NetBackup™ Self Service Configuration Guide

11.2

Document version: 1

COHESITY

NetBackup™ Self Service Configuration Guide

Last updated: 2026-09-15

Legal Notice

Copyright © 2026 Cohesity Inc All rights reserved.

© 2026 Cohesity Inc All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity Inc in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 Configuring a Self Service solution 7

About configuring a Self Service solution 7
Self Service scheduled backup 8
Configuration checklist 8

Chapter 2 Configuring a NetBackup primary server 10

About configuring the NetBackup primary server 10
Enabling communication with a Windows NetBackup primary server 10
Enabling communication with a UNIX NetBackup primary server 11
Enabling communication with a NetBackup appliance 13
Enabling communication with a NetBackup primary server using the REST API 14
Creating NetBackup Template Policies 16

Chapter 3 Configuring Self Service 19

About Self Service configuration 19
Configuring backup servers 20
Configuring protection 23
Configuring storage 31
Configuring tenants 31
Access rights 32
Registering computers 33
Configuring the home page 38
Home page integration settings 38
Configuring mail/SMTP server 41

Chapter 4 Customizing Self Service 43

Language settings 43
Themes 43
Notices 44
Email Template Customization Screen 45

Chapter 5 User authentication methods 46

About user authentication methods 46
Forms based authentication 46
Windows Authentication 47
Active Directory Import 47
Configuring Self Service to use Federated Single Sign-On 48

Chapter 6 Troubleshooting 51

About troubleshooting 51
Where to find troubleshooting information 53
Impersonation of a tenant user 54
Issues with Remote PowerShell to Windows primary servers 54
Issues with HTTPS configuration 58
Configuration troubleshooting 58

Appendix A NetBackup policy types 60

List of NetBackup policy types 60

Appendix B Dashboard traffic light status and usage 63

About dashboard traffic light status and usage 63
Assets with a protection type 63
Assets without a Protection Type 64
Usage and Charging 64
Tenant Quota Enforcement 65

Appendix C Synchronizing data from NetBackup 68

About synchronizing data from NetBackup 68

Appendix D NetBackup Self Service data caching process 70

About NetBackup Self Service data caching process 70
NetBackup Data Synchronization 72
Backup Now 72
Protect 72
Unprotect 73

Appendix E Integration settings 74

About integration settings 74
NetBackup Adapter 75

NetBackup Adapter Usage 78
NetBackup Adapter Access Rights 79

Appendix F REST API 82

About the REST API 82

Appendix G Central configuration and the nsscmd command 83

Central configuration and the nsscmd command 83

Appendix H Glossary 86

Glossary 86

Chapter 1

Configuring a Self Service solution

This chapter includes the following topics:

- About configuring a Self Service solution
- Self Service scheduled backup
- Configuration checklist

About configuring a Self Service solution

NetBackup Self Service allows service providers to offer self-service backup and restore to multiple customers, in a secure, and partitioned manner. In an enterprise environment, business units and project teams can perform self-service backup and restore.

Self Service restore functionality is enabled but additionally you can choose to provide self-service scheduled policy editing and support for on-demand Backup Now functionality.

Caution: All configuration data that is entered in NetBackup Self Service is considered case sensitive. It must match the associated data that is held in NetBackup.

The Self Service solution supports an inventory of assets and their owners.

You can populate the inventory multiple ways:

- A source independent API
- The Self Service portal

- An import from vCloud Director
- An import of cloud assets from NetBackup

Self Service supports a number of NetBackup Policy types. You can either use Self Service to manage all of a tenant's backup needs. This option allows tenants to create their own backup policies. Or you can configure Self Service to only provide restore services based on manually maintained backup policies.

A record of registered assets and their protection types, such as Windows, UNIX, VMware, etc., is maintained within Self Service.

The tenant user manages computer protection status and utilization with a full set of dashboard features. The tenant user can create changes to protection and restore.

Self Service scheduled backup

Configuration of protection enables users to manage their backup schedules. This option provides an abstraction from NetBackup Policy configuration, offering a curated set of backup schedules from which the user can choose.

Configuration checklist

Table 1-1 shows the recommended sequence of steps for configuring Self Service for the first time.

Table 1-1 Configuration checklist

Where	Activity	
Server	Install NetBackup Self Service (see *NetBackup Self Service 11.2 Installation Guide*)	
	For pre-NetBackup 11.2 configure remote PowerShell for a Windows primary server.	
	For pre-NetBackup 10.3, configure SSH for a UNIX primary server.	
	For NetBackup 10.3 or later, follow the steps shown: See "About configuring the NetBackup primary server" on page 10.	
	Portal	Create at least one backup server.
		Create at least one protection type (if needed)
NetBackup primary server	Create Template Policies.	
Portal	Create a Tenant through the user interface.	
	Register at least one asset through the user interface, the API, NetBackup Import, or through vCloud Director import	
	Test each main Self Service operation, where enabled and relevant: ■ Submit a Protect request, then unprotect the computer after protection. ■ Submit a Backup Now request. ■ Submit a Restore File request. ■ Submit a Restore VM request. ■ Submit a Restore Cloud Asset request.	

Chapter 2

Configuring a NetBackup primary server

This chapter includes the following topics:

- About configuring the NetBackup primary server
- Enabling communication with a Windows NetBackup primary server
- Enabling communication with a UNIX NetBackup primary server
- Enabling communication with a NetBackup appliance
- Enabling communication with a NetBackup primary server using the REST API
- Creating NetBackup Template Policies

About configuring the NetBackup primary server

Self Service requires a minimum of NetBackup 8.0 with the latest service pack.

Each NetBackup primary server the system needs to communicate with must be configured as a backup server. To manage backup servers, log on to the Self Service portal as an Admin user, and then go to the **Backup Servers** page using the left-hand navigation.

Enabling communication with a Windows NetBackup primary server

Note: This section is only required for pre-NetBackup 10.3 versions. For NetBackup 10.3 and later it is not required.

NetBackup Self Service uses Windows PowerShell Remoting to communicate with a Windows NetBackup primary server. Windows PowerShell must be installed on the primary server. Windows PowerShell is normally installed by default. Additionally, PowerShell Remoting must be enabled. More information is available.

http://technet.microsoft.com/library/hh847859.aspx

To enable communication with a Windows NetBackup primary server

1. Log on to the NetBackup primary server.
2. Launch a Windows PowerShell window as Administrator.
3. Run `Enable-PSRemoting -Force`.
4. Open Required Firewall ports.

   By Default PowerShell Remoting uses HTTP on Port 5985 or HTTPS on Port 5986.

More information is available.

http://technet.microsoft.com/en-us/magazine/ff700227.aspx

If communication with the primary server from the Self Service Server is not with a trusted domain account, it may not be able to authenticate. To enable authentication you need to add the remote computer to the list of trusted hosts for the local computer in WinRM. To do so, type:

```
winrm set winrm/config/client '@{TrustedHosts="machine1,machine2"}'
```

Add extra computers as needed in the comma-separated list.

More information about testing the connection once you have created your first backup server is available.

See “Configuring backup servers” on page 20.

Enabling communication with a UNIX NetBackup primary server

Note: This section is only required for pre-NetBackup 10.3 versions. For NetBackup 10.3 and later it is not required.

NetBackup Self Service uses Secure Shell (SSH) to communicate with a UNIX NetBackup primary server. The configuration of SSH is outside the scope of this guide. NetBackup Self Service, however, requires the credentials to communicate with the SSH server on the primary server.

- By default SSH uses Port 22.
  To specify a different port, set the server name to *server_name*:*port_number*.
  For example, `MyServer:23`.
- The user account that NetBackup Self Service uses to logon to SSH on the primary server needs `sudo` configuration:
  - The user account should not use `requiretty`.
  - The user account should not require a `sudo` password.
  - With `sudo`, the user account should run all commands in `/usr/openv/netbackup/bin` and `/usr/openv/netbackup/bin/admincmd`.

User authentication modes that are supported include:

- Password
  NetBackup Self Service passes the user name and password at logon.
- Public key
  The public key of the user is stored in the `authorized_keys` for the user on the primary server. The private key of the user is stored in OpenSSH format in the NetBackup Self Service portal.
- Keyboard-interactive
  NetBackup Self Service sends the password for the user to a keyboard-interactive ssh session. The password is sent in response to a configurable password prompt. The default password prompt is **Password:**.

To configure NetBackup Self Service and the NetBackup primary server for public key authentication

1. Create a Public Private key pair using a key generator like `PuTTYgen`.
2. Log on to the primary server as the required primary server user
3. Add the public key to the user's `authorized_keys` file in the primary server's operating system format.

