan host, refer Software Compatibility List.
- For NetBackup malware detection utility to execute on scan host, install `libnsl.so.1` library on scan host. If the latest version of `libnsl` library file is present (for example, `/usr/lib64/libnsl.so.2`), then create a softlink file `/usr/lib64/libnsl.so.1` which points to `/usr/lib64/libnsl.so.2` file.
  Example for creating softlink file:

  ```
  # cd /usr/lib64 # ln -sf libnsl.so.2 libnsl.so.1
  ```

  Note: For assistance on installing `libnsl*` library file, contact operating system administrator.

Non-root user configuration

For non-root user on Linux:

- Allow `ssh` connection using non-root user.
  For example: Add the `Allow Users root scanuser` entry in the `/etc/ssh/sshd_config` file.

  Note: Scanuser is a non-root user created in the system.

- Provide user permission to mount and umount. Add user permission entry in `sodoers` file.
  For example: In the `/etc/sudoers` file add one of the following:
  - **scanuser ALL=(ALL) NOPASSWD:ALL**
  - **scanuser ALL=(ALL) NOPASSWD:/bin/umount, /bin/mount**
- Configure malware tool using non-root user on the scan host.

  Note: If scanning is done using root user, then change the permission of the `/tmp/malware` folder to provide write permissions to the non-root user.

  Note: For example: `chmod a+rwx /tmp/malware`

Configuring a new scan host pool

1. On left, click **Detection and reporting > Malware detection**.
2. On the **Malware detection** page, select **Malware detection settings > Malware scanner host pools** on the top-right corner to go to host pool list page.

   For configuration details, see the NetBackup Security and Encryption Guide.
3. On the **Malware scanner host pools** page, click **Add** to add a new host pool.
4. On the **Add malware scanner host pools** page, enter the details such as **Host pool name**, **Malware scanner**, and **Type of share**.
5. Click **Save and add hosts**.

About backup anomaly detection

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

Note: By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.

The following backup job metadata, attributes, or features are verified during backup anomaly detection:

- Backup image size
- Number of backup files
- Data that is transferred in KB
- Deduplication rate
- Backup job completion time

Any unusual deviation in these backup job attributes is considered to be an anomaly and is notified using the NetBackup web UI.

Workflow of backup anomaly detection and notification

The workflow of the backup anomaly detection and notification is as follows:

Table 4-54 Workflow

Step	Description
Step 1	Install or upgrade NetBackup software on the primary server and the media server. See the NetBackup Installation or Upgrade Guide.
Step 2	Enable the primary server to detect backup anomalies. By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.
Step 3	Configure anomaly detection settings using the NetBackup web UI. See “Configure anomaly detection settings” on page 173.

Table 4-54 Workflow *(continued)*

Step	Description
Step 4	View the anomalies using the NetBackup web UI. See "View anomalies" on page 173.

Detecting backup anomalies on the primary server

This topic provides the procedure to enable the primary server to detect backup anomalies.

To enable the primary server to detect backup anomalies

1. Install the NetBackup primary server software on your system (or upgrade the primary server software).

   After the installation, the following configurations are automatically done on the primary server:

   - The `NetBackup Anomaly Detection Management` service (`nbanomalymgmt`) is started on the primary server.
     The anomaly detection and alert services do not run by default.

     Note: The `NetBackup Anomaly Detection Management` service stops if the proxy server takes more than 45 minutes to connect to the primary server.

2. Configure the backup anomaly settings using the NetBackup web UI. NetBackup takes these settings into account during anomaly detection.

   See "Configure anomaly detection settings" on page 173.

   If any anomalies are detected, they are notified through the NetBackup web UI.

   See "View anomalies" on page 173.

Detecting backup anomalies on the media server

This topic provides the workflow and the procedure that enable the media server to detect backup anomalies.

Note: By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.

To enable the media server to detect backup anomalies

1. Install the NetBackup media server software on your system (or upgrade the media server software).
2. On the primary server, add anomaly proxy server details. The proxy server should be the media server where you want the anomaly algorithms to be run.

   See "Configure anomaly detection settings" on page 173.
3. (Optional) If you want to preserve the data that the primary server has gathered earlier, do the following:
   - Ensure that the `nbanomalymgmt` service is disabled using the web UI.
   - Ensure that the `nbanomalymgmt` service on the media server is stopped.
   - Go to the following directory:
     On Windows: *`Install_Path`*`\NetBackup\var\global`
     On UNIX: `/usr/openv/var/global`
     The directory resides on the shared disk on a clustered primary server.
   - Copy the `NB_Anomaly.db`, `NB_Anomaly.db-shm`, and `NB_Anomaly-wal` files from the `anomaly_detection` folder on the primary server to the `anomaly_detection` folder on the media server.
     You can copy the `anomaly_config.conf` file to preserve the automatic malware scan settings.
   - Start the `nbanomalymgmt` service on the media server.
4. On the media server, start the `nbanomalymgmt` service manually. Use the following script:

   ```
   nbanomalymgmt -start
   ```
5. Configure the backup anomaly settings in the NetBackup web UI. NetBackup takes these settings into account during anomaly detection.

   See "Configure anomaly detection settings" on page 173.

   If any anomalies are detected, they are notified using the NetBackup web UI.

   See "View anomalies" on page 173.

Configure anomaly detection settings

Once you enable anomaly detection setting, anomaly data gathering, detection service, and events are enabled. Basic and advanced anomaly detection settings are available.

