NetBackup Self Service Configuration Guide

7.7

Document version: 1

Documentation version: 7.7

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Licensing

This chapter includes the following topics:

Applying the full License

NetBackup Self Service 7.7 is shipped with a fully featured 60-day trial license. A production license is available from your Customer Care team.

Access the NetBackup Self Service portal to apply the license. Select **Admin > Settings > License > Update License Key**. Copy and paste the new license key. Restart the Windows service after you apply the license key. If the application runs in a server farm environment, all application pools must be restarted.

In the **License** page, a message at the top of the page reports that other features are not included. All features that are required to operate a fully configured NetBackup Self Service solution are, however, included.

Note: Internet Explorer 8 is a limited browser for high-quality display. The use of the **standards mode**, however, provides a reasonable display. Use of the **compatibility mode** is not supported.

Additional information about prerequisites and requirements is available. Please refer to the *NetBackup Self Service Installation Guide* for additional details.

Chapter 2

Configuring a Self Service solution

This chapter includes the following topics:

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 computers and their owners.

You can populate the computer inventory multiple ways:

- A source independent API
- The Self Service portal

- An import from vCloud
  Although only the vCloud hosted computer is listed, the computer name also includes the vDC or vApp, which lets you search for the computer name.

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 computers and their policy 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 Levels 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 2-1 shows the recommended sequence of steps for configuring Self Service for the first time.

Table 2-1 Configuration checklist

Where	Activity
Server	Install NetBackup Self Service Portal (see *NetBackup Self Service 7.7 Installation Guide*)
	Install NetBackup Self Service Adapter (see *NetBackup Self Service 7.7 Installation Guide*)
	Configure remote PowerShell for a Windows Master Server
	Configure SSH for a UNIX Master Server
Portal	Create at least one Location
	Create at least one Protection Level (if needed)
NetBackup Master Server	Create Template Policies

Table 2-1 Configuration checklist *(continued)*

Where	Activity
Portal	Create a Tenant
	Register at least one computer through the user interface, the API, or through vCloud import
	Raise a Backup Now request

Chapter 3

Configuring a NetBackup master server

This chapter includes the following topics:

About configuring the NetBackup master server

A minimum of NetBackup 7.6.1 with the latest service pack is required.

Each NetBackup master server the system needs to communicate with must be configured as a **Location**. To manage locations, log on to the Self Service portal as an Admin user, and then go to the **Locations** tab on the home page.

Note: If you use a vCloud Integrated configuration, NetBackup must be configured for vCloud before you enable NetBackup Self Service. The VMware vCloud director must support a minimum of API version 5.1.

Enabling communication with a Windows NetBackup master server

NetBackup Self Service uses Windows PowerShell Remoting to communicate with a Windows NetBackup master server. Windows PowerShell must be installed on the master 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 master server

1. Log on to the NetBackup master 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 master 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 Location is available.

See “Configuring Locations” on page 23.

Enabling communication with a UNIX NetBackup master server

NetBackup Self Service uses Secure Shell (SSH) to communicate with a UNIX NetBackup Master 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 master server.

- By default SSH uses Port 22.

- The user account that NetBackup Self Service uses to logon to SSH on the master 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 master 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 as long as the password prompt starts with **password**. You configure this behavior by telling NetBackup Self Service to connect to a NetBackup Appliance.

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

1. Create a Public Private key pair using a key generator like `PuTTYgen`.
2. Log on to the master server as the required master server user
3. Add the public key to the user's `authorized_keys` file in the master server's operating system format.
4. Convert the Private key into OpenSSH format encrypted with a pass phrase

```
-----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 Location in NetBackup Self Service:
   - Choose **Encrypted SSH Key** for the Credentials.

- Enter the user account to connect to the master server in **User Account**.
- Paste the encrypted OpenSSH format private key in **NetBackup OpenSSH Key**.
- Enter the pass phrase in **Password** and **Confirm Password**.

More information about testing the connection once you have created your first **Location** is available.

See "Configuring Locations" on page 23.

Enabling communication with a NetBackup appliance

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

Log on to CLISH 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.

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.

Not all NetBackup policy options are required or used by Self Service template policies. Table 3-1 details the relevant tab in the NetBackup policy creation screen and the corresponding information 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 3-1 Requirement policy information for Backup Now policies

NetBackup policy tab	Additional details
Attributes	■ The policy must be deactivated. ■ There is only a single Backup Now policy per policy type. When you specify the storage option, be sure to specify one that is large enough to successfully back up all the data.

Table 3-1 Requirement policy information for Backup Now policies *(continued)*

NetBackup policy tab	Additional details
Schedules	■ The retention value set in the NetBackup policy is not used by Self Service. ■ Do not set the backup window.
Clients	■ The client information is added by NetBackup Self Service so this can be left blank.
Backup Selections	■ The backup selection depends on the operating system of the clients. Windows: `ALL_LOCAL_DRIVES` UNIX/Linux: The root directory (`/`) ■ Because no clients are specified, you must type this information into the policy manually. You cannot select the directive from a drop down.

Template Policies are inactive policies on the master 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 actions that require a policy to be created on the master 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 named correctly for the system to find them. The format of template policy's name is:

Scheduled Backup Template Policies: *Template-PolicyType-ProtectionLevel*

BackupNow Template Policies: *Template-PolicyType-BackupNow*

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

PolicyType

The policy type code for NetBackup. For example, 0 for standard, 13 for Windows, 40 for VMware. The vCloud policies are defined with a special policy type of **vCloud**, although the underlying policy type is VMware (40) policy

More information on NetBackup policy types is available.

See "List of NetBackup policy types" on page 51.

For any type 40 (VMware) template policy:

- On the **VMware** tab, the Primary virtual machine identifier must be **VM display name**.
- On the **Clients** tab for BackupNow policies, Virtual Machine Selection must be set to **Select automatically through VMWare Intelligent Policy query**.

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.

ProtectionLevel

Protection Level is used to select between templates with different Schedules or Retentions configured. The value in the template policy name must match the **Template Suffix** set when you create a Protection Level. This setting allows each configured Protection Level to have its own set of template policies.

Scheduled Backup Template Policies

Scheduled Backup Template policies should be configured with all the options required for a given protection level for each of the required policy types. If using two policy types, standard (0) and Windows (13), configuring a Protection Level with a template suffix of PL1 requires creating 2 template policies, Template-0-PL1, and Template-13-PL1. Each of these templates would need to be set up as needed for the Protection Level.

BackupNow Template Policies

BackupNow template policies should be created for each Policy Type being supported. The template policies should have no backup window on their schedule, which should be called **Default**.

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. More information about Backup Now retention levels is available.

See “Configuring Backup Now retention levels” on page 26.

Template policy naming example

If you support standard (0) and Windows (13) policies, with two different Protection Levels (PL1 and PL2), six template policies must be created:

```
Template-0-PL1
Template-0-PL2
Template-0-BackupNow
Template-13-PL1
Template-13-PL2
Template-13-BackupNow
```

vCloud Template Policies

vCloud template policies are created according to VMware template policies but with different names.

vCloud Template Policies should be named:

vCloud Scheduled Backup Policies: *Template-vCloud-ProtectionLevel*

vCloud BackupNow Policies: *Template-vCloud*-BackupNow

Checking Template Policy Creation

Check the creation of Template Policies within Self Service to see that their naming is correct. You can also confirm that they were created on all master servers.

The **Protection Levels** tab on the Administrator's home page shows which master servers have correctly named policies. If a policy is not present, the home page shows the name of the missing policy. More information about protection level configuration is available.

See "Configuring Protection Levels" on page 25.

Polices created by Self Service

When a computer is protected or a backup now request is raised, Self Service creates policies on the appropriate NetBackup master server. For scheduled backups, the format is *CustomerCode-PolicyType-ProtectionLevelSuffix*.

Example:

```
CUST1-0-PL1
CUST1-13-PL1
CUST1-vCloud-PL3
```

For backup now policies, the format is
CustomerCode-RequestId-PolicyType-RetentionLevel-bn

Example:

```
CUST1-23451-0-3-bn
CUST1-23452-13-1-bn
CUST1-23453-vCloud-1-bn
```

Chapter 4

Configuring Self Service

This chapter includes the following topics:

About Self Service configuration

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

- Locations
- Protection Levels
- Tenants
- Machines

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

About integration settings and editing of Locations, Protection Levels, and vCloud imports

Integrations Settings are a flexible store of named settings with values. They are an integral part of Self Service. You can access all integrations settings as an Administrator from **Admin > Settings > Integration Settings**.

Settings are grouped into sections. Locations, Protection Levels, and vCloud imports exist in Self Service as Integration Settings that are grouped into a section. A single section defines each individual Location, Protection Level, and vCloud import. When you use the Add function for each of these, they create Integration Settings behind the scenes.

You can edit or delete these only through **Integration Settings**. Some advanced configuration options are only available there directly. Care must be taken, however, as no validation is performed when editing values directly through **Integration Settings**.

Configuring Locations

A location represents a connection to a NetBackup Master Server. The system requires at least one location to function.

New locations are created with **Add Location** on the home page **Locations** tab. The on-screen prompts should be completed. A **Location** Integration Setting section is created.

Once the location has been created the system returns to the main **Locations** tab where a Connectivity Check is started. The animated green cog on the Check Connectivity icon indicates that the Connectivity Check is started.

Once the check has finished, the new Location is displayed with a green tick (passed) or a red cross (failed).

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

Integration Settings that are used in a location

None of these settings can be overridden at the tenant or the user level.

Additionally, the name of the section forming the Location must be in the format **Machine Location *abc***, where *abc* is the name of the location. Once computers have been added to the location, do not change the name of the location. Changing the name of the location can result in computers being disassociated from the location.

Table 4-1 Location integration settings

Item	Details
NetBackup server	The NetBackup master server for this location.
Online	Indicates if the master server is considered online. The system does not use the locations that are not online in any way. Users are blocked from taking the actions that affect the location. Used for planned maintenance or in the event of an outage.
NetBackup UserName	The user name to connect to the NetBackup master server.
NetBackup Password	The password that is used for connection to the NetBackup server. If using encryption, an encrypted SSH key is used as the pass phrase.
NetBackup OS	The operating system of the NetBackup server.
NetBackup Folder	The Location on the NetBackup master server that the NetBackup commands are installed in. Default values are: `C:\Program Files\Veritas\NetBackup` for Windows `/usr/openv/netbackup` for UNIX
NetBackup TimeZone	If all NetBackup and NetBackup Self Service servers are in the same time zone then you do not need to configure this setting. If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.
NetBackup DateFormat	Specifies the format the Master Server expects dates to be supplied in. See **Add Location** in the portal for options.
NetBackup DateTimeFormat	Specifies the format the master server expects date and time to be supplied in. See **Add Location** in the portal for options.
NetBackup OpenSSH Key	For connection to UNIX master servers with SSH. The key must be in the OpenSSH format.
NetBackup Use Pooled Connections	Windows master servers only. Enabled by default and should be left on for normal usage. Controls pooling of PowerShell connections to the master server for improved performance.
NetBackup Minimum Pool Size	Windows master servers only. Used for support purposes only.
NetBackup Maximum Pool Size	Windows master servers only. Used for support purposes only.

Table 4-1 Location integration settings *(continued)*

Item	Details
Get Backups Chunk Size in Hours	When Self Service synchronizes computer backup images from NetBackup, they are retrieved in batches of this size. The system defaults to 25 but may need to be reduced for very busy systems with lots of backup activities. Reducing the number results in more calls to NetBackup to retrieve a given number of images. The total number of images that are retrieved remains the same.
Maximum backup duration (hours)	The maximum number of hours to allow a backup job to complete on NetBackup. Used by the synchronization engine to estimate a buffer period to synchronize backup images. Should only be changed if problems in backup image synchronization occur.

Configuring Protection Levels

A Protection Level indicates the standard of protection that is applied to a computer. It corresponds to template policies on all of the NetBackup master servers in the system. These template policies can then have different schedules, retention levels etc., allowing different Protection Levels to have different characteristics. This configuration provides users a level of abstraction away from more complex NetBackup concepts.

As an example the system can be configured with three Protection Levels: Bronze, Silver, and Gold. Increasing the retention level and frequency of backups as you work up the scale of Protection Levels.

Use the **Add Protection Level** option on the home page **Protection Levels** tab to create New Protection levels. Follow the on-screen prompts to create a corresponding Protection Level Integration Setting section.

After you add a Protection Level the system initiates a connectivity check. The cog on the Check Connectivity icon becomes green and animated. This change indicates that the check is active. This check reviews each defined location in the system for Template Policies that correspond to the Protection Levels. Any missing Template Policies are shown on screen with a red cross icon. Clicking this icon provides further details about the Template Policy that needs to be created. More information about template policy creation is available.

See “Creating NetBackup Template Policies” on page 17.

Once the missing Template Policies are created you can use Check Connectivity to confirm that they are correct.

Table 4-2 Integration Settings that are used in a Protection Level

Item	Details
Name	The display name for the Protection Level as displayed to users.
Sequence	A number that is used to order all Protection Levels in the user interface; 1 at the start of any list, higher numbers further down.
Description	A description of the backup schedule and retention, for example Weekly backup, retained for one month.
Visible	Controls whether the Protection Level is available to users. Can be set to True or False. Can be overridden at a tenant level.
TemplateSuffix	Used to select a template policy in NetBackup when you protect a computer with this protection level. For the template policies `Template-0-PL1` and `Template-13-PL1`, the Template Suffix is `PL1`.
Backup warning threshold (hours)	Once a computer has been protected, if no backups have occurred within the backup threshold, the computer is flagged for attention. The value should be related to the backup schedule of the template policy. Example: If the backup schedule is daily, a warning threshold of 48 hours is appropriate.
Color	On-screen color for this Protection Level. Can be any HTML color value, for example yellow would be `yellow` or `#FFFF00`.

Configuring Backup Now retention levels

A Backup Now request uses the default retention levels that come preinstalled with NetBackup Self Service. You can amend the retention levels that are offered to users by editing the request form.

To configure Backup Now retention levels

1. Go to **Admin > Request & Approval > Request Type > Backup Now (DBBACKNOW)**.
2. Click on the **Form** tab and then the Backup retention field.

3 At the base of the page, click on the **Configuration** tab.

4 Listed under the **Items** field is a list of retention levels that are available in the Backup Now request form.

You can delete existing levels using the trash can icon or add new levels. The Code must match the NetBackup retention number and the Description is what the user sees.

Configuring Tenants