4 Convert the Private key into OpenSSH format encrypted with a passphrase

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,997295A8E365412F

SIKdyjX4UoDm03kprqfkCGQYc/thmNIlWYztEomjyRaMyEYlh0ZIC9Kx7XnMNnSk
...
MUxIcZW8d8fF3P4s+OLidxG03H6C/AsGLzJtpecjPQA=
-----END RSA PRIVATE KEY-----
```

5 When you create the backup server in NetBackup Self Service:

- Choose **Public Key** for the Authentication.
- Enter the user account to connect to the primary server in **User Account**.
- Paste the encrypted OpenSSH format private key in **OpenSSH Private Key**.
- Enter the passphrase in **Password** and **Confirm Password**.

More information about testing the connection once you have created your first backup server is available.

See “Configuring backup servers” on page 20.

Enabling communication with a NetBackup appliance

Note: This section is only required for pre-NetBackup 10.3 versions. For NetBackup 10.3 and later it is not required.

A connection to an appliance is configured similarly to a UNIX primary server, but configuration of keys is not available. Use a previously created user name and password to make the connection.

Log on to shell menu on the appliance and create a new user:

Main_Menu > Manage > NetBackupCLI > Create *UserName*

See *Creating NetBackup administrator user accounts* in the *NetBackup Appliance Administrator's Guide* for further details.

Enabling communication with a NetBackup primary server using the REST API

NetBackup Self Service can use the NetBackup REST API for some communication with the primary server. Your NetBackup server must be version 8.1.2 or higher.

Basic Setup

To enable communication using the REST API

1. Log on to NetBackup Self Service as an administrator and navigate to the **Backup Servers** page. Select the appropriate backup server.
2. Fill in the details in the **REST API Connection** section.

   A background task automatically examines the connectivity with the backup server.
3. Once the job has completed, click the status icon to open connectivity summary screen
4. Review that the REST API has been contacted successfully.

Multifactor authentication (for NetBackup 10.3 and later)

To enable multifactor authentication

1. The NetBackup administrator must create a NetBackup Self Service user with RBAC security shown:
   - The account requires a role with at least **View Protection Plans**, **Manage Protection Plans**, **View Assets**, **Manage Assets**, **Recover/Restore**, and **View Jobs**.
   - It also requires an object group with access to all Assets, and all Protection plans.
2. For the user you created, generate an API key and save the API key and API key tag. Cohesity recommends that the user have one year Validity.
3. In NetBackup Self Service use the saved API Key & API key Tag to access the REST API.

Credentials (for pre-NetBackup 10.3)

By default NetBackup Self Service uses the same credentials to access the REST API as it uses to access the CLI. If you want to use a different account and RBAC security, the account requires a role with at least **View Protection Plans**, **Manage Protection Plans**, **View Assets**, **Manage Assets**, **Recover/Restore**, and **View Jobs**. It also requires an object group with access to all Assets, and all Protection plans.

Certificates

Communication with the NetBackup REST API is over HTTPS. HTTPS requires a trust relationship to exist between the client and the server. In this instance the client is the NetBackup Self Service web server or Task engine server, and the server is the NetBackup primary server. The trust relationship is established using a certificate.

You have three options for the certificate:

1. The primary server uses a certificate that is issued from a trusted certificate authority.

   The NetBackup Self Service web server has the trust of the https connection and no other actions are necessary.

2. The primary server certificate is either from a private certificate authority, or a self-signed certificate. You must install the certificate authority certificate manually in the trusted certificate store of the web server and task engine server. See To install the Certificate Authority certificate from the primary server onto the NetBackup Self Service web server or Task Engine server for more information.

3. Ignore certificate errors.

   - Go into NetBackup Self Service as an administrator and navigate to the **Backup Servers** page.
   - Select the backup server. Click **Show Advanced Settings**. In the REST API Connection section review **Ignore Certificate Errors**, and save changes.

     This choice is a good option to use when first setting up the REST API, as it eliminates one source of problems. However, once the REST API connection works, you should only use trusted certificates. Once trusted certificates are established, clear the 'Ignore Certificate Errors' option.

Installing a Trusted Certificate Authority Certificate

To install the Certificate Authority certificate from the primary server onto the NetBackup Self Service web server or Task Engine server

1 In NetBackup Self Service:

- In the **Backup Servers** page, select the backup server. Click the status icon, to open the configuration summary screen.
- In the REST Connection Status section, click to download the primary server's certificate onto your computer.

2 In Windows Explorer, on the appropriate NetBackup Self Service server:

- Locate the certificate and right-click to open it.
- Review the certificate to ensure that it is correct.
- Click **Install Certificate...**.
  - Select the **Local Machine** store location.
  - Browse to the certificate store **Trusted Root Certification Authorities** and select **OK**.
  - Select **Next**.
  - Select **Finish**.

3. This process installs the primary server's Certificate Authority certificate on the NetBackup Self Service server. The server now trusts the primary server certificate.
4. Return to NetBackup Self Service and in the **Backup Servers** page, select the backup server. Ensure that the **Ignore Certificate Errors** option is cleared.
5. Run the connectivity check. Verify that you can still connect to the backup server.

Creating NetBackup Template Policies

Numerous options are available when you create a NetBackup policy. The *NetBackup Administrator's Guide Volume I* contains an entire chapter on creating backup policies. Please refer to that manual for details on the creation of backup policies.

Self Service template policies do not use all NetBackup policy options. For scheduled policies, the information that is specified in Table 2-1 is the only items that affects Self Service. You should configure all other policy data as you would for any other NetBackup policy. Table 2-1 details the relevant tab in the NetBackup policy creation screen and the corresponding information that is required for Self Service template policies. For comprehensive information on how to create NetBackup policies, please see the *NetBackup Administrator's Guide Volume 1*.

Table 2-1 Required policy information for scheduled and Backup Now policies

NetBackup policy tab	Applicable template policy	Additional details
Attributes	Backup Now and scheduled backup	■ The policy must be deactivated. ■ When you specify the storage option, be sure to specify one that is large enough to successfully back up all the data.

Table 2-1 Required policy information for scheduled and Backup Now policies *(continued)*

NetBackup policy tab	Applicable template policy	Additional details
Schedules	Backup Now only	■ If you use **Retention Levels**, you must have a schedule named **Default**. ■ Self Service does not use the retention value that is set in the NetBackup policy. Self Service updates the retention level of the **Default** schedule when the policy is created. ■ Do not set the schedule to run automatically.
Clients	Backup Now and scheduled backup	■ NetBackup Self Service adds the client information so leave this field blank.

Template Policies are inactive policies on the primary server that need to be specially created for the solution. They are only required if you use Protection Levels or offer Backup Now functionality.

When users perform the actions that require a policy to be created on the primary server, the relevant template is copied to create a tenant-specific policy. The policy is modified according to the user's action.

Template Policies must be created on every primary server that is configured as a backup server. The naming of these policies is case-sensitive and all should be marked inactive.

Policy Type

The policy type code for NetBackup. For example, 0 for standard, 13 for Windows, 40 for VMware.

More information on NetBackup policy types is available.

See "List of NetBackup policy types" on page 60.

For any type 40 (VMware) template policy:

- For any vCloud Director template policy on the **Client** tab **Virtual Machine Selection** must specify **Enable vCloud Director integration**.

Backup Now Template Policies

NetBackup Self Service is configured out of the box to use the default NetBackup retention levels for BackupNow policies. If these are changed in NetBackup or different retention levels are offered to users, modifications must be made in the NetBackup Self Service Portal.

Type 40 (VMware) Backup Now template policies

Some consideration is needed around the **Reuse VM selection query results for** value on the **Clients** tab for Backup Now template policies. If the value is left as the 8-hour default value, backup now actions that are performed on a virtual machine that is created within the last 8 hours could fail. If the value is set lower or to 0 hours, the operation might succeed. This change may, however, have performance implications for connected VMware systems as the whole cache is rebuilt. This value may need changing from the default 8 hours, depending on the expected usage of the system.

Chapter 3

Configuring Self Service

This chapter includes the following topics:

- About Self Service configuration
- Configuring backup servers
- Configuring protection
- Configuring storage
- Configuring tenants
- Access rights
- Registering computers
- Configuring the home page
- Configuring mail/SMTP server

About Self Service configuration

You can manage the key creation and editing configuration tasks from the main panel on the home page:

- Backup servers
- Protection
- Tenants
- Assets

Any non-Tenant associated Administrator sees this home page panel.

Configuring backup servers

A backup server represents a connection to a NetBackup primary server. The system requires at least one backup server to function.

New backup servers are created with **Add Backup Server** on the **Backup Servers** page. A drop-list allows the further selection of **Add UNIX or Linux Backup Server** or **Add Windows Backup Server**. On-screen help is available to assist completion of the necessary details.

Once the backup server has been created the system returns to the main **Backup Servers** page where a Connectivity Check is started. The animated cog on the Check Connectivity button indicates that the Connectivity Check is started.

If the check has passed, no further action is required and your backup server is ready for use. If it failed, click the red cross to bring up details of the failure.

Once you have created a backup server, there are three actions available from the **Backup Servers** actions list: **Edit Details**, **View Connectivity**, and **Delete**.

Table 3-1 Backup Servers settings

Item	Details
Name	The name that is displayed to users.
Server Name	The host name or fully qualified domain name (FQDN) of the backup server, for example `netbackupserver` or `netbackupserver.example.com`. Alternatively you can specify the host name with a port number. On a UNIX system the syntax is *`hostname`*`:`*`portnumber`*. For example: `netbackupserver:22`, where 22 is the default port number for SSH. On a Windows system, specify a port number using the URL syntax shown: `http://`*`hostname`*`:`*`portnumber`*`/wsman`. For example: `http://netbackupserver:5985/wsman` or `https://netbackupserver:5986/wsman`.
Version	Range that includes the version of the NetBackup primary server. ■ 8.0 - 8.1.1 ■ 8.1.2 ■ 8.2 ■ 8.3 - 10.2 ■ 10.3 and later

Table 3-1 Backup Servers settings *(continued)*

Item	Details
Enable Agentless File Restore	Indicates that the backup server is configured to support VMware agentless file restore. The backup server must have all the required VxUpdate packages installed. If this option is enabled, any VMware asset that does not have a NetBackup client name configured automatically offers Agentless File Restore.
Online	Indicates if the backup server is online. You may want to take a backup server offline while performing planned maintenance. The system does not process an offline backup server in any way and users are blocked from performing actions such as backup and restore.
Authentication (for pre-NetBackup 10.3)	UNIX or Linux: Authentication mechanism when connection to a UNIX server. When connecting to a NetBackup Appliance choose **Password**. The options are: **Password**, **Keyboard Interactive Password**, or **Public Key**. Windows: CredSSP authentication delegates the user's credentials from the local computer to the remote computer. The options are: **Default** or **CredSSP**.
User Account and Password (for pre-NetBackup 10.3)	UNIX or Linux: The user that connects to the backup server. The user must be able to connect with SSH. Windows: The user must be able to connect to Remote PowerShell.
API Key and API Key Tag (for NetBackup 10.3 and later)	Enter the API Key and API key Tag configured in NetBackup for a user.

Table 3-1 Backup Servers settings *(continued)*

Item	Details
Server Date Format and Server Time Format (for pre-NetBackup 10.3)	The format in which the backup server expects dates and times. `ddMMyyyyHHmmss` ■ `dd` - The day of the month, from 01 through 31 ■ `MM` - The month, from 01 through 12 ■ `yyyy` - The year as a four-digit number ■ `HH` - The hour, from 00 through 23 ■ `mm` - The minute, from 00 through 59 ■ `ss` - The seconds, from 00 through 59 You can select from the example formats listed or enter a custom format. More information about editing the date and the time format is available. https://docs.microsoft.com/en-us/dotnet/standard/base-types/custom-date-and-time-format-strings
Server Time Zone (for pre-NetBackup 10.3)	The time zone of the backup server.
URL	The URL of the backup server API. For example: https://netbackupserver:1556.
Domain Name	The domain name of the user.
Domain Type	The domain type for the user. Allowed values are `NIS`, `NIS+`, `NT`, `vx`, and `unixpwd`.
NetBackup Folder (for pre-NetBackup 10.3)	Physical path on the backup server of the NetBackup commands. You only need to enter this path if NetBackup is not installed in the default location. On a UNIX system the default value is `/usr/openv/netbackup`.
NetBackup Temporary Folder (for pre-NetBackup 10.3)	Physical path on the backup server for NetBackup Self Service temporary files. You only need to enter this path if NetBackup is not installed in the default location. The NetBackup Self Service user must have read and write access to the folder. Additionally, the folder must be on the allowed list in NetBackup. On a UNIX system the default value is `/usr/openv/netbackup/logs/user_ops`. On a Windows system the default value is C:\Program Files\Cohesity\NetBackup.
Command timeout (for pre-NetBackup 10.3)	The number of minutes to wait before a CLI command times out. Leave blank to use the default value.

Table 3-1 Backup Servers settings *(continued)*

Item	Details
Enable In-Place Disk Restore	Allow NetBackup Self Service to offer restore of VMDKs to existing VM. Ensure that the backup server supports **In-Place Disk Restore** using the `nbrestorevm` command.
Enable Usage Insights Data	Allows NetBackup Self Service to submit Usage Insights data to the backup server.
Chunk Size In Hours	Change this value only if instructed to do so by support. When NetBackup Self Service synchronizes backup images from NetBackup, they are retrieved in batches of the chunk size. The default chunk size is 10 hours, but may be reduced in busy systems with lots of backup activities. Reducing the chunk size results in more calls to NetBackup to retrieve a given number of images. If value is empty then the default is 10.
Maximum Backup Duration In Hours	Change this value only if instructed to do so by support. The Maximum Backup Duration represents the maximum time that NetBackup Self Service expects a long running backup to take. The synchronization engine uses this value as a buffer period to make sure that long duration backups are detected. Increase this duration if long running backups are not synchronized into NetBackup Self Service. If value is empty then the default is 24.
Use Pooled Connections (Windows only)	Change this value only if instructed to do so by support. Determines whether PowerShell connection pooling is enabled. Connection pooling is enabled by default to improve performance.