See “About backup anomaly detection” on page 170.

To configure anomaly detection settings

1. On the left, select **Detection and reporting > Anomaly detection**.
2. On the top right, Click **Anomalies settings**.
3. Click **Edit** on the right to configure anomaly detection settings by selecting one of the following options:
   - **Disable all**
   - **Enable anomaly data gathering**
   - **Enable anomaly data gathering and detection service**
   - **Enable anomaly data gathering and detection service and events**
4. Click **Save**.
5. Click **Edit** to modify the following **Basic Settings**:
   - **Anomaly detection sensitivity**
   - **Data retention settings**
   - **Data gathering settings**
   - **Anomaly proxy server settings**
6. Click **Save**.
7. Click **Advanced settings**.
8. Edit **Disable anomaly settings for clients**.
9. Click **Save**.
10. Edit **Disable policy type or specific features for machine learning**.
11. Click **Save**.

View anomalies

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

See “About backup anomaly detection” on page 170.

Note: An anomalies count of `0` indicates there are no anomalies generated or that the anomaly detection services are not running.

To view anomalies

1. On the left, select **Detection and reporting > Anomaly detection**.

   The following columns are displayed:

   - Job ID - Job ID of the job for which the anomaly is detected
   - Client name - Name of the NetBackup client where the anomaly is detected
   - Policy type - The policy type of the associated backup job
   - Count - The number of anomalies that are detected for this job
   - Score - Severity of the anomaly. The score is higher if the severity of the anomaly is more.
   - Anomaly severity - Severity of the anomalies that are notified for this job
   - Anomaly summary - Summary of the anomalies that are notified for this job
   - Received - Date when the anomaly is notified
   - Review status - Indicates whether the detected anomaly is reported as a false positive, an actual anomaly, or it can be ignored.
   - Policy name - The policy name of the associated backup job
   - Schedule name - The schedule name of the associated backup job
   - Schedule type - The schedule type of the associated backup job

2. Expand a row to see the details of the selected anomaly.

   For each anomaly record, the current value of that feature and its actual range based on the past data are displayed.

   Consider the following example:

   An anomaly of the image size feature is displayed as 100MB (Usual 350MB, 450MB). This information implies that the current image size that is reported as anomaly is 100 MB. However, the usual image size range is 350 MB - 450 MB that is derived from the analysis of past data. Because of the significant difference between the current images size and usual image size range, NetBackup notifies it as an anomaly.

3. You can perform the following actions on the anomaly record:

   - Click **Mark as ignore** when you can ignore the anomaly condition. The **Review status** of the anomaly record appears as `Ignore`.

- Click **Confirm as anomaly** when you want to take some action on the anomaly condition.
  The **Review status** of the anomaly record appears as `Anomaly`.
- Click **Report as false positive** if the anomaly is a false positive. Similar anomalies are not shown in the future.
  The **Review status** of the anomaly record appears as `False positive`.

Send audit events to system logs

You can send NetBackup audit events to system logs. Ensure that you have the following permissions to carry out this task:

- View permission on the **Security > Security events** UI
- View, Create, Update, and Delete permissions on the **NetBackup management > NetBackup hosts** UI

To send audit events to system logs

1. On the left, select **Security > Security events**.
2. On the top right, click **Security event settings**.
3. Enable **Send the audit events to the system logs** option.
4. In the **Audit event categories** dialog box, select the audit categories for which you want to send the audit events to the system logs.

   To send audit events for all audit categories to the system logs, select the **Audit event categories** check box.
5. Click **Save**.

   You can view NetBackup audit events in the system logs. For example:

   On a Windows system, use **Windows Event Viewer** to view NetBackup audit events.

   On a Linux system, you can view the system logs on the configured location.

Send audit events to log forwarding endpoints

You can send NetBackup audit events to log forwarding endpoints.

To send audit events to log forwarding endpoints

1. On the left, select **Security > Security events**.
2. On the top right, click **Security events settings**.

3 Enable **Send the audit events to log forwarding endpoints** option.

Once you enable the option, the **Select endpoints and categories** option appears.

4 Click the **Select endpoints and categories** option to see the log forwarding endpoints that are configured in your environment and the available audit categories.

Example of an endpoint: Azure Sentinel.

5 Select the appropriate log forwarding endpoints.

6 Click the **Select audit event categories** option.

7 On the **Select audit event categories** pop-up screen, select the categories of the audit events that you want to forward to the selected endpoints. For example, Alert, Anomaly and so on.

8 Once you select your log forwarding endpoint, options to specify the associated credentials appear. You can either add new credentials for the endpoint or select the existing credentials.

Display a banner to users when they sign in

You can configure a sign-in banner that displays each time that any user signs in to the NetBackup web UI. A different banner can be configured for any primary server. This banner can also require the user to agree to the terms of service before the user signs in.

To display a banner to users when they sign in

1 On the left, click **Security > User sessions**.

2 At the top right, click **User account settings**.

3 Turn on **Sign-in banner configuration** and click **Edit**.

4 Enter the text you want to use for the heading and the body of the message.

5 If you want to require the user to agree to the terms of service, select **Include "Agree" and "Disagree" buttons on the sign-in banner**.

6 Click **Save**.

For active users, the updates are applied the next time the user signs in.

To remove the sign-in banner

1. On the left, click **Security > User sessions**.
2. At the top right, click **User account settings**.
3. Turn off **Sign-in banner configuration**
4. Click **Save**.

   For active users, the updates are applied the next time the user signs in.