NetBackup Read This First for Secure Communications

This document provides critical information about secure communication in NetBackup 8.1. Veritas strongly recommends that you read this document before you install and deploy NetBackup 8.1.

For more information on NetBackup security features, refer to the *NetBackup Security and Encryption Guide*.

https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.index.html

About secure communications in NetBackup

NetBackup 8.1 hosts can communicate with each other only in a secure mode.

NetBackup uses Transport Layer Security (TLS) protocol for host communication where each host needs to present its security certificate and validate the peer host's certificate against the Certificate Authority (CA) certificate.

In NetBackup 8.1, each host must establish trust with the CA after which a CA certificate is added in the trust store. Each NetBackup 8.1 host must also have a host ID-based certificate for successful communication.

A host ID-based certificate is deployed on a host during NetBackup installation. If, for some reason, a certificate cannot be deployed on a host during installation, the host cannot communicate with other hosts. In that case, you must manually deploy a host ID-based certificate on the host using the `nbcertcmd` command to start host communication after installation.

The following nodes in the **NetBackup Administration Console** provide secure communication settings: **Host Management** and **Global Security Settings**.

The following commands provide options to manage certificate deployment and other security settings: `nbhostmgmt`, `nbhostidentity`, `nbcertcmd`, and `nbseccmd`.

If you have NetBackup 8.0 or earlier hosts in your environment, you can enable insecure communication with them.

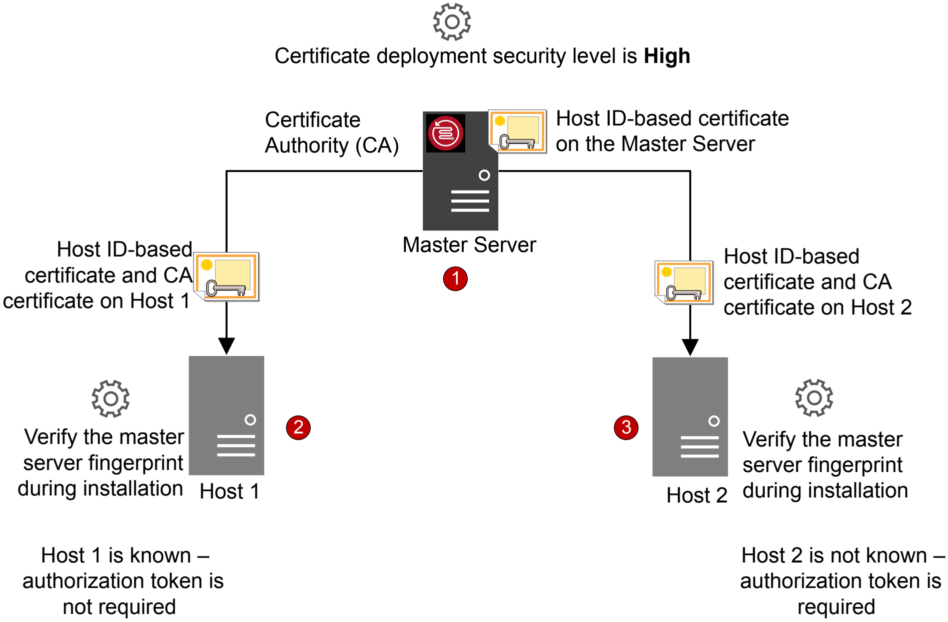
See “How NetBackup 8.1 hosts communicate with NetBackup 8.0 and earlier hosts” on page 8.

A host name-based certificate is required in the following scenarios:

- NetBackup Access Control or NBAC-enabled hosts require a host name-based certificate.
- Enhanced Auditing operations require that the hosts have a host name-based certificate.
- The NetBackup CloudStore Service Container requires that the host name-based certificate be installed on the media server.