Minimum Pool Size	Change this value only if instructed to do so by support. Minimum number of connections in the PowerShell connection pool. If value is empty the default is 1.
Maximum Pool Size	Change this value only if instructed to do so by support. Maximum number of connections in the PowerShell connection pool. If value is empty the default is 3.

Configuring protection

A protection type defines all the ways a user can protect an asset. If all your users' assets have similar backup requirements you may only need a single protection type. If you offer different protection options for some assets, then each option needs a protection type. Examples of different protection types can include SQL servers, cloud volumes, or a mix of virtual and physical computers. As a general rule you need a protection type for each NetBackup Policy Type you support.

Within each protection type you can define a number of managed, unmanaged and Backup Now protection levels. Managed and Backup Now protection levels are the options that users see when they protect or back up an asset. They can be used to provide varying schedules, retention levels, or other options that you can configure directly on a NetBackup policy.

Each managed protection level or Backup Now level then defines one or more policies. These represent the policies that are created on the backup server in response to a user selecting that level. They define how the policy on the backup server is created, and how it is named. Each unmanaged protection level defines one or more policies. These represent manually created policies on the backup server.

Additionally you can configure a protection level to enable the availability of a Backup Now action. Use this Backup Now action for a computer using the policy it's protected by within the protection level.

Any changes you make to the protection definition are not automatically applied to NetBackup. The changes are not applied to the computers that use this protection type. If the change results in a different set of target policies, existing computers now have an unknown protection level. This change is shown as a black checkmark. You can remove the unknown protection level policies from each asset or container and reapply the modified protection level.

Creating Protection Types

From the **Protection Types** cog button on the **Protection** page, select **Add**.

Table 3-2 Settings on Protection Types

Item	Details
Name	The name identifying a protection type. This option is displayed to the users.
Code	The unique code for this protection type. NetBackup policies use this code in the policy name. For example *[CustomerCode]-[Code]*-[...]

Creating Protection Levels and Backup Now Levels

With a protection type selected, click the relevant **Add Protection Level** option. The **Name**, **Description**, and **Color** properties are all used to distinguish the level for users. The other settings control functionality.

Table 3-3 Settings on Protection Levels and Backup Now Levels

Item	Details
Name	Name of the level (for users).
Description	A description that helps the users decide between different levels.
Code	Code is used when creating NetBackup policies that are associated with this level. It forms part of the name of the policy created. It must be unique within the protection type.
Color	Color is mainly used in the user screens to visually distinguish the different levels that are applied to different computers.
Request type code	Should be left at the default value (DBNEWBACK for protection levels, DBBACKNOW for Backup Now levels) unless you need to customize the system. **Note:** This setting is not relevant to unmanaged protection levels and is not displayed on the screen. For Managed and Backup Now, you can display the field if you select **Show Advanced Settings**.
Visible	Controls the visibility of the level to users. **Note:** This setting is not relevant to unmanaged protection levels and is not displayed on the screen.

Creating Policies

From the details of a **Protection Level** or **Backup Now Level**, click **Add Policy** to create a policy within that level.

Managed protection levels offer the options shown: **Scheduled**, **Scheduled with File Selection**, **Cloud Protection Plan**, **Immediate**, and **Immediate with File Selection**. Backup Now protection levels offer the options shown: **Immediate** and **Immediate with File Selection**.

File Protection policies let you protect a list of files or folders on the target computer. File protection is only available for Standard (0) and MS-Windows (13) Policy Types. **Immediate** policies are run as a one-off backup using a new policy, rather than being added to an ongoing scheduled policy.

On the Policy you can set its **Code**. You can also see the **Target Policy Name** that is created with a combination of the code and the parent protection type and protection level codes.

Table 3-4 Settings on Policies

Item	Details
Name	Used only for administration; not displayed to users.
Code	Code must be unique within the containing level. NetBackup policies use this code in the policy name. For example *CustomerCode*-*Code*-[...]. If there is only one policy within the level you may leave the code blank.
Target Policy Name	Not editable. This field shows an example of the name of the target policy that is created on the backup server when a user selects this level. It is made up of the three codes from protection type, level (either protection level or Backup Now) and policy code. **Note:** This setting is not relevant to unmanaged protection levels and is not displayed on the screen.
Policy Name	This setting is for unmanaged protection level only. The policy determines which backups in the catalog are used to calculate the traffic light status. You can specify an exact policy name or use * to match backups from any policy.

Table 3-4 Settings on Policies *(continued)*

Item	Details
Template Name	The name of a template policy that exists on the backup server which is copied to create the target policy. You can either accept the default name, choose from an existing template, or specify a template name that you create later. **Note:** This setting is not relevant to unmanaged protection levels and is not displayed on the screen. More information is available. See "Creating NetBackup Template Policies" on page 16.
Policy Type	You must specify the NetBackup policy type of the template policy. **Note:** This setting is not relevant to unmanaged protection levels and is not displayed on the screen.
Always Show as Protected	Used to bypass the calculation of a computer's traffic light status. When selected the computer always shows as protected.
Warning (hours)	Used in the calculation of a computer's traffic light status. More information is available. If the field is left blank computers without a backup are flagged for attention. If the field is completed, the computer is flagged for attention when a backup with the correct policy name has not occurred within the specified number of hours. See "About dashboard traffic light status and usage" on page 63.

Table 3-4 Settings on Policies *(continued)*

Item	Details
Single Client Backup Schedule Name	If you enter a value in this field, this **Protection Level** is shown as a **Backup Now** option once a computer has been protected with the level. This field specifies the name of the Schedule that is used when the backup of the single computer is initiated. **Note:** This field applies only to scheduled policies.
Storage Lifecycle Policy Name	The name of the storage lifecycle policy that is used when the **Template** policy is copied.
VM File Restore	Use this field to determine if the virtual machine backup extracts information to allow for file restore. This field is only available for VMware or Hyper-V policies.

Table 3-4 Settings on Policies *(continued)*

Item	Details
Client Selection Type	Use this field to select how computers are identified in a VMware or Hyper-V policy. Options are: ■ **Client Based Display Name**: Use a Client List and the VM Display Name ■ **Client Based Hostname**: Use a Client List and the host name, or the NetBackup client name ■ **Query Display Name**: Use a VMware or Hyper-V Intelligent Policy and use the VM Display Name. This option is the default. ■ **Query Hostname**: Use a VMware Intelligent Policy and the host name, or the NetBackup client name. Hyper-V does not support this option. ■ **Query Computer Name (SCVMM only)**: Use a Hyper-V intelligent policy and the NetBackup Client Name for the SCVMM computer name. ■ **Query Name (SCVMM only)**: Use a Hyper-V intelligent policy and the VM Display Name for the SCVMM name. If you use vCloud Director Imports then you must use **Query Display Name**. This option allows vApp and vDC protection as well as the import only obtaining the VM Display Name. This field is only available for VMware or Hyper-V policies.

Policies that are created within a **Backup Now** level are always set to **Run Immediately**. Backup Now policies do not have the **Warning (hours)** option. Managed protection levels need to contain at least one policy that is not **Run Immediately**, before they are available for users to select.

Schedule Overrides

You may want to have different protection levels change schedule information when the policy that protects the computer is created. This option helps reduce the number of template policies you create on your backup servers. Schedule overrides allow

a number of changes to be made. Use **Add Schedule Override** in a policy to create an override for each schedule that you want to modify.

Table 3-5 Schedule Overrides settings

Item	Details
Name	The name of the schedule that you want to modify. The schedule must exist in the template policy. You can either select from the list or enter the name.
Override Frequency	If this option is selected you can set the frequency at which the schedule runs.
Override Storage Lifecycle Policy Name	If this option is selected you can either select or enter the name of a Storage Lifecycle Policy this schedule uses. This option cannot be used with **Override Retention Level**.
Override Retention Level	If this option is selected you can either select a retention level or enter the number that is associated with the retention level. This option cannot be used with **Override Storage Lifecycle Policy Name**.
Override Backup Window	If this option is selected you can set the backup window for the schedule. You can either use the mouse to create windows in the grid, or use the detailed settings. The values completely replace the backup window that is associated with the schedule.

Multiple Policies within a Level

You may want to specify multiple policies within a single level. For example, you want to provide protection for a database server with policies to back up both the database and the operating system.

After you add a protection level and the associated policies, click **Refresh** link from the cog icon on the **Protection** page. This action ensures that this data matches policies on the NetBackup primary servers. The cog icon becomes animated which indicates that the check is active. The check reviews each defined backup server in the system for the template policies that correspond to the protection levels. Please be aware the system does not check for unmanaged protection levels. Any issues within template policies are highlighted on screen. If you click the highlighted row, further details about the issue that must be resolved are displayed. Once the

issues are resolved on the backup server you can refresh to confirm that they are correct. More information about template policy creation is available.

See “Creating NetBackup Template Policies” on page 16.

Creating Cloud Protection Plans

From the details of a **Protection Level**, click **Add Policy** and select **Cloud Protection Plan** to create a plan within that level.

Self Service uses the details in a **Cloud Protection Plan** to create an appropriate Protection Plan on the NetBackup primary server when assets are protected. The created Protection Plan is named after the codes of the Protection Type, Level, and Plan, and displayed in the Cloud Protection Plan UI.

Cloud Protection Plans can set multiple schedules, but must always have at least one.

Configuring storage

This screen is used to configure the storage name from the corresponding Backup server and protection plan name from NetBackup Self Service.

Configuring tenants

A tenant is an organizational unit and at least one tenant must exist. A tenant can be created with the **Add Tenant** button in the **Tenants** page. The first (admin level) user of the tenant is created at the same time. If any vCloud Director Import sources are defined, the tenant's credentials can be set. A tenant record, related tenant Integration Settings, and the user record are added to the database when you click **OK**.

A tenant’s details can be edited through **Left menu > Tenants**. A tenant's **Customer Code**, which is set when you create a tenant, can be viewed in the **Details** tab. You can also set the **vCloud Director credentials** and the **vCloud Director imports** here. All users that are associated to the tenant are visible in the **Users** tab. Tenant level Integration settings are available in the **Integration** tab. The tenant administrator can subsequently set the updated vCloud Director password when required, using the change facility on their home page vCloud Director Infrastructure tree view node. Tenant level theming can be carried out in the **Theme** tab.

More information about how to define tenant level theming is available. See “Themes” on page 43.

Adding users

You can add additional users to the tenant in a number of ways:

- Manually through the portal from the **Left menu > Tenants > Users** tab
- Active Directory (**Users > Import Active Directory**). The Cost Center Code must be the same as that found in the Tenant record.
- Base Data Import through CSV (**Users > Import /Export Users**). When you click on **Import/Export Users** a new form is displayed. The form has the option to select a CSV file to import users. You also have the option to export the current users to a CSV or unicode text files. The Cost Center Code must be the same as that found in the Tenant record.

Note: Once a user is associated to a tenant this association cannot change.

A user record can be deactivated to prevent access to the system. If using Forms Authentication, password rules can be defined using a number of criteria. These rules can be configured in **Left menu > Settings > System Configuration**.

A tenant user with an `Administrator` access profile can manage their own user records.

Access rights

By default all users can carry out all possible actions on every computer that is registered to their tenant. This ability depends on the functionality that the computer can support. All users can see the monthly usage data for their tenant. You can control the available actions at two levels: globally or per tenant.

Control of these access rights is available through **Left menu > Settings > System Configuration > Integration Settings tab** in the **NetBackup Adapter Access Rights** section. The access rights are: **Allow Backup Now**, **Allow Protect Machine**, **Allow Restore File**, **Allow Restore Vm**, **Allow Unprotect Machine**, **Allow Usage Report**, **Allow Register for File Restore**, **Allow Restore Sql**, **Allow Restore Oracle**, **Allow Restore Cloud Asset**, **Allow Agentless Restore File**, **Allow Agentless Restore File To Alternate Vm**, **Allow Expire Backups**, **Allow Restore Disks**, **Allow Restore Kubernetes Namespace**, **Allow Protect MSSQL**, **Allow Unprotect MSSQL**, and **Allow Restore Longterm Backup**.

To globally enable or disable an action for all users

1. Click the required **access right** in the **NetBackup Adapter Access Rights** section.
2. Choose **Enabled** or **Disabled** in the **Value** field.

   Ensure **Allow Tenant Override** is not checked.
3. To allow different tenants to have different actions available to them.
   - Click the required **access right** in the **NetBackup Adapter Access Rights** section
   - Choose **Enabled** or **Disabled** in the **Value** field. This setting is the default for any existing tenants or any new tenants
   - Check **Allow Tenant Override**

Only a non-tenant associated administrator who has access to all of the Tenants can change the value.

To configure the value of the access rights for each tenant

1. Select the **Integration** tab in the **Tenant Admin** screen (**Left menu > Tenants > *select a tenant***).
2. Click the required **access right** in the **NetBackup Adapter Access Rights** section.
3. Choose **Enabled** or **Disabled** in the **Value** field.

Registering computers

Computers within the estate must be registered to NetBackup Self Service. This requirement includes the name for display in the UI and configuration data for use with NetBackup.