A Tenant is an organizational unit and at least one tenant must exist. A Tenant can be created with the **Add Tenant** icon in the home page **Tenants** tab. The first (admin level) user of the tenant is created at the same time. If any vCloud Import sources are defined, the tenants 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 **Admin > Organization > Tenant**. All users associated to the tenant are visible in the **Users** tab. Tenant level Integration settings are available in the **Integration** tab. vCloud credentials, and also additional vCloud imports, can be set here. Tenant level theming can be carried out in the **Themes** tab.

You can also use an API to create Tenants. A PowerShell script is provided as a starting point for automating the creation of tenants and their users. It makes use of the Front Office SDK to call the Public Web Services.

Further information about the SDK is available in the help files. The help files are found in the install location of the NetBackup Self-Service portal. By default, the files are located in `C:\Program Files (x86)\Biomni\Front Office 8.3\Sdk\`. Microsoft developers should use the SDK. Non-Microsoft developers can call the web service directly. The URL is found in **Admin > Support > Configuration Check** in the Public Web Service section of the **Server** tab. The web service is `DirectaApi.svc`.

Deactivating a Tenant

To deactivate a tenant:

1. Go to **Admin > Organization > Tenant**.
2. Deactivate the tenant.

   Deactivate the tenant with the **Deactivate** link on the right of the specific tenant row from the entry page. Or deactivate the tenant from the **Details** tab by deselecting the **Active** check box in tenant record.

   This action prevents logon from Tenant users.
3. All computers, backup, protection, and usage data is deleted for the tenant during the nightly scheduled task.
4. Delete all policies for the tenant in NetBackup.

   You can identify the policies by their name if you used the naming convention that is detailed in the NetBackup Self Service Configuration Guide. More information about the naming convention is available.

   See "About configuring the NetBackup master server" on page 14.

Adding users

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

- Manually through the portal from the **Admin > Organization > Tennant > User** tab
- Active Directory (**Admin > Organization > User** right-click **Import Active Directory**). The Cost Center Code must be the same as that found in the Tenant record.
- Master Data import through CSV (**Admin > Organization > User** right-click **Import / Export Users**. **Users** tab in the **Import File Template**). The Cost Center Code must be the same as that found in the Tenant record.
- Using the API

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 Form Authentication, password rules can be defined using a number of criteria. These rules can be configured in **Admin > 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 three levels: globally, per tenant, or per user.

Control of these access rights is available through **Admin > Settings > Integration Settings** 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 Register for File Restore**, and **Allow Usage Report**.

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.

   Ensure **Allow User Override** is **(None)**.
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**
     Ensure **Allow User Override** is set to **None**.

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 Right for each tenant

1. Select the **Integration** tab in the **Tenant Admin** screen.
2. **Admin > Organization > Tenant > Integration**.
3. Click the required **Access Right** in the **NetBackup Adapter Access Rights** section.
4. Choose **Enabled** or **Disabled** in the **Value** field.

To allow different users to have different actions available to them

1. Click the required **Access Right** in the **NetBackup Adapter Access Rights** section.
2. Choose **Enabled** or **Disabled** in the **Value** field. This setting is the default for any existing or any new users.
3. Ensure **Allow Tenant Override** is not checked.
4. Set **Allow User Override** to **For User**.

When **For User** overriding is chosen the value can be changed in any of the following places:

- By an Administrator user in the **Integration** tab of User Administration (**Admin > Organization > User > Integration**)
- By an Administrator user in the **Integration** tab of Tenant User Administration (**Admin > Organization > Tenant > Users > Select User > Integration**)
- By a Tenant Administrator in the **Integration** tab of their tenant's User Maintenance screen (**Admin > User Management > Select User > Integration**).
  - Click the required **Access Right** in the **NetBackup Adapter Access Rights** section
  - Choose **Enabled** or **Disabled** in the Value field

Do not select the **By User override** option.

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 the API, or automatically through vCloud import. A single tenant can have more than one source of computer, for example, virtual machines imported from vCloud and physical computers imported through the API.

Registering a computer with the user interface

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

To remove a computer registration, go to the **Machines** tab on the home page and use the **Remove Registration** link. 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 computer row on the list, 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.

Registering a computer with the API

For automated or bulk import of computer details, an API is available. The SDK allows clients to be written in .NET and is the preferred usage of the API. A REST API can, however, be used outside Microsoft environments.

Please see the SDK documentation in Install directory.

Registering a computer from vCloud Director with an import

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

A vCloud import defines two things: the vCloud instance that computers are imported from and the NetBackup Self Service location that the computers are registered to. You can only register a vCloud computer to a single location and to a single tenant.

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

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

When you create a new tenant, the **Add Tenant** form supports specifying credentials for a single vCloud system as part of the tenant creation process. Further credentials can be supplied either using the API or through the **Integration Settings** tab in **Tenant** administration.

Table 4-3 Integration Settings that are used in a vCloud Import

Item	Details
vCloud Api	This value should be set to the URL of the vCloud API, in the format of `https://hostname/api/`.
Location	The name of the NetBackup location 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 user name that the tenant uses to connect to the vCloud 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 password. Must be set at the tenant level only.

Configuring the home page

The home page is presented as a dashboard. This configuration allows the user to view current status of their inventory (computers) and initiate actions with a minimum of mouse clicks.

The tenant-user view presents as three panels: two small summary panels at the top of the page, and a full width panel at the bottom. This view is either a **Machine Inventory** dashboard (default) or a **Usage** dashboard, displayed as two tabs. The main panel changes content if either of the top panels are clicked. These panels are referred to as the Status, Usage and (computer) Inventory panels.

These panels are installed fully configured but the setup can be viewed in the Service Catalog (**Admin > Service catalog and Notices > Service Catalog**). Each **Service Catalog** panel references the **Integration Setting Panels** URL in the **NetBackup Adapter** section for the URL of the **NetBackup Self Service Adapter (Admin > Settings > Integration Settings**). User group level access controls are here but typically the shipped data would not be changed.

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 **Admin > Settings > Integration Settings** or **Admin > Organization > Tenant > Integration**.

Table 4-4 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.
Default backup warning threshold (hours)	Warning period since last backup; used in traffic lights only when no protection levels are specified.

The Action Request Type controls the request type that is associated with the following computer actions:

Table 4-5 Action Request Types (advanced customization only)

Item	Details
Protect Machine	The Request Type Code of the customized request type. Defaults to `DBNEWBACK`.
Backup Now	The Request Type Code of the customized request type. Defaults to `DBBACKNOW`.
Unprotect machine	The Request Type Code of the customized request type. Defaults to `DBREMBACK`.
Restore VM	The Request Type Code of the customized request type. Defaults to `DBRESTVM`.
Restore File	The Request Type Code of the customized request type. Defaults to `DBRESTFILE`.