How host ID-based certificates are deployed during installation

The following diagram illustrates how certificates are deployed on hosts during installation:


Certificate deployment security level is **High**
Certificate Authority (CA)
Host ID-based certificate on the Master Server
Master Server
1
Host ID-based certificate and CA certificate on Host 1
Host ID-based certificate and CA certificate on Host 2
2
3
Verify the master server fingerprint during installation
Host 1
Host 2
Verify the master server fingerprint during installation
Host 1 is known – authorization token is not required
Host 2 is not known – authorization token is required

Host ID-based certificate deployment occurs in the following order:

1. A host ID-based certificate is automatically deployed on the NetBackup master server during installation. The master server is the CA.
2. A host ID-based certificate is deployed on Host 1 during installation after confirming the CA fingerprint that is made available by the installation wizard or the script.

   An authorization token is not required because the certificate deployment security level on the master server is set to High and Host 1 is known to the master server.

A fingerprint is used to authenticate the CA of the master server before it is added to the trust store of a host. The master server administrator communicates the CA fingerprint to the host administrators by email or file, or publishes it on a website.

An authorization token is used as a mechanism to authorize a host’s certificate request that is sent to the NetBackup master server. An authorization token is confidential and only the master server administrator can create it. The master server administrator then passes it on to the administrator of the host where you want to deploy a certificate. A reissue token is a special authorization token that is used to redeploy a certificate on a host to which a certificate was previously issued.

If you continued with the NetBackup installation without confirming the master server fingerprint, you need to carry out manual steps before backups and restores can occur.

https://www.veritas.com/support/en_US/article.000127129

3. A host ID-based certificate is deployed on Host 2 during installation after the master server fingerprint is confirmed. An authorization token is required, because the certificate deployment security level on the master server is set to High and Host 2 is not known to the master server.

How certificates are deployed on hosts during upgrades

During a NetBackup 8.1 upgrade, NetBackup deploys host ID-based certificates before the upgrade. If the certificates cannot be deployed, you can terminate the upgrade process. The upgrade script retains the existing NetBackup setup that you can use.

If you have upgraded NetBackup from 8.0 to 8.1, host ID-based certificates may already be present on the hosts. In such a case, certificates are not deployed during the upgrade process.

Certificates are not deployed during the upgrade process, if the software is upgraded using a utility (that downloads and installs security updates and software patches). You need to manually deploy the certificates.

How secure communication works with master server cluster nodes

Review the following scenarios about certificate deployment if you have a clustered master server:

- In the case of fresh NetBackup installation, the certificate on an active node is deployed automatically. You must manually deploy certificates on all inactive nodes.
- In the case of disaster recovery, certificates for active and inactive nodes are not recovered. After you install NetBackup in a disaster recovery mode after a disaster, you must manually deploy certificates on all nodes using a reissue token.
- In the case of upgrade, active or inactive nodes may already have a certificate. You can verify whether a cluster node has a certificate or not by viewing the certificate details with the `nbcertcmd -listCertDetails` command.

If you have configured NetBackup Access Control (NBAC) or Enhanced Auditing (EA) on a master server cluster node, you also need to manually deploy host name-based certificates on all nodes.

In a cluster setup, the same virtual name is used across multiple cluster nodes. Therefore, the virtual name should be mapped with all associated cluster nodes.

About NetBackup clients installed on nodes of a clustered application

Review the following scenarios about secure communication with NetBackup clients installed on nodes of a clustered application:

- For successful communication, you need to simultaneously upgrade all cluster nodes to 8.1.
- Ensure that the virtual name is mapped to all cluster nodes to avoid backup failures after a failover. Veritas recommends that you monitor the **Security Management > Host Management > Mappings for approval** tab for any conflicts that are detected and approve the required mappings.

When an authorization token is required during certificate deployment

The security level setting determines whether an authorization token is required to deploy a certificate. You can set the security level on the master server to different levels, depending on your needs. Use the **Security Management > Global Security Settings > Secure Communication** tab in the **NetBackup Administration Console**.

The following settings are available. The default setting is High.

- **Medium** - The master server fingerprint must be confirmed during certificate deployment. An authorization token is not required.
- **High** - The master server fingerprint must be confirmed during certificate deployment. An authorization token is not required if the host is known to the master server.

- **Very High** - The master server fingerprint must be confirmed during certificate deployment. An authorization token is required for every host.