You can register a computer in three different ways: through the user interface, through NetBackup cloud asset import, or automatically through vCloud Director import. A single tenant can have more than one source of computer, for example, virtual machines imported from vCloud Director and physical computers imported through the API.

Registering a computer with the user interface

You can register a computer from the **Assets** page on the home page with **Register Computer**. Help text is available to assist in completion of the data. Fields are validated for accurate data either during entry or when you click **Save**.

To remove a computer registration, go to the **Assets** list on the **Assets** home page, select an asset, and use the **Remove Registration** link from the **Actions** button. Computer registration cannot be edited so it is recommended that a computer registration is deleted and recreated if changes are required. Be sure to use the same computer code when you recreate a computer registration.

The computer registration process includes an automatic refresh of protection data and image data from NetBackup. Protection data indicates what is protected either by schedule or by a one-off Backup Now task. If you click **Refresh NetBackup Data** from the **Actions** button on the asset details page, you can synchronize protection and backup images of a computer. Typically synchronization should not require manual intervention. Exceptions might be if you want to immediately see images from a new protection policy or images that have been created manually.

See the SDK documentation in the Install directory.

Registering by vCloud Director Import

You can automatically import a vCloud hierarchy from vCloud Director and register the computers with NetBackup Self Service. The import is performed on a tenant by tenant basis using individual credentials.

A vCloud Director import must define the vCloud Director instance from which the hierarchy is imported. Additionally, it must specify the NetBackup Self Service settings you want to associate with it.

An import must specify a **Protection Type** and a **Backup Server** that the imported hierarchy is associated with.

An import may optionally use virtual data center (vDC) filtering. When vDC filtering is enabled, only vDCs in the filter are imported. Filtering occurs on a per tenant basis and each must be set up with a filter to import any vDCs. Each vDC should appear only in a single tenant's filter.

When vDC filtering is disabled, all vDCs that are visible through the import credentials are imported.

Use the **Add Import** option on the **Asset Imports > vCloud Director** page to create a new vCloud Director Import. Follow the on-screen prompts to create a corresponding **vCloud Import Integration Setting** section.

If the vCloud Director is version 9.5 or higher, you must specify an administrator user name and password for the vCloud Director system. You must also add credentials for each of the underlying vCenter servers that the vCloud Director manages if you use version 10.1 or earlier. The credentials are not required for version 10.2 and later. Each vCenter server must be running version 6.5 or higher. Select **Manage vCenter Credentials** and then **Add vCenter Credential** to add each vCenter. The vCenter is identified using the **URL**. This URL must match the name that is registered in vCloud Director.

You must specify logon credentials at a tenant level to enable import. The credentials in vCloud Director are defined against an Organization and must have the **General > Administrator View** right. Only a single tenant can import computers from any vCloud Director Organization.

When you create a new tenant, the **Add Tenant** form supports specifying credentials for a single vCloud Director system as part of the tenant creation process. You can update credentials on the **Details** tab in **Tenant administration**. Once the initial password is set, a tenant-administrator can update the vCloud Director password that is used to access vCloud Director. The tenant-administrator updates the password through a drop-down on the root node of their Computers list.

Table 3-6 vCloud Director Import Settings

Item	Details
vCloud Director API URL	This value should be set to the URL of the vCloud Director API, in the format of `https://hostname/api/`.
Location	The name of the NetBackup backup server the computers are registered to.
Online	Indicates if the vCloud Director instance is considered online. Self Service does not use the instances that are not online.
Ignore SSL Certificate Errors	This option allows the Self Service to connect to vCloud Director instances where the SSL certificate is not valid.
vCloud UserName	The username that the tenant uses to connect to the vCloud Director API. Each tenant must have their own credentials. It must be in the format *userid@vOrg*. Must be set at the tenant level only.
vCloud Password	The tenant's corresponding vCloud Director password. Must be set at the tenant level only.
Protection Type Code	The protection type that is applied to imported computers.
Use vDC Filter	Set to enable vDC filtering.

Table 3-6 vCloud Director Import Settings *(continued)*

Item	Details
vDC Filter	The filter to apply to vDCs during an import. This filter is a comma separated list and vDC names are case-sensitive. Set at the tenant level only.
Display Name	The name that is displayed for users. This name is displayed on the default view of the home page
Include Metadata	Determines if the metadata should be included in the import.
vCloud Admin UserName	The administrator user for vCloud in the format: `Administrator@System`. Required if using vCloud Director 9.5 or higher.
vCloud Admin Password	The password of the account with Admin credentials in vCloud. Required if using vCloud Director 9.5 or higher.

Computers that are imported from vCloud Director are displayed to the tenant-user in a two-paned tree-view. Computers are listed within their parent containers. If the computer is from vCloud, containers display in left pane. When you click on the lowest level container, the contents are displayed on the right pane. Protection can be applied at either the container or the computer level. When only non-vCloud Director computers are registered, they are displayed in a full width list.

Registering Kubernetes Assets by NetBackup Import

You can automatically import Kubernetes assets from NetBackup and register them with Self Service. The import is performed on a tenant by tenant basis, using filters or individual credentials.

You must define the NetBackup server from which the assets are to be imported.

Additionally, you must specify the Self Service settings you want to associate with it.

You must specify a Protection Type and a Tenant that you want to associate the imported assets with.

You must specify at least the Kubernetes cluster to identify the imported assets. You may also specify a set of other filter criteria (one or multiple names spaces) which every asset must meet for it to be imported. During setup you can preview the results of the current filter criteria.

Registering Nutanix Assets by NetBackup Import

You can automatically import Nutanix assets from NetBackup and register them with Self Service. The import is performed on a tenant by tenant basis. The import uses filters or individual credentials.

You must define the NetBackup server from which the assets are to be imported. Additionally, you must specify the Self Service settings you want to associate with it.

You must specify a Protection Type and a Tenant that you want to associate the imported assets with.

You must specify at least the Nutanix prism central or Nutanix Cluster to identify the imported assets. You may also specify a set of other filter criteria which every asset must meet for it to be imported. The criteria can include things like project name or VM Display name (starts with, ends with, or contains). During setup you can preview the results of the current filter criteria.

Additional validation exists for when you save the Nutanix import. Self Service validates that the selected primary server and the selected protection plan are configured with the storage in the **Configure Storage** screen. This validation has been added because we need storage information for creating the protection on the fly in NetBackup primary server from NetBackup Self Service.

Be aware that during the import NetBackup Self Service does not allow duplicate assets with the same display name. This behavior is default behavior for all workloads in NetBackup Self Service.

Registering Cloud Assets by NetBackup Import

You can automatically import cloud assets from NetBackup and register them with Self Service. The import is performed on a tenant by tenant basis, using individual credentials.

You must define the NetBackup server from which the assets are to be imported. Additionally, you must specify the Self Service settings you want to associate with it.

You must specify a Protection Type and a Tenant that you want to associate the imported assets with.

You may also specify which types of cloud assets are to be imported.

You must specify logon credentials for each import. These credentials must only have access to the specified tenant’s assets.

Registering vCenter Assets by NetBackup Import

You can automatically import vCenter assets from NetBackup and register them with Self Service. The import is performed on a tenant by tenant basis, using filters or individual credentials.

You must define the NetBackup server from which the assets are to be imported.

Additionally, you must specify the Self Service settings you want to associate with it.

You must specify a Protection Type and a Tenant that you want to associate the imported assets with.

You must specify at least the vCenter server to identify the imported assets. You may also specify a set of other filter criteria which every asset must meet for it to be imported. During setup you can preview the results of the current filter criteria.

Alternatively, you can set up individual credentials for the import and use the NetBackup RBAC configuration to determine which assets are imported.

Configuring the home page

The home page allows the user to view the current status of their assets and initiate actions with a minimum of mouse clicks.

The top sections are a traffic light-style status, consumption total tile, and consumption trend graph. Visibility of these top sections can be configured within **Integration Settings**.

Home page integration settings

The integration settings that are shown affect the display and information that is included in the **Status** and the **Usage** panels.

You can find the relevant Integration settings either by **Left menu > Settings > System Configuration > Integration Settings** or **Left menu > Tenants > select a tenant > Integration**.

Table 3-7 NetBackup Adapter

Item	Details
Contracted Space (TB)	Used to augment **used space** display; maintainable at tenant level.
Usage Retention Period (months)	The number of months retained for display in Usage trend graph or list.

Table 3-7 NetBackup Adapter *(continued)*

Item	Details
Show Traffic Light Tiles	This setting determines whether traffic lights are displayed on the home page.
Show Consumption Total Tile	This setting determines whether the total usage is displayed on the home page.
Show Consumption Trend Tile	This setting determines whether the usage trend graphs are displayed on the home page.
Quota enforcement	This setting toggles the tracking of space usage at the tenant level. It helps enforce the contracted space that every tenant is given with values set in **Contracted Space (TB)**. By default this option is disabled. To enable quota enforcement, this option must be enabled for each tenant.

The NetBackup adapter access rights controls the actions all users, individual tenants, or specific users are allowed to perform against an asset.

Table 3-8 NetBackup Adapter Access Rights

Item	Details
Allow Backup Now	Determines if the Backup Now option is displayed.
Allow Protect Machine	Determines if the Protect Computer option is displayed.
Allow Restore File	Determines if the Restore File option is displayed. This option also includes the Restore Folder option.
Allow Restore Vm	Determines if the Restore Vm option is displayed.
Allow Restore Kubernetes Namespace	Determines if the Restore Kubernetes Namespace option is displayed.
Allow Restore Nutanix VM	Determines if the Restore Nutnaix VM option is displayed.
Allow Restore Longterm Backup	Determines if the Restore Longterm Backup option is displayed.

Table 3-8 NetBackup Adapter Access Rights *(continued)*

Item	Details
Allow Unprotect Machine	Determines if the Unprotect Computer option is displayed.
Allow Usage Report	Controls the display of the Usage report on the home page.
Allow Register for File Restore	Determines if the Register for File Restore option is displayed.
Allow Restore SQL	Determines if the Restore SQL Database option is displayed (if backups are found).
Allow Restore Oracle	Determines if the Restore Oracle Backups option is displayed (if backups are found).
Allow Restore Cloud Asset	Determines if the Restore Cloud Asset option is displayed.
Allow Agentless Restore File	Determines if the **Restore File** option is displayed. This option also includes the Restore Folder option.
Allow Agentless Restore File to Alternate Vm	Determines if the **Restore File to Alternate VM** option is displayed. This option also includes the **Restore Folder** option.
Allow Expire Backups	Determines if the **Expire Backups** option is available on the **Asset > Backups** tab.
Allow Restore Disks	Determines if the **Restore Disks** option is displayed.
Allow Protect MSSQL	Determines if the **Add Protection** option for SQL Server instance/database is displayed.
Allow Unprotect MSSQL	Determines if the **Remove Protection** option for SQL Server instance/database is displayed.

More information about access rights is available in the **Configuring Tenants** section.

See “Configuring tenants” on page 31.

NetBackup Adapter Usage controls features within the Usage tab.

Table 3-9 NetBackup Adapter Usage

Item	Details
Charging Type	Basis of charge calculation: New backup, Consumed Capacity, or none; maintainable at tenant level
Use Data Transferred values	Controls whether to use Transferred Size or Image Size in usage statistics. Transferred Size values can be lower, such as when you use Accelerators. Transferred Size values only available on NetBackup 7.7.1 and later.

Configuring mail/SMTP server

SMTP server configuration involves specifying the mail server's host, port, authentication credentials, and security protocols to allow automated email to be sent.

Find the SMTP configuration in **Left Menu > Task > Send Email** and enter the SMTP server details and enable SSL (if required) to complete the configuration.

Table 3-10 SMTP server details

Item	Details
Due Date	Displays the date when the **Send Email** task is expected to run.
Last Run	Displays the date when the **Send Email** task was last run.
Enabled	Select the check box to use SSL to access an SMTP mail server. By default, the check box is not enabled.
Max Send Retries	Enter maximum retries allowed to send emails.
Delivery Method	Select the delivery method for emails.
Host	Enter the hostname of the SMTP mail server to be used for SMTP transactions.
Port	Enter the port number to connect to the SMTP mail server. The default value is 25.
Pickup Directory Location	Enter the directory where applications can save emails for processing by the SMTP server.

Table 3-10 SMTP server details *(continued)*

Item	Details
Target Name	Enter the Service Provider Name (SPN) to use for authentication when using extended protection for SMTP transactions. This attribute has no default value.
Use SSL	Select the check box to use SSL to access an SMTP mail server.
Use Default Credentials	Select the check box to use the default user credentials to access the SMTP mail server for SMTP transactions. By default, the check box is not selected.
Username	Enter the username to use for authentication to the SMTP mail server.
Password	Enter the password to use for authentication to the SMTP mail server.
Confirm Password	Enter the password again.

Click **Run Now** to configure the SMTP server configuration and to run the send email task or click **OK** to configure the SMTP server configuration.

Chapter 4

Customizing Self Service

This chapter includes the following topics:

- Language settings
- Themes
- Notices
- Email Template Customization Screen

Language settings

Although the portal supports multiple languages, NetBackup Self Service solution data is currently only available in a subset of those languages. These languages include English, Simplified Chinese, Japanese, and French. This setting encompasses language and regional settings, including date formats.

Themes

You can adjust the pre-shipped NetBackup Self Service theme.

To customize the NetBackup Self Service theme, you should modify the variables that are defined in the `Theme`*`ThemeName`*`.css` file under `%Program Files%\Cohesity\NetBackup Self Service` *`version`*`\Website\wwwroot\css`.