Register for File Restore	The Request Type Code of the customized request type. Defaults to `DBREGDNS`.

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

Table 4-6 NetBackup Adapter Access Rights

Item	Details
Allow Backup Now	Determines if the Backup Now option is displayed.
Allow Protect Machine	Determines if the Protect Machine 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 Unprotect Machine	Determines if the Unprotect Machine option is displayed.
Allow Usage Report	Controls the display of the Usage report on the home page.

More information about **Access Rights** is available in the **Configuring Tenants** section.

See "Configuring Tenants" on page 27.

NetBackup Adapter Usage controls features within the Usage tab.

Table 4-7 NetBackup Adapter Usage

Item	Details
Currency Code	Currency denotation for display (no calculation)
Cost (Per GB)	Cost per gigabyte, used to calculate Charge
Charging Type	Basis of charge calculation: New backup, Used Space or none; maintainable at tenant level
Columns	The columns that are displayed in the **Usage** tab; Used Space, New backups or both

Table 4-8 Protection Level *abc*

Item	Details
Backup warning threshold (hours)	The time period before a protected computer is flagged for attention. The time period is defined as the backup schedule frequency plus the tolerance.

Chapter 5

Customizing Self Service

This chapter includes the following topics:

Language settings

Although the portal supports multiple languages, NetBackup Self Service solution data is currently only available in US English. This setting encompasses language and regional settings, including date formats.

Creating or customizing a request form

You can customize a request type but normal operation does not require this customization. All shipped request types are implementation-ready.

Note: If changes to a shipped request form are essential, it should be copied first, then you can edit the copy as required.

NetBackup Self Service is shipped with fully preconfigured request forms (request types). These forms are launched when a backup or restore option is selected from the home page dashboard. If additional data or integration is required, you can override the default request form with an association to a customized form. This override takes effect at the system-wide level.

You should be aware that a customization may be overwritten on upgrade and any customizations must be reapplied.

The shipped request form should be selected from the list and then copied. Access the form through **Admin > Request and Approval > Request Type**. Additional request fields, approval stages, or workflow can then be added and the **Request Type Active** check box enabled. Ensure that the **Request Type Name** is amended to text suitable for viewing in the **Request List**.

Note: No shipped request fields or workflow steps should be removed. This facility is available as a means of adding fulfillment steps or an approval process.

You should edit the relevant **Action Request Type**setting from the **Integration Settings** section.

1. Access the setting through **Admin > Settings > Integration Settings**.
2. Edit it by replacing the existing value with the new **Request Type Code**.
3. You can then deactivate the shipped request form.

Note: The service catalog and a full list of shipped request types is available if a restore to default values is required. They can be found in the Configuration folder, under the Installation location.

Themes

The pre-shipped NetBackup Self Service theme can be adjusted. Change the theme in an Admin area screen by editing the colors that are used as well as many of the images and styles. Many elements are editable by an edit page. You can also do additional customized editing with an online CSS editor.

The shipped theme can be adjusted system wide with **Admin > Settings > Theme** or for an individual tenant with **Admin > Organization > Tenant > Theme**.

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. An API supports these notices.

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

Chapter 6

User authentication methods

This chapter includes the following topics:

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 **Admin > Settings > System Configuration**.

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 **Admin > 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 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 of whether the Domain Name is pre-pended to the user ID when you import it. Find the system configuration setting in **Admin > 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 attendant effect 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 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 `web.config` 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 web.config to enable Federated Single Sign-On

To change the `web.config` file to enable federated single sign-on:

1. Navigate to *`install_path`*`\WebSite`.
2. Open `web.config` with Notepad as Administrator.
3. Find the `<modules>` section and uncomment the two `IdentityModel` modules.
4. Find the `<authentication>` section and change the mode to `None`.
5. Enter the URL of the WS-Federation website in the issuer attribute of the `<wsFederation>` element
6. Find the `<trustedIssuers>` section and enter the token-signing certificate thumbprint of the WS-Federation server.

   Note: You should not use cut and paste for the thumbprint as it can insert hidden characters into the file which interfere with the thumbprint matching.

7. If these changes are on a test system that uses self-sign SSL certificates, uncomment the `<certificateValidation>` element.
8. Save the `web.config` file.

If you have to switch back to **Forms Authentication**, the `web.config` file can be edited and the authentication mode set to forms: `<authentication mode="Forms">`.

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

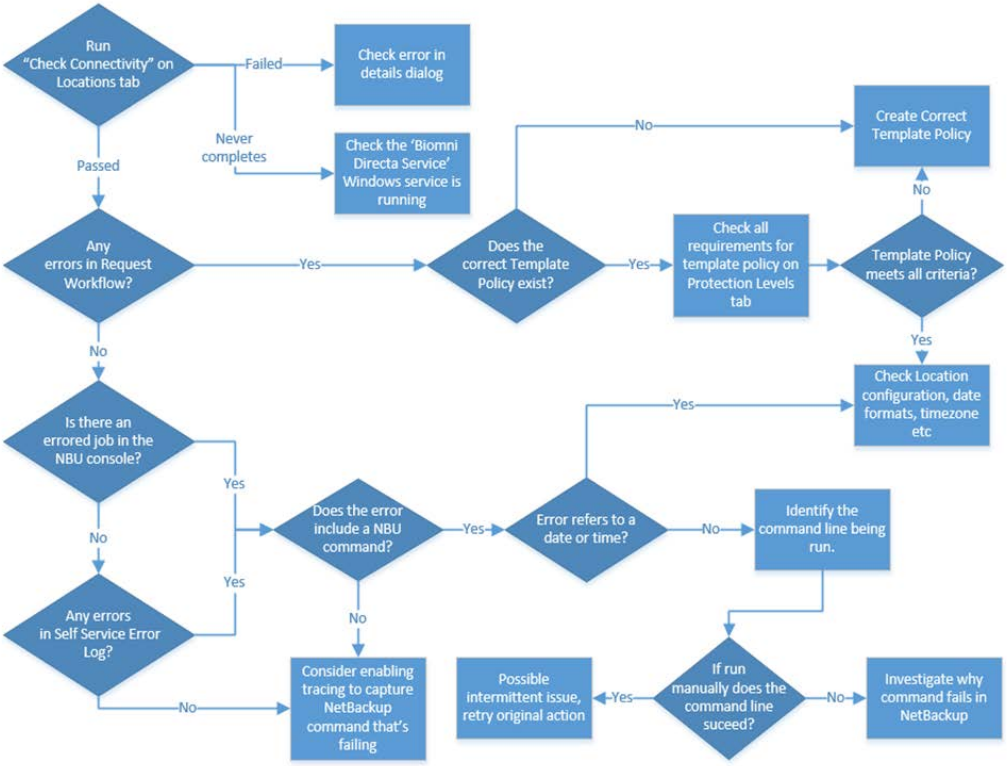
Chapter 7

Troubleshooting

This chapter includes the following topics:

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.



Where to find troubleshooting information

Check Connectivity

On the **Locations** tab the **Check Connectivity** icon tests the connection to each master server in the system. Any failures show as a red cross which can be clicked to show error information.

Request Workflow

Each action in Self Service creates a request in the system. From the **Requests Top** menu you can find the request which can be a good source of troubleshooting information:

Table 7-1 Tab information

Tab name	Details
Fulfillment tab	Any failed steps are red and have errors against them.
Audit tab	Will show progress against the action and can also provide the NetBackup Job Id.

Self Service Error Log

Found in **Admin > Support > Error Log**

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.

Additional activity reporting

An additional source of activity reporting can be found in the **Support** category of the **Admin** home page. This category includes access to Integration Logs, Audit Logs, and Email Logs, as well as a Task Queue and Email Queue.

NetBackup Command-Line Errors

Self Service works by running NetBackup Commands on the command line of the master 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 Master 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 Levels** tab in Admin. Make sure that the Template meets all the criteria that are displayed when you select the green tick that corresponds with its Protection Level.

Synchronization Errors

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

Details incorrect for computer

In the case that image or protection details don't seem correct for a computer, run **Refresh NetBackup Data** for the computer.

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 mouse-over the logged on user name, the option **Raise a request for 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 Master Servers

Concurrent Remote PowerShell Connection Limits

The NetBackup master 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 master 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 master 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\Veritas\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, Windows 2008 R2 defaults to 15. On the master 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 Master Server. Higher throughput is achieved because every call does not require the computer to create and destroy a new Run Space.

Settings

Table 7-2 Location integration settings that are used for PowerShell Connection Pooling

Name	Details
NetBackup Use Pooled Connections	In the event of problems with connection pooling, it can be switched off by changing this setting to False.
NetBackup Minimum Pool Size	Minimum number of run spaces to keep in the pool.
NetBackup Maximum Pool Size	Maximum number of run spaces to keep in the pool.

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 master server:

```
$machineName = 'master_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 Background Tasks

Self Service runs a number of tasks in the background. These background 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 now displayed to the left of the **Monitoring** tab of the home 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 **Task Details** window is displayed. This window shows any error messages, which aids the troubleshooting process.

The **Task Queue** area of the **Monitoring** tab 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 check for errors in Admin > Support > Error Log.

Table 7-3 Background tasks and descriptions

Background task	Description
`FullCacheBuild`	Imports the backup images from all Master Servers since the last time it ran, expires old backup images, and calculates usage. This task runs once per day on schedule.
`ProcessTaskQueue`	Runs frequently to process user actions such as requesting protection.
`RemoveOldActiveRequests`	Performs the internal maintenance of active requests.
`SyncMachineBackupImages`	Handles on-demand refresh NetBackup Image and Protection Data for a single computer.
`UpdateActiveRequests`	Ensures accurate and timely reporting of activities within the user interface.

Table 7-3 Background tasks and descriptions *(continued)*

Background task	Description
`VCloudImport`	Synchronizes the computers from vCloud according to configured imports. This task runs once per day on schedule but can be initiated manually.

Appendix A

NetBackup policy types

This appendix includes the following topics:

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
0	Standard
4	Oracle - client based
6	Informix-On-BAR
7	Sybase
8	MS-SharePoint
10	NetWare
11	DataTools-SQL-BackTrack
12	Auspex-FastBackup
13	MS-Windows-NT
14	OS/2
15	MS-SQL-Server - client based
16	MS-Exchange-Server

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

ID	Name
17	SAP
18	DB2
19	NDMP
20	FlashBackup
21	Split-Mirror
22	AFS
24	DataStore
25	Lotus-Notes
27	OpenVMS
2	FlashBackup-Windows
31	BE-MS-SQL-Server
32	BE-MS-Exchange-Server
34	Disk Staging
35	NBU-Catalog
37	CMS_DB
38	PureDisk Export
39	Enterprise Vault
40	VMware
41	Hyper-V - client based
42	NBU-Search

Appendix B

Dashboard traffic light status and usage

This appendix includes the following topics:

About dashboard traffic light status and usage

The **Status** panel displays a traffic-light presentation. The number of computers in the estate that do not have a backup within the threshold are shown in red. The number of computers in the estate that do not have protection are shown in amber. The number of computers in the estate that have backup within the threshold are shown in green. Full details are shown in Table B-1.

For tenants creating their own backup policies, the Threshold number, which is set in hours, is taken from the relevant Protection Level, if set. The Threshold number is taken from the system-wide default Integration Settings for those tenants who are not creating their own backup policies.

Computer states and the corresponding traffic light status:

Where a tenant creates their own backup policies: threshold from Protection Level threshold used

Table B-1 Protection levels

Protection level	Details
Tenant has protection levels, with a threshold, and computer is protected	■ Backup within threshold > green ■ Backup outside threshold > red ■ No Backups > red

Table B-1 Protection levels *(continued)*

Protection level	Details
Tenant has protection levels, with no threshold, and computer is protected	■ Backup(s) exist > green ■ No backup(s) > red
Tenant has protection levels and computer is not protected	■ Backup within threshold > amber ■ Backup outside threshold > amber ■ No Backup(s) > amber

At the tenant level, the following associated description is used:

- Red: Protected computers with no backup within threshold
- Amber: Computers with no protection
- Green: Protected computers with backup within threshold

Where manually maintained backup policies are used: system default threshold only used

Table B-2 System default threshold value

Default threshold setting	Details
Tenant has no protection levels and a default threshold exists	■ Backup within default threshold > green ■ Backup outside default threshold > red ■ No Backup(s) > amber
Tenant has no protection levels and no default threshold exists	■ Backup(s) exist > amber ■ No backup(s) > amber

At the tenant level, the following associated description is used:

- Red: Computers with no backup within threshold
- Amber: Either computers with no backups (with threshold) or No threshold configured (no threshold)
- Green: Computers with backups within threshold (with threshold)

Clicking on any of the traffic lights automatically expands the Inventory in the central table.

The **Usage** panel is split into two parts: the amount of space that is used as a total and as a graph by month.

Used space 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, both as a percentage and as an absolute amount against that total.

Appendix C

Synchronizing data from NetBackup

This appendix includes the following topics:

About synchronizing data from NetBackup

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

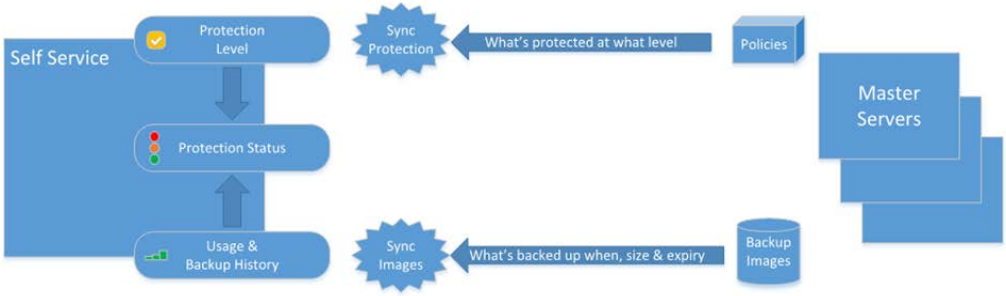


Table C-1 Synchronization process and associated details

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 (colored tick icons). ■ Self Service keeps local cache up to date itself with add and remove protection requests. ■ Contributes to Protection Status, if Protection Levels configured.
Synchronization images	■ Builds the backup history in Self Service from the catalog on master server. ■ Regular task keeps backup history up to date in Self Service with daily incremental synchronization. ■ When a computer is first registered in Self Service initial import of backup history is performed. ■ Images for an individual computer are resynchronized on backup now request completion or when an administrator selects the synchronize backups in the administration panel. ■ 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. ■ Backup History contributes to Protection Status.

Appendix D

NetBackup Self Service data caching process

This appendix includes the following topics:

About NetBackup Self Service data caching process

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

A Custom Task in the portal named **Update Machine Cache** runs every minute and calls code in the Adapter that performs work on a schedule.

The scheduled pieces of work include:

- **Full Cache Build** – runs daily at 12:15 AM.
  Imports the new computers and new or expired backup images. This scheduled work also performs roll-up of image data into totals and calculates traffic light statuses. It also flags the new computers for NetBackup data synchronization.
- **Sync machine images** – runs every minute.

Processes a batch of computers that are flagged for NetBackup data synchronization. Imports the protection levels and backup images, then recalculates traffic light status.

- **Process task queue** – runs every minute.
  Processes a batch of tasks that are queued, for example, when a **Backup Now** request has completed, a computer is protected.

Full Cache Build

The full cache build:

- Imports images from the last day for all online locations. The import includes a 24 hour overlap to get the backups that had started but not completed when the last cache build took place.
- Flags the expired images.
- Updates the last backup time and calculates traffic light status.
- Performs the roll-up calculations on images for computer utilization.
- Deletes rolled up image data and expired images older than 'Utilization Retention Period (Months)' integration setting.

Note: Adding a new location does not trigger any independent action in the system. Any new synchronizations or ongoing synchronizations now include this new location. For example, getting backup images or importing policies. Older images are not imported without manual intervention.

Integration settings

The integration settings listed are relevant to the Full Cache Build.

Utilization Retention Period (Months) (NetBackup Adapter integration section)

The period of time which rollup data and expired backup images are retained for and the number of months displayed in the charts. After this period the rollup data and expired images are deleted in the Full Cache Build as part of Rollup.