Certificate deployment in certain scenarios always requires a token, such as in the case of clients in a demilitarized zone or for certificate reissue.

For more information on certificate deployment security levels, refer to the *NetBackup Security and Encryption Guide*.

https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.v120724164-127424841.html

Why do you need to map host names (or IP addresses) to host IDs

Hosts can be referenced with multiple names.

For example: In the case of multiple network interfaces or if hosts are referenced by both short names and Fully Qualified Domain Names (FQDN).

For successful secure communication in NetBackup 8.1, you should map all associated host names to the respective host ID. The NetBackup-configured client name of a host (or the primary name) is automatically mapped to its host ID during certificate deployment. Additional host names are discovered during communication and may be automatically mapped to the respective host ID or may appear in the **Mappings for Approval** list. Perform this configuration in the **Host Management** properties on the master server.

For more information on host ID-to-host name mappings, refer to the *NetBackup Security and Encryption Guide*.

https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.v126691093-127424841.html

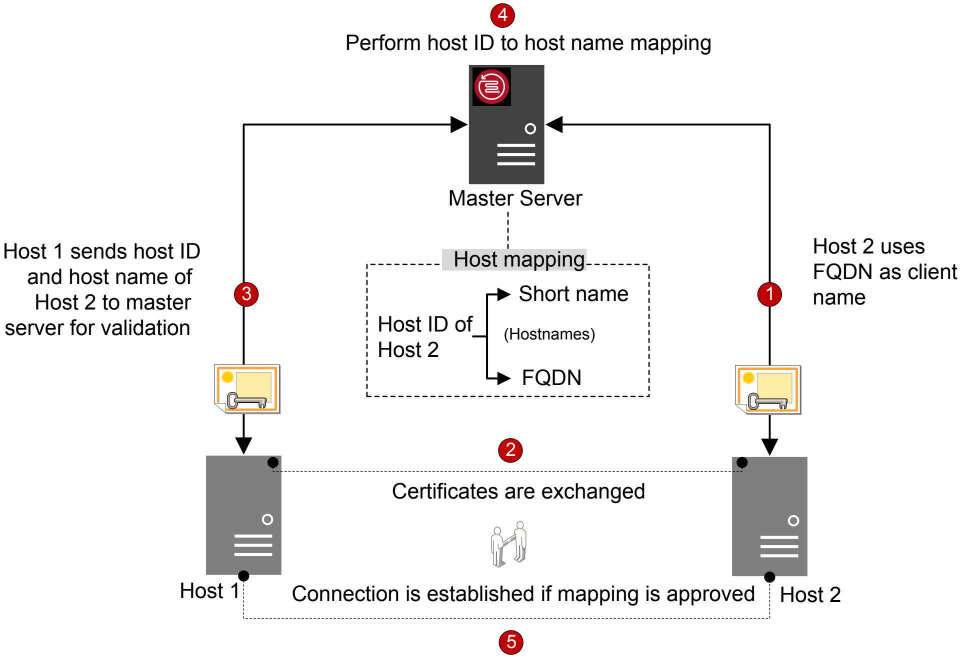
Examples of configurations that have multiple host names include:

- If you have multiple network interfaces, a host has both a public and a private host name.
- A host can have a short name and a fully qualified domain name (FQDN).
- A host can be associated with its IP address.
- For a file system or database that is clustered, a host is associated with its node name and the virtual name of the cluster.

Note the following:

- The Exchange, SharePoint, and SQL Server agents also require that you configure host information in the **Distributed Application Restore Mapping** host properties on the master server.
- For highly available environments, the SQL Server agent no longer requires a second policy that contains the cluster or AG node names. You also do not need to configure permissions for redirected restores for the cluster or AG nodes. For successful backups and restores of a SQL Server cluster or AG, you need only configure the mappings in the **Host Management** properties and the **Distributed Application Restore Mapping** host properties.