```
:root {
    --headerHeightNumber: 60px;
    --headerLogoImage: url(../Images/Icons/Netbackup/nss_logo.png);
    --headerBackgroundImage: none;
    --headerBackgroundColor: #F9F9F9;
    --pageOuterColor: #F0F0F0;
    --pageOuterBackgroundImage: none;
```

```
    --noticeInformationBackgroundColor: #FFFFFF;
    --noticeInformationTextColor: #1D1D1D;
    --noticeAlertBackgroundColor: #990101;
    --noticeAlertTextColor: #FFFFFF;
}
```

If you want to modify the default theme file, copy the `ThemeDefault.css` to a new file, such as `ThemeVeritas.css`. Then, modify the `ThemeVeritas.css` accordingly. Then, modify the `appsettings.json` file as shown:

```
"Theme": {
    "DefaultName": "Veritas",
    "AllowTenantOverride": false
  }
```

If you want to give a tenant a different theme, you need to create a theme file for the tenant. If you have a tenant named **TeantA**, then you can create a theme file `ThemeTenantA.css`. The default theme is applied for tenants without a customized theme file.

To enable the tenant-specific theme feature, you must change the `appsettings.json` file as shown:

```
"Theme": {
    "DefaultName": "Default",
    "AllowTenantOverride": true
  }
```

Dark mode

You can toggle dark mode settings in the UI or set it as per-browser preference.

Notices

You can display news ticker-style notices at the top of the home page. These notices can be either alert type or information types. You can change the theme of the notice and filter the notice by tenant. You can control the publication of a notice by both start date and end dates.

A tenant with an access profile of **Administrator** can maintain their organization's notices.

Email Template Customization Screen

Use the Email Templates screen to customize the email messages that are sent during restore and backup operations. When you click **Save**, the changes are stored in the database.

Required access

You must have the **Admin Settings** access right to customize email templates.

Customize an email template

1. Go to **Settings** > **Email Templates**.
2. Select the template that you want to update.
3. Edit the subject and message for each required language.
4. Click **Save**.

Restore default content

To restore the factory default subject and message for a template, click **Reset**.

Upgrade considerations for version 11.1 or earlier

In releases earlier than 11.2, customized email templates were stored as XML files in the `Website\EmailTemplates` folder. Starting with 11.2, customizations are stored only in the database. Existing XML customizations are not imported automatically during upgrade.

- Before you upgrade, copy any customized XML files from the previous installation's `Website\EmailTemplates` folder to a safe location. The upgrade replaces the installation directory and removes those files.
- After the upgrade, open each customized template in **Settings** > **Email Templates**.
- Re-enter the subject and message by using your saved XML files as a reference.
- Click **Save** to store the customizations in the database.
- After this one-time step, manage email templates only from the Email Templates page.
- Include the database in your backup procedures to preserve customized templates. Future upgrades do not require copying XML files.

Chapter 5

User authentication methods

This chapter includes the following topics:

- About user authentication methods
- Forms based authentication
- Windows Authentication
- Active Directory Import
- Configuring Self Service to use Federated Single Sign-On

About user authentication methods

NetBackup Self Service supports three different methods of authenticating users:

- Forms based authentication that uses a user name and password. This configuration is the default configuration that ships with Self Service.
- Windows authentication, optionally with an Active Directory Import. This option is only suitable for Enterprise type deployments.
- Federated Single Sign-On by the WS-Federation Passive Protocol.

Forms based authentication

Users access the Self Service portal by entering a user ID and password on the logon page. This configuration is the default method of accessing the system and no additional configuration is required.

Password rules can be defined in the **Password Policies** category of .

Windows Authentication

To use Windows Authentication, the users must be set up in the database with the user names that match the users' domain names. This format is either *DOMAIN_NAME\username* or *username*. The format depends on the system setting.

Configure `REMOVE_DOMAIN_NAME` in **Left menu > Settings > System Configuration**. Switch it on if it uses *`firstname.lastname`* or switch off if it uses *`DOMAIN\firstname.lastname`*.

Once at least one Windows user has access to the Administration area, disable both Anonymous Authentication and Forms Authentication in IIS. Then enable Windows Authentication. This configuration in IIS insures the `web.config` file is updated and Self Service address is changed accordingly.

You can only use the shipped `admin` user ID to access the system until Windows Authentication is configured in IIS. After that point, no manual logon is available.

Note: If you use Active Directory import to synchronize users, ensure that at least one user is associated to the `Supervisor` access profile on initial import. Otherwise, access to the Admin area is compromised.

Note: These instructions only apply to configuration on initial implementation of the system and are not appropriate for later changes to the logon protocol. This limitation is due to effect on historical data.

Active Directory Import

You can synchronize Self Service with Active Directory for easier maintenance. Import is managed from a scheduled import task. This process lets you specify a time or frequency for the process. The schedule should reflect the full user set as any user that is not included is deactivated in Self Service.

You can create multiple import profiles with a different source for each profile. For each profile a Self Service access profile, cost center, and user account status must be specified. The users may be automatically assigned to zero or more user groups. The user group, however, must already exist in Self Service. You can source the Self Service user name from either **Full Name** (default) or **Display Name**. You can select a language, otherwise the system base language is used. You can specify an import profile by group or organizational unit, and with or without children included.

Import profiles are processed from the top of the list so you can modify the order to fit your requirements. If the same user is present in multiple profiles, only the **Imported User Fields** from the latest profile that is processed apply. User group membership is updated from all profiles.

The user that is specified within the Active Directory Import requires the **List Contents** and **Read All Properties** rights at the root level of the domain. These rights are required so that the user can search all organizational units and organizational groups and import all users.

A system configuration setting lets you control whether the Domain Name is pre-pended to the user ID when you import it. Find the system configuration setting in **Left menu > Settings > System Configuration**. Verify the appropriate setting value before you create the first user accounts. Subsequent change causes new user accounts to be created and existing accounts are disabled, along with the impact on accessing historical requests. A change of SAM account name causes the creation of a new Self Service user account.

You can create locally maintained Self Service users for the records that are not maintained in Active Directory. Active Directory update ignores these users.

Note: If you use Windows Authentication, ensure that at least one user is associated to the `Supervisor` access profile on initial import. Otherwise access to the Administration area is compromised.

Note: These instructions only apply to configuration on initial implementation of the system. They are not appropriate for later changes to the logon protocol due to effect on the user-maintained method

---

Configuring Self Service to use Federated Single Sign-On

Self Service supports Federated Single Sign-On through the WS-Federation Passive Protocol. It is implemented with Microsoft Windows Identity Foundation (WIF), and uses Security Assertion Markup Language (SAML) tokens for claims transfer. It does not, however, support the SAML2 Protocol, SAML-P.

When Self Service is installed, it is configured with Forms Authentication that requires the first logon to use the **admin** account.

To authenticate through the identity provider:

1. Create users in the Self Service database, who correspond to users in the identity provider.
2. Edit the Self Service `appsettings.json` file to enable federated single sign-on.

Create a user in Self Service

The **User ID** is used to identify users in Self Service. **Claims** are used to identify users in the identity provider. For authentication to succeed, users in Self Service must have a **User ID** that matches the value in one of the claims from the identity provider.

Self Service looks at the following claims when it attempts to find the Self Service user: **Name**, **Email**, **Windows Account Name**, and **UPN**. Typically **Name** and **Windows Account Name** have the format `domain\username`, and typically **Email** and **UPN** have the format `username@domain`.

You can enter Users through the portal or import in bulk, either directly from Active Directory or by a `.CSV` file.

Edit appsettings.json to enable Federated Single Sign-On

To change the `appsettings.json` file to enable federated single sign-on:

1. Navigate to *`install_path`*`\WebSite`.
2. Open `appsettings.json` with Notepad as Administrator.
3. Find the `<FederationAuthentication>` section and set `Enabled` to `true`, and set `Wtrealm` and `MetadataAddress` to the desired values.
4. Save the `appsettings.json` file.

If you have to switch back to **Forms Authentication**, edit the `appsettings.json`, and set the `Enabled` option to `false` in the `FederationAuthentication` section. One instance where you would switch back to **Forms Authentication** is to recover from a problem.

Log on to Self Service

To confirm that the system is fully configured for Federated logon:

1. Close and re-open Internet Explorer
2. Restart IIS
3. Enter the URL of Self Service

4. If your environment uses test certificates, accept the two certificate errors
5. Enter the credentials for the previously created user. The user should successfully log on.

Chapter 6

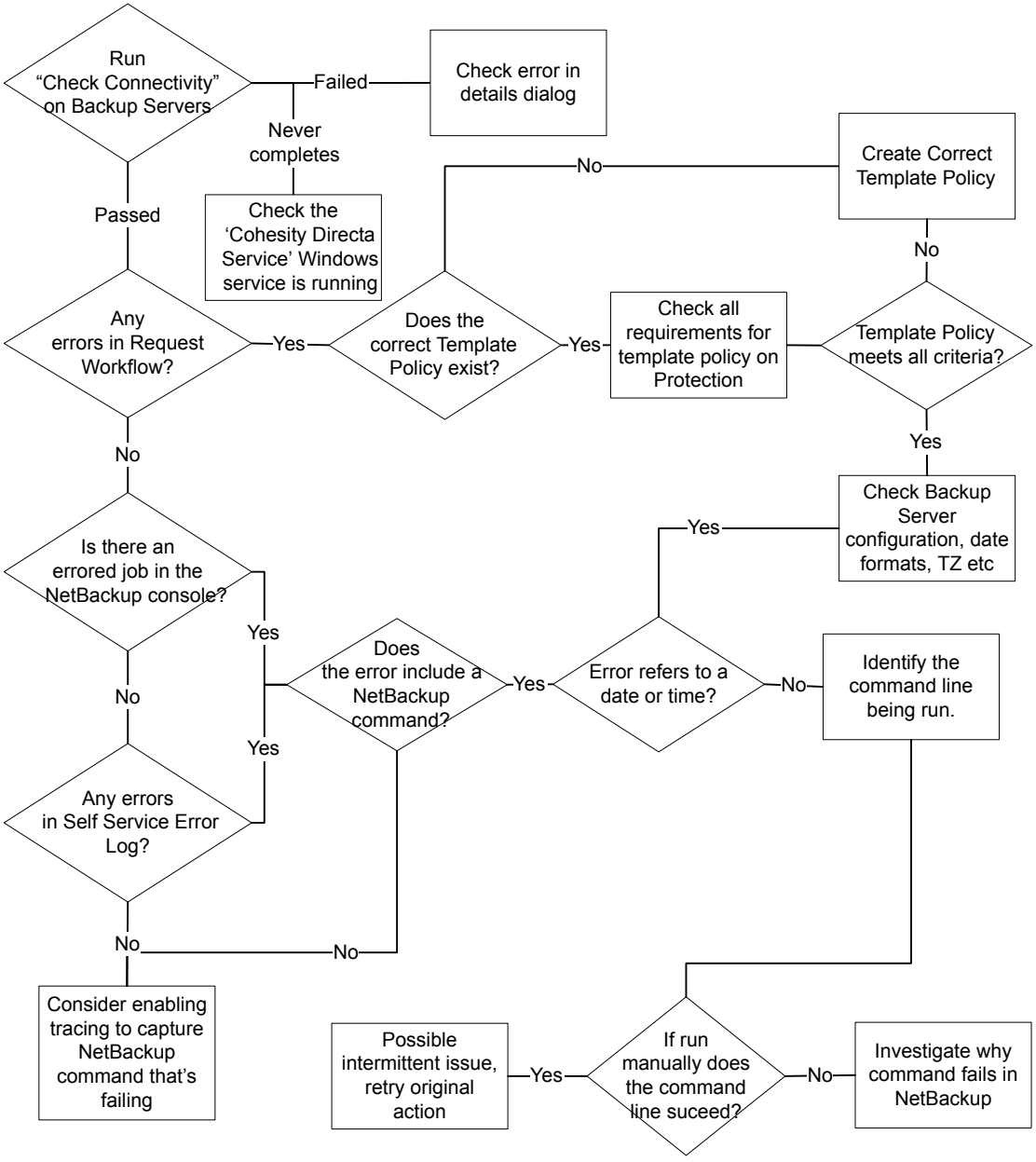
Troubleshooting

This chapter includes the following topics:

- About troubleshooting
- Where to find troubleshooting information
- Impersonation of a tenant user
- Issues with Remote PowerShell to Windows primary servers
- Issues with HTTPS configuration
- Configuration troubleshooting

About troubleshooting

The first step in troubleshooting a problem is to determine if it lies with Self Service or NetBackup itself. Unless there is an error or a failure message that points in a clear direction, the best first course of action is to try and manually perform the action on the NetBackup console. If this action fails it points to a NetBackup issue. Once NetBackup issues have been ruled out proceed with diagnosing in Self Service.


Run
“Check Connectivity”
on Backup Servers
Failed
Check error in
details dialog
Never
completes
Check the
‘Cohesity Directa
Service’ Windows
service is running
Passed
Any
errors in Request
Workflow?
Yes
Does the
correct Template
Policy exist?
No
Create Correct
Template Policy
Yes
Check all
requirements for
template policy on
Protection
Template Policy
meets all criteria?
No
Yes
Check Backup
Server
configuration, date
formats, TZ etc
Yes
Is there an
errored job in the
NetBackup console?
Yes
No
Does
the error include a
NetBackup
command?
Yes
Error refers to a
date or time?
No
Identify the
command line
being run.
Yes
No
Any errors
in Self Service Error
Log?
Yes
No
No
Consider enabling
tracing to capture
NetBackup
command that’s
failing
Possible
intermittent issue,
retry original
action
Yes
If run
manually does
the command
line suceed?
No
Investigate why
command fails in
NetBackup

Where to find troubleshooting information

Check Connectivity

On the **Backup Servers** page the **Check Connectivity** button tests the connection to each backup server in the system. Any failures show as a red cross which can be clicked to show error information.

Self Service Error Log and additional activity reporting

Various log files, including the Error Log, are found in `%ProgramData%\Cohesity\NetBackupSelfService`. This directory is also where the Integration, Audit, and Email logs are found. Errors can contain a System Reference which can be used to tie it back to a specific Request, and hence an Action.

If trying to locate failed NetBackup commands, performing a search for the text `/bin` or `\bin` can be helpful.

NetBackup Command-Line Errors

Self Service works by running NetBackup Commands on the command line of the primary server. If there is a problem running a command, it is included in the error in Self Service. Locating these errors is very helpful. Once you have an error with a NetBackup Command line, you can copy the command and try running it manually on the primary server. This technique is useful for troubleshooting.

Errored Jobs in NetBackup Console

Check for any errors on the NetBackup Activity Monitor especially against Job IDs that are identified.

Checking Template Policies

Template Policies must be configured in certain ways to function correctly. When you check policy templates, refer to the **Protection** page in Admin. Click **Export Template Policies** from the **Protection Types** cog button to generate a summary of outstanding changes.

Problem assets

An amber or a red cog in the **Assets** page highlights the problem assets.

- A red cog indicates that a synchronization or an activity failure error has occurred previously.
- An amber cog indicates that a synchronization or an activity failure error has occurred previously but that an activity is currently in progress.

From the details pop-up select the **Details** tab which provides you with the last error and the stack trace.

Synchronization Errors

Can be viewed as an MSP admin user in computer detail pop-up.

Details incorrect for asset

In the case that image or protection details don't seem correct for an asset, run **Refresh NetBackup Data** for the asset using the **Actions** button.

Tracing

Tracing can be configured to analyze problems on a more detailed level. This method is a more advanced troubleshooting method. Do not attempt this method without the assistance of support. See the `ReadMe.txt` in *`Services Site`*`\Logs` and *`Panels Site`*`\Logs`.

Impersonation of a tenant user

You can impersonate a tenant-user to see their home page view, as well as perform actions on their behalf.

From the home page, when you click the logged on user initials icon, the option **Act as another user** is displayed. If this option is selected, it displays a user list. Select the required tenant-user and their home page view is displayed.

Issues with Remote PowerShell to Windows primary servers

Concurrent Remote PowerShell Connection Limits

The NetBackup primary server limits the number of remote connections. The server defaults are typically sufficient.

In high usage installations it may be necessary to increase this limit. If the limit is exceeded the following error may occur:

```
NetBackup server name Connecting to remote server NetBackup server
name failed with the following error message : The WS-Management
service cannot process the request. The maximum number of concurrent
shells for this user has been exceeded. Close existing shells or
raise the quota for this user. For more information, see the
about_Remote_Troubleshooting Help topic.
```

To increase the limit:

1. On the NetBackup primary server, run the PowerShell command that is shown to determine the number of connections allowed:

   ```
   Get-Item WSMan:\localhost\Shell\MaxShellsPerUser
   ```

2. On the NetBackup primary server, run the PowerShell command that is shown to increase the number of connections allowed:

   ```
   Set-Item WSMan:\localhost\Shell\MaxShellsPerUser interger_value
   ```

Concurrent User Operation Limits

Symptom of reaching this limit is an error similar to:

```
RunCommand failed.
"C:\Program Files\Cohesity NetBackup\NetBackup\bin\admincmd\bpimagelist"
"-d" "03/02/2015 09:58:11" "-e" "03/02/2015 11:58:11"
"-json_compact"
Run-Process script threw exception:
Starting a command on the remote server failed with the following
error message : The WS- Management service cannot process the
request. This user is allowed a maximum number of 15 concurrent
operations, which has been exceeded. Close existing operations for
this user, or raise the quota for this user. For more information,
see the about_Remote_Troubleshooting Help topic.
```

Windows 2012 defaults to 1500. On the NetBackup primary server, run the command that is shown to increase this limit:

```
winrm set winrm/config/Service
@{MaxConcurrentOperationsPerUser="1500"}
```

PowerShell Connection Pooling

By default, Windows locations use PowerShell Connection Pooling. This option allows much higher throughput when you call PowerShell on the NetBackup primary server. Higher throughput is achieved because every call does not require the computer to create and destroy a new Run Space.

Settings

Table 6-1 The backup server fields that are used for PowerShell Connection Pooling

Name	Details
NetBackup Use Pooled Connections	Determines whether PowerShell connection pooling is enabled. Connection pooling is enabled by default to improve performance. Only change this value if instructed to do so by Support.
NetBackup Minimum Pool Size	Minimum number of connections in the PowerShell connection pool. If value is empty, the default is 1. Only change this value if instructed to do so by Support.
NetBackup Maximum Pool Size	Maximum number of connections in the PowerShell connection pool. If value is empty, the default is 3. Only change this value if instructed to do so by Support.

Diagnostics

The diagnostic tracing captures a large amount of information about the PowerShell connection creation, use, and disposal.

The following PowerShell script can be used to find information about the connections to a NetBackup primary server:

```
$machineName = 'netbackup_primary_server_machine_name'
$userName = 'user_name_-_same_as_the_location_integration_setting'
$password = '<password>'

$connectionURI = ('http://{0}:5985/wsman' -f $machineName)

$securePassword = ConvertTo-SecureString $password -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential
($userName, $securePassword)

$connections = Get-WSManInstance -ConnectionURI $connectionURI
-Credential $credential -ResourceURI shell -Enumerate #| where
{ $_.Owner -eq $userName }


if($connections.length -eq 0) { "There are no remote PowerShell
```

```
connections" }

$connections | ForEach-Object {
    # To remove the connection, uncomment the line below
    # Remove-WSManInstance -ConnectionURI $connectionURI shell
      @{ShellID=$_.ShellID}

    $_
    "Owner: {0}" -f $_.Owner
    "HostName: {0}" -f (Resolve-DnsName $_.ClientIP | select
    -expand NameHost)
    "-------------------------------------------------------"
}
```

Monitoring Scheduled Tasks

Self Service runs a number of scheduled tasks in the background. These scheduled tasks synchronize data between external systems and keep the user interface as up to date as possible. The status and timing of these tasks is displayed to the left of the **Monitoring** page when logged on as non-tenant administrator user.

The action cog is red if there are any problems running a particular task. If you click the task name, the **Scheduled Task Details** window is displayed. This window shows any error messages, which aids the troubleshooting process. You can resolve errors and then click **Run Now** in the drop-down to retry the task.

The **Activity** area of the **Monitoring** page displays tasks queued for action. If this queue is over ten items and shows no sign of change over several minutes, there could be a problem with the main task engine of Self Service. Make sure the Windows Service is running and review the Error log found in `%ProgramData%\Cohesity\NetBackupSelfService`. You can initiate a rebuild of the utilization data from the **Monitoring** page. This action updates both current month and previous months' data.

Table 6-2 Background tasks and descriptions

Background task	Description
`System Sync`	Imports backup images from all backup servers since the last time it ran. The task expires old backup images and calculates usage. This task runs once per day on schedule.

Table 6-2 Background tasks and descriptions *(continued)*

Background task	Description
`System Update`	Performs system updates such as syncing backup images and updating active requests. This task runs once per minute on schedule.
`Asset Import`	Synchronizes the computers from NetBackup Import or vCloud Director, according to configured imports. This task runs once per day on schedule but can be initiated manually.

Issues with HTTPS configuration

Starting with NetBackup Self Service 10.0, the default configuration for Self Service is HTTPS. Cohesity made this change for security reasons.

The steps that are shown can assist you as you troubleshoot any issues with your HTTPS configuration.

To verify HTTPS is correctly configured:

1. Make sure that the installer created an SSL certificate. Search the **Start** menu for **Internet Information Service**. You can see bindings with corresponding SSL certificate.
2. Make sure the binding for port 443 is created and the certificate is assigned to that port. Search the **Start** menu for **Internet Information Service**. You can see bindings with corresponding SSL certificate.
3. Validate the integration settings. Under **Admin > Integration Settings**, confirm all URLs are HTTPS.
4. Under **Admin > Integration Settings** confirm the Panel URL and Service URL use the same host name.

Example:

```
https://example.com/NetbackupSelfServiceNetBackupPanels
https://example.com/NetBackupSelfServiceNetBackupServices
```

Configuration troubleshooting

Follow this table to troubleshoot configuration.

Table 6-3 Configuration troubleshooting

Symptom	Likely cause	Action
ApplicationKey in central config does not match	Wrong key or stale Config	Fix `Install.ini`; remove stale Config.
`validateconfig` failed	Missing or corrupt Config	Run `-readconfig`; run `-initconfig` with a matching key.
Portal login fails after DR	Wrong ApplicationKey	Restore the correct key from backup.
Second node cannot start	Copied `.enc` file	Use the same hex key per node; run local `initconfig`.
Upgrade aborted on Config copy	Destination key differs	Align keys or remove stale destination Config.
Dapi / integration errors	ChangeMe password	Configure Dapi after installation.

Appendix A

NetBackup policy types

This appendix includes the following topics:

- List of NetBackup policy types

List of NetBackup policy types

Table A-1 is a list of the Policy Types available in NetBackup and their associated IDs. You must use these when you create the Policy Types Integration Setting.

Table A-1 Policy types and associated IDs

ID	Name	NetBackup Self Service	Backup selection
0	Standard	Protection; file restore	Defined in policy template and applies to all clients in the policy.
4	Oracle	Protection (client based only); database restore	Defined by a script that resides on the client.
6	Informix-On-BAR	Not supported	
7	Sybase	Protection	Defined by a script that resides on the client.
8	MS-SharePoint	Protection	Defined in policy template and applies to all clients in the policy.
10	NetWare	Not supported	
11	DataTools-SQL-BackTrack	Not supported	
12	Auspex-FastBackup	Not supported	

Table A-1 Policy types and associated IDs *(continued)*

ID	Name	NetBackup Self Service	Backup selection
13	MS-Windows	Protection; file restore	Defined in policy template, applies to all clients.
14	OS/2	Not supported	
15	MS-SQL-Server	Protection (client based only); database restore	
16	MS-Exchange-Server	Protection	Defined in policy template and applies to all clients in the policy.
17	SAP	Protection	Defined by a script that resides on the client.
18	DB2	Protection	Defined by a script that resides on the client.
19	NDMP	Protection	Defined in policy template and applies to all clients in the policy.
20	FlashBackup	Protection	Defined in policy template and applies to all clients in the policy.
21	Split-Mirror	Not supported	
22	AFS	Not supported	
24	DataStore	Not supported	
25	Lotus-Notes	Not supported	
27	OpenVMS	Not supported	
29	FlashBackup-Windows	Not supported	
31	BE-MS-SQL-Server	Not supported	
32	BE-MS-Exchange-Server	Not supported	
34	Disk Staging	Not supported	
35	NBU-Catalog	Not supported	
37	CMS_DB	Not supported	
38	PureDisk Export	Not supported	

Table A-1 Policy types and associated IDs *(continued)*

ID	Name	NetBackup Self Service	Backup selection
39	Enterprise Vault	Not supported	
40	VMware	Protection (intelligent policies or client based); restore VM; restore file	
41	Hyper-V	Protection (intelligent policies or client based); restore VM; restore file	
42	NBU-Search	Not supported	
47	Nutanix AHV	Protection; Restore Nutanix VM	Restore Nutanix VM.
50	Kubernetes	Protection; Restore Namespace; and Persistent volume	Restore Namespace and Persistent volume.

At this time, computers cannot be protected with snapshot-enabled policies. This issue is a known issue.

Appendix B

Dashboard traffic light status and usage

This appendix includes the following topics:

- About dashboard traffic light status and usage
- Assets with a protection type
- Assets without a Protection Type
- Usage and Charging
- Tenant Quota Enforcement

About dashboard traffic light status and usage

The dashboard status section shows the number of computers in a given protection state: red, amber, or green. This color calculation is dependent on a computer having a protection type.

Consumed capacity is visible as a total and by month.

If you are a tenant-user you see totals for your tenant. If you are a service provider, you see totals reflecting the full estate.

Assets with a protection type

When a user selects a managed protection level from those available to a protection type, this action adds the computer to one or more NetBackup policies. Self Service holds a threshold (in hours) for each policy it is aware of. Evaluating the thresholds of all the known policies that an asset is in determines its red, amber, or green status. Assets with a protection type that includes an unmanaged protection level

are evaluated with a red or a green traffic light. The traffic light color is dependent on the existence of a backup matching the unmanaged protection level's policy name.

Table B-1 Computers with Protection Types

Color	Computer state
Green	Protection level applied, and all policies have backups within their threshold; or the policy has been set to **Always show as protected**.
Amber	No protection level has been applied to the computer.
Red	Protection level applied, but one or more policies have no backups, or the most recent backup is outside of its threshold.

Note: If an asset is in a NetBackup policy but no protection level is found, the policy is not considered when the color status is determined.

Assets that are protected with only a **Backup Now** process are not included in the count and are not shown as protected.

Assets without a Protection Type

When an asset does not have a protection type, the status always displays as amber.

Usage and Charging

The **Usage** section is split into two parts: the amount of consumed capacity as a total and as a graph by month.

Consumed capacity is calculated from all non-expired images belonging to the tenant. It can be expressed either as an absolute figure, in gigabytes, or in relation to the amount of contracted space for the tenant. When consumed capacity is shown in relation to contracted space, the value is shown both as a percentage and as an absolute amount against that total. The calculation for consumed capacity depends on the **Use Data Transferred Values** integration setting.

Configuring charging

You can configure charging data per tenant, per protection level or both.

When **Usage** calculates the price for a backup, the rules that are shown are applied:

1. If the Tenant has charge rates and there is one for this backup's Protection Level then that charge rate is used, otherwise:
2. If the Tenant has a default charge rate, then this default rate is used, otherwise:
3. If there is a system-wide Protection Level charge rate for the backup then that is used, otherwise:
4. The default system charge rate is used.

By default, NetBackup Self Service has a single system-wide charge rate that is configured to 0 USD.

If a Tenant requires Protection Level charge rates then you must provide a Tenant-wide cost.

To add or edit charges, you must log on as a service provider or administrator account and click on the **Charge Rates** link on the home page. Click on Add or Edit and you can set a System/Tenant wide charge rate or override individual Protection Levels with the appropriate charge.

Note: A computer has an associated usage record if it has a backup in NetBackup Self Service.

Note: Only NetBackup Self Service aware NetBackup policy backups count towards usage.

Note: When you view the Tenant Usage data, the reported **CostPerGb** figure is the tenant's value. If you configure the system to use Protection Level overrides, this **CostPerGb** is not correct. The actual costs, however, are calculated using Protection Level costs. You should use the Tenant Protection Level data for a breakdown of that Tenant's usage.

Tenant Quota Enforcement

The **Tenant Quota Enforcement** feature ensures that tenants comply and work within their respective contracted space usage amounts. This functionality lets providers enforce limits on a per tenant basis. You can enable or disable this feature per tenant, which lets you control who is monitored. This option is disabled for all tenants by default. You must enable this functionality for each tenant you want to monitor.

Once you enable the feature, Self Service tracks the total size of backups from the tenant account. The current **System Sync** task works with the new **Lock Calculation Task** scheduled task to track usage. The **Lock Calculation Task** updates the backup sizes from the primary server before it applies or removes locks on the tenant account.

To enable or disable quota enforcement

1. Go to the **Netbackup Adapter** settings section for the tenant you want to enable quota enforcement.
2. Locate the **Quota Enforcement** settings section.
3. Use this option to enable or disable quota enforcement as required.

System administrators have a new view that lets them see who is currently locked out. From this view, they can unlock users after they have increased the contracted space amount.

Note: Once a tenant is locked out for exceeding their contracted space, they cannot take backups or protect new assets until they are compliant again. Until the lock is reset, when the user attempts a backup or an asset protection, they receive a detailed message.

To unlock a tenant:

1. Select the **Tenant lockout** screen from the left side menu.
2. Deselect the **Locked Out** option.
3. Once the account is unlocked, the user can resume normal backup and asset protection activities.

Note: After a tenant is locked out for exceeding the contracted space, a user cannot take backups or protect any new assets until they are compliant again. If a user attempts a back up or an asset protection operation during the lockout, they receive a detailed message. In addition to blocking manual operations, NetBackup Self Service automatically disables all backup policies for that tenant on the respective NetBackup master server. It ensures that scheduled backups do not run while the tenant remains over the contracted limit. When the lockout is reset, NetBackup Self Service automatically enables all previously disabled policies on the corresponding master server again. Backup schedules are restored and the tenant can resume protection operations.

The correct way to unlock a user is from the Tenant lockout screen. Make the tenant account compliant as shown:

- Increase their contracted space amount and unlocking them from that page.
- Have the user delete backups so that they are under their contracted amount of space usage.
- Then run the tenant lockout calculation job which unlocks the user.

Appendix C

Synchronizing data from NetBackup

This appendix includes the following topics:

- About synchronizing data from NetBackup

About synchronizing data from NetBackup

Two different processes are responsible for synchronizing data from NetBackup to Self Service. The processes are illustrated.

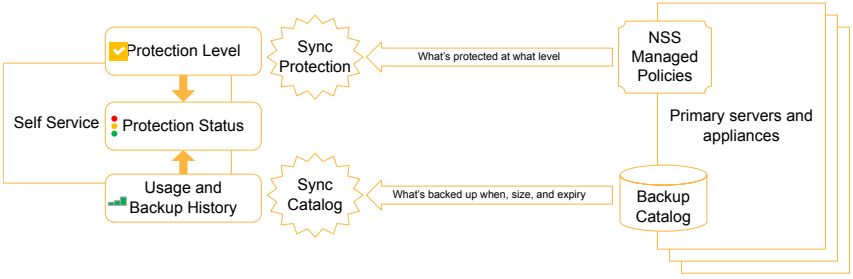


Table C-1 Synchronization process and associated details

Synchronization process	Details
Synchronization protection	■ Only synchronized when protection levels are configured. For example, Self Service managing policies. ■ Searches the policies on NetBackup for client computers. ■ Displays the protection level against computer or container (colored tick icons). ■ Self Service keeps local cache up to date itself with add and remove protection requests. ■ Can be manually initiated in the **Administration** panel.
Synchronization catalog	■ Synchronizes the backup catalogs and transfers details of all active images to Self Service. ■ Initial post-installation full synchronization that is carried out in configurable batch sizes. ■ Regular task keeps records up to date at Self Service with daily incremental synchronization. ■ Image records are matched against computers in the Self Service inventory. ■ Self Service rolls up image size data per computer and tenant on a nightly basis for summary dashboards. ■ Images for an individual computer are resynchronized on a Backup Now request completion or when an administrator manually initiates in the administration panel.

Appendix D

NetBackup Self Service data caching process

This appendix includes the following topics:

- About NetBackup Self Service data caching process
- NetBackup Data Synchronization
- Backup Now
- Protect
- Unprotect

About NetBackup Self Service data caching process

The NetBackup Adapter caches data about assets, protection, and backup images for improved performance.

Scheduled Tasks run periodically to keep the data up to date. Scheduled tasks include:

- **System Sync**
  - Imports the backup images from all backup servers since the last time it ran.
  - Expires the old backup images.
  - Calculates the usage.
  - Calculates the traffic light statuses.
  - Runs daily at 12:15 A.M. (UTC) by default.

- **System Update**
  This task processes the computers that are flagged for NetBackup data synchronization. Imports the protection levels and backup images, then recalculates traffic light statuses. Runs every minute by default.
- **Asset Import**
  Synchronizes the computers from vCloud Director and cloud assets from NetBackup according to configured imports. This task runs once per day at 12:30 A.M. (UTC) by default, but can be initiated manually.
- **Lock Calculation Task**
  This task is the scheduled task for Quota enforcement. It refreshes the backup images and calculates the latest usage at that point in time. Based on the totals, the locks are either applied or removed.
  You can run this task manually on demand.

System Sync

- Imports the images from the last day for all online backup servers. The import includes a 24 hour overlap to get the backups that started but not completed when the last System Sync took place.
- Flags the expired images.
- Updates the last backup time and calculates traffic light status.

Note: Adding a new backup server does not trigger any independent action in the system. Any new synchronizations or ongoing synchronizations, such as getting backup images or importing policies, now include this new backup server. Older images are not imported without manual intervention. Click **Refresh NetBackup Data** or call the API to import older images. These actions are required for every computer that may have backups.

Integration settings

The Integration Settings that are listed are relevant to the System Sync:

- Utilization Retention Period (Months) (NetBackup Adapter integration section)
  The period of time which usage data and expired backup images are retained for and the number of months displayed in the charts. After this period the usage data and expired images are deleted in the System Sync.

If quota enforcement is enabled, the contracted space amount must be set in the Integration Settings.

NetBackup Data Synchronization

When an asset is imported, **Refresh NetBackup Data** is clicked, or `SyncNetBackupData` is called in the API, the asset is flagged for synchronization. This marks the asset as ready for synchronization and it is picked up by the System Update. This process imports the protection and images, then recalculates traffic light status.

The task processes batches of 100 assets for 5 minutes (by default) or until there are no assets requiring import. Assets added longest ago are processed first. All assets have the same priority initially but if a **Backup Now** is performed, that asset is marked as high priority.

If a synchronization fails, the synchronization is locked for a period of time. This lock allows other assets without errors to be processed.

Integration Settings

The integration settings that are listed are relevant to the NetBackup Data Synchronization:

- Image Import Batch Processing (minutes) (NetBackup Adapter integration section)
  The System Update gets data for a period of time while there are computers marked for synchronization. This defaults to five minutes.
- Image Import Lock Delay (minutes) (NetBackup Adapter integration section)
  This value defines how long to lock a computer image synchronization for a computer if its image retrieval fails. This defaults to 60 minutes.

Backup Now

When a **Backup Now** request completes, the computer is flagged for synchronization with high priority so that the computer synchronizes the new image as soon as possible.

Protect

When a **Protect** request completes, a task is queued to add the protection level to the database and update the traffic light status.

Unprotect

When an **Unprotect** request completes, a task is queued to remove the protection level from the database and update the traffic light status.

Appendix E

Integration settings

This appendix includes the following topics:

- About integration settings
- NetBackup Adapter
- NetBackup Adapter Usage
- NetBackup Adapter Access Rights

About integration settings

Integration Settings are a flexible store of named settings with values. They are used to configure the integration between NetBackup Self Service and NetBackup. Individual Settings are grouped within sections and are accessed through **Left menu > Settings > System Configuration > Integration Settings**. This section includes the full list of Integration Settings relevant to the NetBackup Self Service solution. Individual sections or settings are referred to throughout the document, in the appropriate functional area.

Some settings have **Allow Tenant Override** set to **yes**. These settings typically need to be configured on a per tenant basis and should not normally be completed in the top-level Integration Settings. Instead they are configured under the details for the specific tenant. The NetBackup Adapter Access Rights settings also have the option of user override. More information about access rights is available.

See “Access rights” on page 32.

If an override setting is manually changed from the values automatically created for the system-wide Integration Setting, that new value is ignored.

Most Tenant level integration settings are created from the home page but are edited through **Left menu > Tenants**, on a separate tab within each tenant record.