NetBackup Data Synchronization

When a computer is imported, **Refresh NetBackup Data** is clicked, or `SyncNetBackupData` is called in the API, the `SyncNetBackupData` flag on computer is set to true. This marks the computer as ready for synchronization and it is picked

up as part of the schedule that runs every minute. This process imports the protection levels and images, then recalculates traffic light status.

The task processes batches of 100 computers for 5 minutes (by default) or until there are no computers requiring import.

Computers added longest ago are processed first.

NetBackup data syncing has a priority value that is defined by the `SyncPriorityId` field in the computer. All computers have the same priority initially but if a 'Backup Now' is performed, that computer is marked as high priority.

If a synchronization fails, the synchronization is locked for a period of time using the `SyncLockedUntil` field on the computers table. This lock allows other computers without errors process.

Integration Settings

The integration settings listed are relevant to the NetBackup Data Synchronization.

Image Import Batch Processing (minutes) (NetBackup Adapter integration section)

The NetBackup data sync gets data for a period of time while there are computer 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, a `BACKUPNOWCOMPLETE` task is queued. This request runs the next time the scheduled task runs.

The task sets the `SyncNetBackupData` flag against the computer to true and `SyncPriorityId` set to high. These values are set so that the computer synchronizes the new image as soon as possible.

Protect computer

When a **Protect Machine** request completes, a `MACHINEPROTECTED` task is queued. This command runs the next time the scheduled task runs.

When the task runs, the protection level is added to the `MachineProtectionLevel` table and the traffic light status is updated.

Unprotect computer

When an **Unprotect Machine** request completes, a `MACHINEUNPROTECTED` task is queued. This command runs the next time the scheduled task runs.

When the task runs, the protection level is removed from the `MachineProtectionLevel` table and the traffic light status is updated.

Appendix E

Integration settings

This appendix includes the following topics:

About integration settings

Integration Settings are used to configure the integration between NetBackup Self Service and NetBackup. Individual Settings are grouped within sections and are accessed through **Admin > Settings > More > 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 (**System wide > tenant > user**). Read the Access Rights section before use.

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 **Admin > Organization > Tenant**, 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.
Action Request Types	This section supports overwrite of specific shipped request types. There should be only one of these sections.

The Integration Settings sections that are generated from completion of an **Add Location** or **Add Protection Level** are:

Table E-2 Generated integration settings

Setting	Details
Machine Location *location*	This type of section contains details for connecting to a NetBackup Master Server which is configured for the Mixed Inventory solution. There can be multiple Machine Location sections: one for each Master Server.
Protection Level *level*	This type of section contains details of the protection options available to tenants when they protect computers. This section includes retention levels and frequencies. Each Protection Level section maps to a NetBackup template policy. There can be multiple Protection Level sections. More information is available. See "Creating NetBackup Template Policies" on page 17.

Table E-2 Generated integration settings *(continued)*

Setting	Details
vCloud Import *import*	This type of section contains details of the vCloud Director instance. Computers are imported from here and this section determines the Self Service location that is associated with the imported computers. Individual tenant credentials are specified against the Tenant. You can have multiple vCloud Import sections. More information is available. See "Registering computers" on page 30.
vCloud Location *location*	This type of section contains details for connecting to a NetBackup Master Server which is configured for the Alternate vCloud configuration. There can be multiple vCloud Location sections: one for each Master Server. More information is available. See "Configuring Locations" on page 23.

NetBackup Adapter

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

Table E-3 NetBackup Adapter settings

Setting	Tenant Override	Details
Customer Code	Yes	A unique value key for associating a computer with a tenant. This value must not be amended post initial use. Mandatory value.
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

Table E-3 NetBackup Adapter settings *(continued)*

Setting	Tenant Override	Details
Default backup warning threshold (hours)	No	The period since last backup, after which the computer status is flagged to the user. This system wide setting is for the traffic light calculation for an unmanaged estate, that is, when no protection levels are specified. Where the estate is managed, the value is taken from the protection level.
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.
Panels URL	No	The URL of the NetBackup Adapter Panels, the installer sets this value initially.
Service URL	No	The URL of the NetBackup Adapter Web Services. The installer sets this value initially.
Policy Types	No	A comma separated list of the NetBackup policy type codes in use. For example, if a system uses Windows and VMware policies, entered values should be 13, 40. More information about policy types is available. See "List of NetBackup policy types" on page 51.
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.

NetBackup Adapter Usage Section

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-4 Adapter settings

Setting Name	Tenant Override	Details
Currency Code	Yes	The short currency code that is used on the home page Usage list, to qualify the Charge column figure.
Cost (per GB)	Yes	Cost per gigabyte, used to calculate Charge.
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, Used Space, or None.
Columns	Yes	Determines whether new backups, used space, or both are displayed in the **Usage graph** and in the **Usage list** as columns of data. Options: New Backups, Used Space, or Both.

NetBackup Adapter Access Rights Section

Determines the actions that are available from the home page for any listed computer. The actions are system wide, for a specific tenant, or for an individual tenant user. The actions are:

- **Backup Now**
- **Protect Machine**
- **Restore File**
- **Restore VM**
- **Unprotect Machine**
- **Register for File Restore**

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

There should be only one of these sections.

Table E-5 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.
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.

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 27.

Action Request Types

This section supports overwrite of specific shipped request types. There should be only one of these sections.

If you choose to change the shipped request type detail, create a copy of the shipped request type first. Then the new request type is amended as required. Once that is complete, the new request type can be activated and this section updated with the new request type code. The shipped request type can then be deactivated.

Table E-6 Action Request Type

Setting Name	Tenant Override	Details
DB Backup Now	No	The request type code that is associated with the Backup Now dashboard option. Defaults to DBBACKNOW.
DB Restore VM	No	The request type code that is associated with the Restore VM dashboard option. Defaults to DBRESTVM.
DB Restore File	No	The request type code that is associated with the Restore File dashboard option. Defaults to DBRESTFILE.
DB Protect Machine	No	The request type code that is associated with the Protect Machine dashboard option. Defaults to DBNEWBACK.
DB Unprotect Machine	No	The request type code that is associated with the Unprotect Machine dashboard option. Defaults to DBREMBACK.
DB Register for File Restore	No	The request type code that is associated with the Register for File Restore dashboard option. Defaults to DBREGDNS.

Machine Location

This section type contains details for connecting to a NetBackup Master Server. There can be multiple Machine Location sections: one for each Master Server.

Table E-7 Machine Location

Setting	Tenant Override	Details
NetBackup server	No	The NetBackup Master server for this location.
NetBackup UserName	No	The user name to connect to the NetBackup Master server.

Table E-7 Machine Location *(continued)*

Setting	Tenant Override	Details
NetBackup Password	No	The password for connection to the NetBackup server. If using encryption, an encrypted SSH key is used as the pass phrase.
NetBackup Folder	No	The Location on the NetBackup Master server that the NetBackup Commands are installed in. Default values are: `C:\Program Files\Veritas\NetBackup` for Windows `/usr/openv/netbackup` for UNIX
NetBackup OS	No	The Operating system of the NetBackup server.
NetBackup TimeZone	No	If the server time zone for the Self Service NetBackup Adapter and your NetBackup Master server are the same you do not need to configure the timezone. If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.
NetBackup DateFormat	No	Specifies the format the Master Server expects dates to be supplied in. MM\/dd\/yyyy See "Configuring Locations" on page 23.
NetBackup DateTimeFormat	No	Specifies the format the Master Server expects date and time to be supplied in. MM\/dd\/yyyy HH\:mm\:ss See "Configuring Locations" on page 23.
NetBackup OpenSSH Key	No	For connection to UNIX Master Servers with SSH. The key must be in the OpenSSH format.
NetBackup Use Pooled Connections	No	Windows Master Servers Only. Enabled by default, and should be left on for normal usage. Controls pooling of PowerShell connections to the Master Server.
NetBackup Minimum Pool Size	No	Windows Master Servers Only. Used for support purposes only.