The following diagram illustrates the host ID-to-host name mapping process:


4
Perform host ID to host name mapping
Master Server
Host mapping
Host ID of Host 2
Short name
(Hostnames)
FQDN
Host 1 sends host ID and host name of Host 2 to master server for validation
3
Host 2 uses FQDN as client name
1
2
Certificates are exchanged
Host 1
Host 2
Connection is established if mapping is approved
5

Host name-to-host ID mapping occurs in the following order:

1. The FQDN of Host 2 is mapped to its host ID during certificate deployment.
2. Host 1 initiates a secure connection to Host 2 using the short name. Both hosts exchange their host ID-based certificates as part of the TLS handshake.
3. Host 1 sends the host ID and short name of Host 2 to the master server for validation.
4. The master server looks up the host ID and the short name in its database. Since the provided short host name is not already mapped to the host ID of Host 2, one of the following occurs:
   - If the **Automatically map host ID to host names** option in the **NetBackup Administration Console** is selected and the short name is not already mapped to another host ID, the discovered short name is automatically mapped to the host ID of Host 2, and Host 1 is instructed to continue the connection.
   - If the **Automatically map host ID to host names** option is not selected or the short name is already mapped to another host ID, the discovered mapping is added to the pending approval list and Host 1 is instructed to drop the connection. The mapping should be manually approved before any connections to Host 2 using the same short name can succeed.
5. Connection is established between the hosts if the mapping is approved. If the mapping is not approved, the connection is dropped.

How to reset host attributes or host communication status

The **Reset Host Attributes** option deletes host properties and host name-to-host ID mappings information. The primary host name and host ID-based certificate are not deleted.

Resetting host attributes is useful in the following scenarios:

- If you have downgraded a host to 8.0 or earlier to enable insecure (or back-level) communication.

- If you experience host communication issues and you want to delete the host information.

For more information on resetting host attributes, refer to the *NetBackup Security and Encryption Guide*.

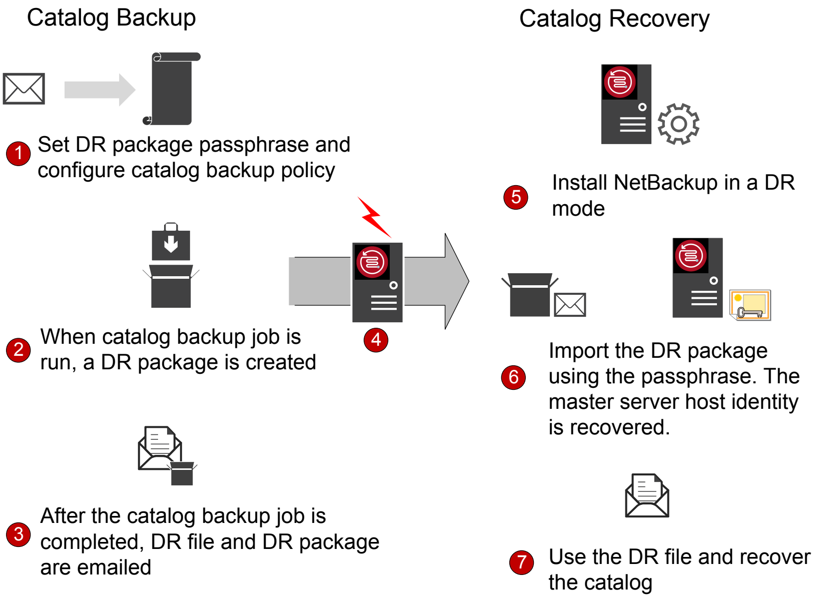
https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.v126691350-127424841.html

What has changed for catalog recovery

In NetBackup 8.1, the master server requires you to recover its host identity when you restore NetBackup after a disaster. The host identity includes certificate information, security settings, and other information.

With the earlier host identity in place, the master server can communicate with media server and clients in the new NetBackup instance. A disaster recovery package is created during each catalog backup that retains the master server host identity. As the disaster recovery package contains sensitive data such as security certificates and security settings, it is encrypted with a passphrase.

The following diagram shows the workflow for the catalog recovery.