Accessing from within the tenant, only the settings that can be edited at the tenant level are available.

The Integration Settings sections that are pre-shipped are:

Table E-1 Preset integration settings

Setting	Details
NetBackup Adapter	This section holds the settings which affect the whole of the solution. There should be only one of these sections.
NetBackup Adapter Usage	This section controls the data and calculations in the **Usage** panel on the home page. There should be only one of these sections.
NetBackup Adapter Access Rights	This section determines what backup and restore actions are permitted in the solution. There should be only one of these sections.

NetBackup Adapter

This section holds the settings which affect the whole of the solution. There should be only one of these sections.

Table E-2 NetBackup Adapter settings

Setting	Tenant Override	Details
Report Customer Root	Yes	The path of a folder on the web server where this tenant's reports are stored.
Report File Extensions	No	A semicolon-separated list of file extensions can be specified.
Contracted Space (TB)	Yes	The total amount of space, in terabytes, agreed for use. Optional value; if set, typically configured at tenant level
Quota enforcement	Yes	This setting toggles the tracking of space usage at tenant level. It helps to enforce the contracted space that every tenant is given with values set in **Contracted Space (TB)**. By default this setting is disabled. To enable quota enforcement, this option must be enabled for each tenant.

Table E-2 NetBackup Adapter settings *(continued)*

Setting	Tenant Override	Details
Usage Retention Period (months)	No	The number of months the historical rolled up data is retained for display in the home page Usage graph and table.
Image Import Batch Processing (minutes)	No	The computer image load retrieves images for a period of time while there are computers marked for synchronization. This defaults to 5 minutes.
Image Import Lock Delay (minutes)	No	This setting determines how long to lock a computer synchronization for a computer if an error occurs during image retrieval. The default is 60 minutes.
Send Usage Email	No	An email detailing system usage is sent on the 1st of each month. If you do not want this email to be sent, set the setting to **No**.
Show Traffic Lights Tiles	Yes	This setting determines whether traffic lights are displayed on the home page.
Show Consumption Total Tile	Yes	This setting determines whether the total usage is displayed on the home page.
Show Consumption Trend Tile	Yes	This setting determines whether the usage trend graphs are displayed on the home page.

Table E-2 NetBackup Adapter settings *(continued)*

Setting	Tenant Override	Details
ESX Host Selection Algorithm	Yes	This setting has three options: Random Match, Best Match, and First Match. The default is Random Match. This option is used when NetBackup Self Service tries to restore a VCD VM from one vApp to another if the source vApp and the destination one are on different Organization vDCs. Allowed values for this setting are: Random Match: ■ Randomly choose an ESX host A from all available ones. ■ For host A, randomly choose a resource pool. ■ For host A, choose the datastore with the maximum free space. First Match: ■ Choose the first available ESX host A. ■ For host A, randomly choose a resource pool. ■ For host A, choose the datastore with the maximum free space. Best Match: ■ Choose the ESX host A which is attached to the datastore with the maximum free space. ■ For host A, randomly choose a resource pool. ■ For host A, choose the datastore with the maximum free space.
Automatic ESX Host Selection On vAppRestore	No	This setting enables automatic selection of an ESX host during the vApp restore process. If enabled, the system automatically selects the appropriate host to restore the vApp without requiring manual input. The default setting is **Enabled**.
Allow Cross Site Selection For vAppRestore	No	This setting allows the user to select an ESX host from another site (another master server) during the vApp restore operation. The default setting is **Disabled**.

Table E-2 NetBackup Adapter settings *(continued)*

Setting	Tenant Override	Details
Enable Restored Virtual Disks	No	This setting when enabled on the vApp restore screen, allows you to restore the associated virtual disks along with the vApp. The default setting is **Disabled**.
Enable Transport Mode for vApp Restore	No	This setting controls whether transport mode is enabled during vApp restore. When enabled, the option appears on the restore screen, allowing you to choose from transport modes, such as SAN, NBD, or NBDSSL for the restore process. The default setting is **Disabled**.
Enable Storage Policies for vApp Restore	No	This setting displays a storage policy drop down on the vApp restore screen. The system uses the selected storage policy from VCD to automatically choose the datastore during the restore process. The default setting is **Enabled**.

NetBackup Adapter Usage

This section controls the data and calculations in the **Usage** panel on the home page. There should be only one of these sections.

Table E-3 Adapter Usage settings

Setting Name	Tenant Override	Details
Charging Type	Yes	The base parameter for whether the charge represents new backups or used space, or whether no calculation is made. Options: New Backups, Consumed Capacity, or None.
Use Data Transferred Values	No	Controls whether to use **Transferred Size** or **Image Size** in usage statistics. **Transferred Size** values can be lower such as when you use Accelerators. The **Transferred Size** value is only available on NetBackup 7.7.1 and later.

NetBackup Adapter Access Rights

- **Backup Now**
- **Protect Machine**
- **Restore File**
- **Restore VM**
- **Unprotect Machine**
- **Register for File Restore**
- **Restore SQL**
- **Restore Oracle**
- **Restore Cloud Asset**
- **Agentless Restore File**
- **Agentless Restore File to alternate VM**
- **Expire Backups**
- **Restore Disks**
- **Restore Kubernetes Namespace**

This section also allows control of the home page **Usage graph** and **Usage list**.

There should be only one of these sections.

Table E-4 NetBackup Adapter Access Rights

Setting Name	Tenant Override	Details
Allow Backup Now	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Protect Machine	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Restore File	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Restore VM	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.

Table E-4 NetBackup Adapter Access Rights *(continued)*

Setting Name	Tenant Override	Details
Allow Unprotect Machine	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Usage Report	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Register for File Restore	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Restore SQL	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Restore Oracle	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Restore Cloud Asset	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Agentless Restore File	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Agentless Restore File to Alternate VM	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Expire Backups	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Restore Disks	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.
Allow Restore Kubernetes Namespace	Yes	To override this value at the user level, select **for user** from the drop-down list. See the note that follows this table.

Table E-4 NetBackup Adapter Access Rights *(continued)*

Setting Name	Tenant Override	Details
Allow Restore Nutanix VM	Yes	To override this value at the user level, select for user from the drop-down list. See the note that follows this table.
Allow Tenant Expire Backup	No	The setting when enabled allows tenants to expire backups in the system. If enabled, a corresponding option is displayed to tenants, allowing them to manually expire older backups as required. The default setting is **Disabled**.
Allow Tenant Register Computer	No	The setting when enabled, allows tenants to register computers in the system. The tenants see the option to add and register their own computers within the environment. The default setting is **Disabled**.
Enable Restore Approval Workflow	No	The setting when enabled, activates the restore approval workflow. All tenant restore requests require administrator approval before the restore job is triggered. The administrator has the option to approve or deny the request. If the request is denied, the tenant is notified, and the request status is marked as **Denied** in the status list. The default setting is **Disabled**.

Note: The recommendation is that you only set a system wide or tenant level flag. An override at tenant user level should only be considered if the system-wide setting is set to **enabled**.

More information about the configuration of tenants is available.

See “Configuring tenants” on page 31.

Appendix F

REST API

This appendix includes the following topics:

- About the REST API

About the REST API

A REST API supports both administrative actions and operational actions against the system, such as adding, protecting, and restoring computers.

You can find the REST API's URL in the portal's **About NetBackup Self Service** page. Documentation for the REST API is found by adding `/help` to the end of the REST API's URL.

Version 6 of the API is enabled and requires logon with a user's credentials.

Appendix G

Central configuration and the nsscmd command

This appendix includes the following topics:

- Central configuration and the nsscmd command

Central configuration and the nsscmd command

Central configuration overview

NetBackup Self Service stores shared settings and secrets in the central configuration folder, `{ProgramFolder}\Config\`.

Table G-1 Central configuration files

File	Purpose
`connectionStrings.json`	Main and Adapter SQL connection strings; DapiConnectionString
`machine.secrets.enc`	DPAPI-protected secrets, including ApplicationKey and JWT key material
`machine.secrets.json`	Development or plaintext only; not used in production installs

Services load configuration from this folder at runtime. After Phase 2 migration, do not edit connection strings in individual service `appsettings.json` files.

After installation or upgrade, connection strings are no longer stored in the per-service `appsettings.json` files under Website, API, DirectaService, or WebService.

nsscmd configuration commands

Run these commands from `{ProgramFolder}\Install Files\`.

Table G-2 nsscmd configuration commands

Command	Use
`nsscmd -getconfig`	Export configuration for backup, load balancing, or disaster recovery.
`nsscmd -readconfig -configDir "{ProgramFolder}\Config"`	Read secrets, including the ApplicationKey, on this machine.
`nsscmd -setconfig "<string from getconfig>"`	Apply configuration from another node for load balancing.
`nsscmd -initconfig -programFolder ...`	Create central Config from `Install.ini` during a fresh install.
`nsscmd -migrateconfig -programFolder ...`	Migrate the legacy layout during upgrade and preserve the ApplicationKey.
`nsscmd -validateconfig -configDir "{ProgramFolder}\Config"`	Validate secrets and connection strings.
`nsscmd -showsecrets -configDir ... -name ApplicationKey`	Verify that the key is present. Output is masked.

ApplicationKey requirements

- Fresh install with a new database: The installer generates the ApplicationKey automatically.
- Existing database: The ApplicationKey must match the database when UseExistingDatabase=1.
- Upgrade: The ApplicationKey is preserved. You cannot change it with `nsscmd -setsecret` after initial configuration.
- Disaster recovery: `UnInstall.bat` preserves `Config\`. Back up the configuration with `nsscmd -getconfig` after every production install and upgrade.
- Load-balanced servers: Do not copy `machine.secrets.enc` between servers because DPAPI is machine-specific. Use the same ApplicationKey hex value and run -initconfig or -setconfig on each node.

Manual Install.ini updates

Edit `{ProgramFolder}\Install Files\Install.ini` only for non-GUI or automation scenarios. For details, see *NetBackup™ Self Service Installation Guide*..

For the **Use existing database** option in the 11.2 Configurator, enter the ApplicationKey in the UI. Add or maintain an ApplicationKey= line only when you bypass the Configurator.

Idempotent initconfig behavior

If `machine.secrets.enc` already exists and the supplied -applicationKey matches, the installer keeps the existing secrets. When `-fromInstallIni` is used, `connectionStrings.json` is refreshed from `Install.ini`.

Appendix H

Glossary

This appendix includes the following topics:

- Glossary

Glossary

Table H-1 Glossary of terms

Term	Definition
ApplicationKey	Hexadecimal encryption key stored in `Config\machine.secrets.enc`. It is required to decrypt integration passwords and must be preserved for upgrades and disaster recovery.
Asset	Any computer or volume of which the solution is aware.
Backup Now	A user action in Self Service that creates a temporary Policy on the NetBackup primary server and schedules it for immediate backup. The template policy is deleted afterwards. If a computer is already protected and residing in a scheduled policy, you can use this option to initiate an immediate backup using that policy.
Backup servers	A backup server represents a connection to a NetBackup primary server. Backup server is the new UI terminology but Location is still used in the Rest API.
Central configuration	The `{ProgramFolder}\Config\` folder that stores `connectionStrings.json` and `machine.secrets.enc` for all NSS services.
Cloud Import	A computer source which allows automated import of CloudPoint assets.

Table H-1 Glossary of terms *(continued)*

Term	Definition
Computer	Any physical or any virtual computer that the solution is aware of.
Customer Code	A unique code that is used to identify the tenant in NetBackup Self Service. This code is used in policy naming in NetBackup.
Image Sync	Process where Self Service collects information about computer backups from NetBackup.
Integration Settings	Integration Settings are a flexible store of named settings with values held in the Self Service Portal. All integrations settings can be accessed as an Admin user from **Admin > Settings > Integration Settings**. If they are configured with Tenant level exceptions, you can access them from **Admin > Organization > Tenant > Integration**.
Location	A location represents a connection to a NetBackup primary server. This connection is more commonly known as a backup server.
Machine	Any physical or any virtual machine that the solution is aware of.
NetBackup Self Service	Term that is used to describe the whole solution, also known as Self Service.
NetBackup Self Service Adapter	Second part of a Self Service system; responsible for communications with NetBackup.
NetBackup Self Service Portal	First part of a Self Service system, the solution's main website.
Panels	A sub area in the home page of the Self Service portal. Sometimes called home page widgets.
Protect (computer)	A user action in Self Service that results in a computer being scheduled for regular backups through its addition to a NetBackup Policy.
Protection Level	A protection level represents a level of protection which can be applied to a computer. Configuring protection levels means that the users can maintain their own scheduled backups against NetBackup Policies. This maps to template policies on each NetBackup primary server.

Table H-1 Glossary of terms *(continued)*

Term	Definition
Protection type	A protection type defines all the ways you can protect a computer. This protection may be by a single protection level or by multiple protection levels, for example to cover a mix of physical and virtual computers. Scheduled protection and one-off backup require different protection levels.
Refresh NetBackup Data	Computer level manual or automated process to rebuild image data, protection data, and traffic lights.
Register Machine	The process that is used to update the Self Service system with information about a tenant's computer.
Restore File/Folder	A user action in Self Service that creates a job to restore a file or folder in NetBackup.
Restore Namespace	A user action in Self Service that creates a job to restore a kubernetes namespace in NetBackup.
Restore Nutanix VM	A user action in Self Service that creates a job to restore a Nutanix VM in NetBackup.
Restore VM	A user action in Self Service that creates a job to restore a virtual machine in NetBackup.
Self Service	Term that is used to describe the whole solution, also known as NetBackup Self Service.
Service Catalog	The home page that is presented to users of the Self Service portal. Can be edited from **Admin > Service Catalog & Notices > Service Catalog**.
Service Provider	Refers to the top-level organization administering the Self Service system.
SYS_APP_KEY_CHECK	Database value in SYSTEM_SETUP that verifies whether the ApplicationKey matches the database during an existing-database installation.
Template Policies	Inactive NetBackup Policies on a primary server the system uses to create active policies for users.
Tenant	An organizational group of users. May be used as a business unit within an enterprise scenario, or a customer for a service provider. All users must be in a tenant.

Table H-1 Glossary of terms *(continued)*

Term	Definition
Unmanaged (computer)	An additional class of protection. It lets you restore computers and monitor their health. It assumes protection (policy management) is handled outside of NetBackup Self Service.
Unprotect (computer)	A user action in Self Service that results in a computer being removed from a NetBackup Policy.
vCenter Import	A computer source which allows automated import of VMware assets.
vCloud Director Import	A computer source which allows automated import from vCloud Director.
Web Services	An API for the portal, can be used to automate adding Tenants, users, etc. Sometimes referred to as DAPI.