Table E-7 Machine Location *(continued)*

Setting	Tenant Override	Details
NetBackup Maximum Pool Size	No	Windows Master Servers Only. Used for support purposes only.
Get Backups Chunk Size in Hours	No	When Self Service synchronizes computer backup images from NetBackup, they are retrieved in batches of this size. The system defaults to 25 but may need to be reduced for very busy systems with lots of backup activities. Reducing the number results in more calls to NetBackup to retrieve a given number of images. The total images that are retrieved remains the same.
Maximum backup duration (hours)	No	The maximum time a backup should take in hours on NetBackup. Used by the synchronize engine to estimate a buffer period when you synchronize backup images. This value should be changed only if synchronization problems occur.
Online	No	Indicates if the Master Server is considered online. The system does not use the locations that are not online in any way. Users are blocked from taking the actions that affect the location. Used for planned maintenance or in the event of an outage.

Note: More information about editing the date and the time format is available.

https://msdn.microsoft.com/en-us/library/8kb3ddd4%28v=vs.110%29.aspx

Protection Level

This type of section contains details of the protection options available to tenants when they protect computers, for example retention levels and frequencies. Each Protection Level section maps to a NetBackup template policy. There can be multiple Protection Level sections.

See “Creating NetBackup Template Policies” on page 17.

Table E-8 Protection level information

Setting name	Tenant override	Details
Name	No	The display name for the Protection Level as displayed to users.
Sequence	No	A number that is used to order all Protection Levels in the UI, 1 at the start of any list, higher numbers further down.
Description	No	A description of the backup schedule and retention, for example, Weekly backup, retained for one month.
Visible	Yes	Controls whether the Protection Level is available to users. Can be set to True or False. Can be overridden at a tenant level.
Template suffix	No	Used to select a template policy in NetBackup when you protect a computer with this protection level. Template-0-SL1 or Template-13-SL1 where 'SL1' is the specified Template Suffix.
Backup warning threshold (hours)	Yes	Once a computer has been protected, if no backups have occurred within the backup threshold, the computer is flagged for attention. The value should be related to the backup schedule of the template policy. If the backup schedule is daily, a warning threshold of 48 hours could be appropriate.
Color	No	On-screen color for this Protection Level. Can be any HTML color value, e.g. yellow would be `yellow` or `#FFFF00`.

vCloud import

This type of section contains details of the vCloud import process which allows computers to be imported from a specific vCloud Director instance and registered with NetBackup Self Service. The computers are imported on a tenant by tenant basis using individual credentials. There can be multiple vCloud Import sections.

Table E-9

Setting name	Tennant override	Details
vCloud Api	No	This value should be set to the URL of the vCloud API, in the format of `https://hostname/api/`.
Location	No	The name of the NetBackup location the computers are registered to
Online	No	Indicates if the vCloud Director instance is considered online. Self Service does not use the instances that are not online.
Ignore SSL Certificate Errors	No	This option allows the Self Service to connect to vCloud Director instances where the SSL certificate is not valid.
vCloud *username*	Yes	The user name that the tenant uses to connect to the vCloud 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*	Yes	The tenant's corresponding vCloud password. Must be set at the tenant level only.

Appendix F

Policy Modifiers

This appendix includes the following topics:

About policy modifiers

Policy Modifiers are a method of selecting a set of Template Policies at a finer level of control than either a location or a master server. This feature is an advanced feature that should be used with care.

In a typical Self Service solution each Location and hence each NetBackup Master Server has one set of Template Policies. All computers that are associated with that location use the same Template Policies. If more flexibility is required it is possible to set a Policy Modifier on a per computer basis. This option makes the system select a different set of Policy Templates for use with that computer.

Template Policy Naming with Policy Modifiers

PolicyType and ProtectionLevel are as per normal Template Policy configuration.

Scheduled Backup: Template-*PolicyModifier-PolicyType-ProtectionLevel*

BackupNow: Template-*PolicyModifier-PolicyType*-BackupNow *PolicyModifier*

The actual policy modifier can be any arbitrary text, within the restrictions of NetBackup policy naming.

Registering computers with Policy Modifiers

You cannot register a computer with a policy modifier through the Self Service Portal. Policy Modifiers are only supported in the CreateMachine method of the NetBackup Adapter API. See the NetBackup Adapter API documentation in install directory for more information.

Policy Modifier Example

When you use a single Master Server with multiple geographically separated media servers, you can associate each computer to its closest media server by setting a policy modifier against it. Two sets of Template policies are then created on the Master Server, each configured for a particular media server.

Given the following:

- A single master server
- Two media servers, one at **SiteA** and one at **SiteB**
- Requirements to support policy type 0 (standard) and 13 (Windows), for scheduled backups and Backup Now

You can use Policy Modifiers of **SiteA** and **SiteB** for each media server. The Master Server would need Template Policies created referring to each policy modifier:

```
Template-SiteA-0-PL1
Template-SiteA-13-PL1
Template-SiteA-0-BackupNow
Template-SiteA-13-BackupNow
Template-SiteB-0-PL1
Template-SiteB-13-PL1
Template-SiteB-0-BackupNow
Template-SiteB-13-BackupNow
```

The **SiteA** Template Policies would then be configured for one media server, and **SiteB** for the other. Computers can then be registered in the system with Policy Modifiers of **SiteA** or **SiteB** accordingly.

Appendix G

Configuring Self Service Alternate vCloud

This appendix includes the following topics:

Configuring the Alternate vCloud Configuration

The vCloud integrated configuration of the previous Self Service versions is now known as **Alternate vCloud Configuration**. The Alternate vCloud Configuration in Self Service provides real-time interrogation of vCloud at the time a user wants to protect, backup, or restore. It has no compatibility with the main Self Service dashboards but does provide the extra flexibility of container level (vDC, vApp) backups.

You cannot use this configuration with the main dashboards of Self Service. As such, it has limited out of the box reporting.

It does not require you to import the vCloud infrastructure into Self Service on schedule. Instead, this option allows the user to browse the infrastructure at the

time of request. It also provides container level protection of vDC's and vApp's. This solution requires manual configuration.

Note: You must configure vCloud in NetBackup must before you enable NetBackup Self Service. The VMware vCloud director must support API version 5.1.

Integration Settings and creating and editing Locations or Protection Levels

Integration Settings are a flexible store of named settings with values. They are an integral part of Self Service. All integration settings can be accessed as an Admin user from **Admin > Settings > Integration Settings**.

Settings are grouped into sections. Locations and Protection Levels exist in Self Service as Integration Settings that are grouped into a section. A single section defines each individual Location or Protection Level.

Care must be taken, however, as no validation is performed when entering values or editing values directly through Integration Settings. A sample location is available on installation to demonstrate the data and format of what you must complete.

Configuring vCloud Locations

A location represents a connection to a NetBackup master server and its associated vCloud instance. The system requires at least one vCloud Location.

A PowerShell script `Create-AlternateVCloudLocation.ps1` is provided that creates a new Alternate vCloud Location. By default, this script is located in the installation folder.`C:\Program Files (x86)\Biomni\Front Office 8.3\Sdk\Docs`.