Catalog Backup
Catalog Recovery
1 Set DR package passphrase and configure catalog backup policy
2 When catalog backup job is run, a DR package is created
3 After the catalog backup job is completed, DR file and DR package are emailed
4
5 Install NetBackup in a DR mode
6 Import the DR package using the passphrase. The master server host identity is recovered.
7 Use the DR file and recover the catalog

1. Set a passphrase for the disaster recovery package and then configure a catalog backup policy. Catalog backups use the passphrase that is configured at the time of policy execution.
   To set a passphrase, use the **Security Management > Global Security Settings > Disaster Recovery** tab in the **NetBackup Administration Console**.
   If you change the passphrase at any time, the passphrase of the disaster recovery packages that were created earlier is not changed. It only changes the passphrase of the disaster recovery packages that are created subsequently.
   To recover older catalogs, you must use the corresponding passphrase.

You must set the passphrase before you configure the catalog backup policy. If the passphrase is not set, catalog backups fail. If the catalog backup policy is upgraded from a previous version, catalog backups continue to fail until the passphrase is set.

2. A disaster recovery package is created during each catalog backup.

   To verify the passphrase after the catalog backup is successful, run the following command:

   ```
   nbhostidentity -testpassphrase -infile dr_package_location
   ```
3. Disaster recovery packages are stored along with the disaster recovery files and emailed to the recipient that you have specified during policy configuration.
4. Disaster strikes.
5. After a disaster, install NetBackup on the master server in a disaster recovery mode. This process prompts you to specify the disaster recovery package path and passphrase.
6. If the appropriate passphrase is specified, the master server host identity is recovered. You must provide the passphrase that corresponds to the disaster recovery package that you want to recover.

   If you lost the passphrase, you must deploy security certificates on all NetBackup hosts manually.

   For more details, refer to the following article:

   http://www.veritas.com/docs/000125933
7. You should perform the catalog recovery immediately after you have recovered the host identity to avoid any information loss specific to certificate-related activities that may have taken place after the host identity restore. Use the appropriate disaster recovery (DR) file and recover the required catalog.

   The passphrase is not recovered during the host identity (or disaster recovery package) restore or during catalog recovery. You must set it again in the new NetBackup instance.

If you need to restore the host identity after the normal NetBackup installation (when the disaster recovery mode is not selected), you can use the `nbhostidentity` command.

To restore the host identity of NetBackup Appliance, you must use the `nbhostidentity` command after the normal installation.

What has changed with Auto Image Replication

To use NetBackup Auto Image Replication (A.I.R.) with secure communications, you must establish trust from both the source and the target master servers.

When you upgrade both the source and the target master servers to 8.1, you must update the trust relationship on both master servers.

After the 8.1 upgrade, if the trust is not re-established on both the servers, new storage lifecycle policies (SLP) do not work.

You can configure the trust relationship using the **NetBackup Administration Console** or the `nbseccmd -setuptrustedmaster` command.

For more information on trusted master servers for Auto Image Replication, refer to the *NetBackup Deduplication Guide*.

https://www.veritas.com/content/support/en_US/doc-viewer.25074086-127355784-0.v81800250-127355784.html

How the hosts with revoked certificates work

Host ID-based certificates can be revoked by the master server administrator for various reasons. A Certificate Revocation List (CRL) containing information about the revoked certificates is created by the master server and is periodically fetched by all hosts. The time interval to update the CRLs is determined by the certificate deployment security level on the master server.

During communication between hosts, CRLs are verified. The host that uses a revoked certificate is no longer trusted. Communication with such hosts is terminated.

For more information on CRLs, refer to the *NetBackup Security and Encryption Guide*.

https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.v126192948-127424841.html

How communication happens when a host cannot directly connect to the master server

In a demilitarized zone (DMZ), NetBackup clients may not be able to directly send requests (for certificate deployment and so on) to the master server. The HTTP tunnel on the media server is used to accept the web service requests sent by the client hosts and forward them to the master server. The configuration of the HTTP tunneling is automatic and no setup is required. The NetBackup client and the media server must be 8.1 or later for HTTP tunneling to work.

Irrespective of the certificate deployment security level that is set on the master server, you require an authorization token to deploy a host ID-based certificate on a host in a demilitarized zone.

For more information on clients in a DMZ, refer to the *NetBackup Security and Encryption Guide*.

https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.v125482382-127424841.html

Are security certificates backed up

For security reasons, security certificates are not backed up during backups. Certificates are automatically deleted when NetBackup is uninstalled. If required, you can manually back them up before you uninstall NetBackup.

For more information on retaining the host ID-based certificates, refer to the *NetBackup Security and Encryption Guide*.

https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.v122201443-127424841.html

How communication with legacy media servers happens in the case of cloud configuration

If the **Enable insecure communication with NetBackup 8.0 and earlier hosts** option is disabled, NetBackup cannot communicate with legacy media servers that you use for cloud storage irrespective of the value of the `CSSC_LEGACY_AUTH_ENABLED` cloud configuration option.

The **Enable insecure communication with NetBackup 8.0 and earlier hosts** option is available in the **NetBackup Administration Console** on the **Security Management > Global Security Settings > Secure Communication** tab.

How NetBackup 8.1 hosts communicate with NetBackup 8.0 and earlier hosts

NetBackup 8.1 hosts can communicate with other 8.1 hosts only in a secure mode. For a 8.1 host to communicate with hosts at 8.0 or earlier, or for a 8.1 master server to communicate with OpsCenter 8.1, you need to allow insecure communication.

By default, the **Enable insecure communication with NetBackup 8.0 and earlier hosts** option is enabled. The option is available in the **NetBackup Administration Console**on the **Security Management > Global Security Settings > Secure Communication** tab.

If you disable the option to allow only secure communication, you must restart the NetBackup services on the master server to terminate any insecure communications and allow only secure communications.

During insecure communication, the NetBackup 8.1 host first connects to the master server for host validation. The master server verifies whether insecure communication is enabled or not. If the option is enabled, the communication between the two hosts is established. If the option is disabled, the communication is dropped.

Communication failure scenarios

Review the following scenarios to resolve host communication issues that you may face in NetBackup 8.1.

Failure during communication with 8.0 or earlier hosts

If insecure communication is not allowed in NetBackup, communication with 8.0 and earlier hosts fails. For successful communication with 8.0 and earlier NetBackup hosts, use one of the following methods:

- In the **NetBackup Administration Console** on the master server host, select the **Security Management > Global Security > Hosts > Enable insecure communication with NetBackup 8.0 and earlier hosts** option.
- On the master server host, run the following command: `nbseccmd -setsecurityconfig -insecurecommunication on`.

Catalog backup failure

If the disaster recovery package passphrase is not set, catalog backups fail with status code 2524. The following error message is displayed:

```
Catalog backup failed because the passphrase for the disaster recovery
package is not set.
```

To set a passphrase, use the **Security Management > Global Security Settings > Disaster Recovery** tab in the **NetBackup Administration Console**.

Secure communication support for other hosts in NetBackup domain

Use this section to learn about how NetBackup 8.1 supports communication with OpsCenter and BMR (Bare Metal Restore) hosts.

Communication between NetBackup 8.1 master server and OpsCenter 8.1 server

Ensure that the following options are configured before you collect data from a NetBackup 8.1 master server using OpsCenter 8.1 server:

- The OpsCenter server name must be added against the `OPS_CENTER_SERVER_NAME` configuration option in the NetBackup configuration file (`bp.conf` on UNIX or registry key for Windows).
- Insecure communication is enabled in NetBackup. Check one of the following:
  - In the **NetBackup Administration Console** on the master server host, the **Security Management > Global Security > Hosts > Enable insecure communication with NetBackup 8.0 and earlier hosts** option is selected.
  - On the master server host, `nbseccmd -setsecurityconfig -insecurecommunication` command-line option is set to ‘on’.

Secure communication support for BMR

With secure communications, NetBackup Bare Metal Restore (BMR) functionality is not supported for restoring the NetBackup version 8.1 hosts. However, you can use BMR for restoring NetBackup 8.0 and earlier hosts. While restoring 8.0 and earlier hosts, Veritas recommends that you use Shared Resource Tree (SRT) with 8.0 or earlier versions.