To use the provided PowerShell script to create a vCloud location

1. Edit the script and set the URL of the Public web services correctly.

   The correct URL is found in **Admin > Configuration Check** page in Self Service.

2. Run the script. Follow the onscreen prompts to create the location.

3. Once the script completes you can check or edit the details of the new location in **Admin > Settings > Integration Settings**. The new section is named **vCloud Location *name***

Note: Create your vCloud locations using the PowerShell script as the **NetBackup TimeZone**, **NetBackup DateFormat**, and **NetBackup DateTimeFormat** values that are associated with the location are complex. The PowerShell script provides assistance in correct entry.

Integration Settings that are used in an Alternate vCloud configuration

vCloud vOrg and logon credentials must be overridden at a tenant level. No other settings should have tenant or user overrides.

The name of the section forming the Location is in the format `vCloud Location abc`, where *abc* is the name of the location.

Table G-1 vCloud location integration settings

Item	Details
NetBackup server	The NetBackup Master server for this location.
Online	Determines if the Master Server is considered online. The system does not use the locations that are not online in any way. Users are blocked from taking the actions that affect the location. Used for planned maintenance or in the event of an outage.
NetBackup UserName	The user name to connect to the NetBackup Master server. This value is typically empty at the top level.
NetBackup Password	The password for the connection to the NetBackup server. If using an encrypted SSH key is used as the pass phrase. This value is typically empty at the top level.
NetBackup OS	The Operating system of the NetBackup server.
NetBackup Folder	The Location on the NetBackup Master server that the NetBackup Commands are installed in. Default values are: `C:\Program Files\Veritas\NetBackup` for Windows `/usr/openv/netbackup` for UNIX
NetBackup TimeZone	If the server time zone for the Front Office NetBackup Adapter and your NetBackup Master server are the same you do not need to configure the timezone. If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.
NetBackup DateFormat	Specifies the format the Master server expects dates to be supplied in. See "Configuring Locations" on page 23.

Table G-1 vCloud location integration settings *(continued)*

Item	Details
NetBackup DateTimeFormat	Specifies the format the Master Server expects date and time to be supplied in. See "Configuring Locations" on page 23.
NetBackup OpenSSH Key	For connection to UNIX Master Servers with SSH. The key must be in the OpenSSH format.
NetBackup Use Pooled Connections	Windows Master Servers Only. Enabled by default, and should be left on for normal usage. Controls pooling of PowerShell connections to the Master Server.
Backup Minimum Pool Size	Windows master servers Only. Used for support purposes only.
NetBackup Maximum Pool Size	Windows master servers Only. Used for support purposes only.
vCloud API	This value should be set to the URL of the vCloud API, in the format of `https://hostname/api`.
vCloud vOrg	The tenant's vOrg in vCloud. Must be set at the tenant level only.
vCloud UserName	The vCloud user name that Front Office uses to access the vCloud API (specified in the General Integration Settings). 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 password. Must be set at the tenant level only.
File Restore Domain Suffix	The File Restore Domain Suffix is only required if using File Restore. When you restore files to a NetBackup client, the client computer must be addressable from the NetBackup media server through a DNS name in the format: *`VM name.vApp name.vDC name.vOrg Name.Domain Suffix`* The Domain Suffix is this setting, and should start with a dot (.), for example `.vcloud.local`

Configuring Protection Levels for vCloud

A Protection Level indicates the standard of protection that is applied to a computer. The Protection Level corresponds to template policies on all of the NetBackup master servers in the system. These template policies can then have different schedules, retention levels, etc., allowing different Protection Levels to have different characteristics. This functionality provides users a level of abstraction away from more complex NetBackup concepts.

As an example the system can be configured with three Protection Levels: Bronze, Silver, and Gold. Retention level and frequency of backups increase as you work up the scale of Protection Levels.

You must create your Protection Level or Levels in **Admin > Settings > Integration Settings**. To add a new protection level, click **Add Section** at the top of the page. Enter the name of your protection level with the prefix **Protection Level**. For example, **Protection Level *name***.

Once you have created the section, click **Add Setting** to insert each of the settings in Table G-2. Use the value in the **Item** column as the setting name.

You can configure multiple protection levels in this fashion.

See "Creating NetBackup Template Policies" on page 17.

Table G-2 Integration Settings that are used in a Protection Level

Item	Details
Name	The display name for the Protection Level as displayed to users.
Sequence	A number that is used to order all Protection Levels in the user interface, 1 at the start of any list, higher numbers further down.
Description	A description of the backup schedule and retention, for example Weekly backup, retained for one month.
Visible	Controls whether the Protection Level is available to users. Can be set to True or False. Can be overridden at a tenant level.
TemplateSuffix	Used to select a template policy in NetBackup when you protect a computer with this protection level. For Template-0-SL1 or Template-13-SL1 the specified Template Suffix is SL1.

Configuring Alternate vCloud Backup Now retention levels

Backup Now requests use the default retention levels. The default retention levels come preinstalled with NetBackup Self Service. You can, however, amend and modify the retention levels that are offered to users if you edit the request form.

To edit the request form:

1. Go to **Admin > Request & Approval > Request Type > Backup Now (VCDBACKNOW)**.
2. Click on the **Form** tab and then the **Backup retention** field.
3. At the base of the page, click on the **Configuration** tab.
4. Listed under the **Items** field is a paged list of retention levels that are available in the Backup Now request form. You can add new levels or delete the existing levels with the trashcan icon.
5. The code must match the NetBackup retention number. The description is what the user sees.

Configuring Tenants

Create and edit vCloud tenants with **Admin > Organization > Tenant**. Once the name is created, navigate to the **Integration** tab and complete the vCloud vOrg, vCloud UserName, and vCloud Password for all appropriate vCloud Location sections.

You can also create tenants with an API. More information about the API and SDKs available can be found in the install location of the NetBackup Self Service portal. The default install location is `C:\Program Files (x86)\Biomni\Front Office 8.3\Sdk\`. Microsoft developers should use the SDK. Non-Microsoft developers can call the web service directly. The URL can be found in **Admin > Support > Configuration Check** in the **Public Web Service** section of the **Server** tab. The web service is `DirectaApi.svc`.

Configuring the home page for Alternate vCloud configuration

NetBackup Self Service is shipped with the main dashboard configuration enabled and Alternate vCloud configuration disabled. If running in Alternate vCloud

configuration, it is necessary to disable the dashboard and enable the correct home page panels and request types.

To configure the home page

1. Go to **Admin > Service Catalog and Notices > Service Catalog**.
2. Disable the **Status Summary** panel.

   Click on the top left link **Status Summary**. From the next page, click the **Edit** icon, at the top right of the page. Uncheck the **Enabled field**.
3. Disable the **Usage Summary** panel.

   Click on the top right link **Usage Summary**. From the next page, click the **Edit** icon, at the top right of the page. Uncheck the **Enabled field**.
4. No more than the six bespoke request types are needed to support the Alternate vCloud configuration. You must activate these request types. To activate these requests, go to **Admin > Request & Approval > Request Type**. Select **Inactive** from the Active filter and click **Go**. Activate the request types that are listed. All other Request Types shown in the **Request Type** list may be deactivated, as they are not used in this configuration.

Backup Now	`VCDBACKUPNOW`
Protect Machine	`VCDNEWBACK`
Register VM for File Restore	`VCDREGDNS`
Restore File	`VCDRESTFILE`
Restore Machine	`VCDRESTVM`
Unprotect Machine	`VCDREMBACK`

5. Enable the **vCloud NetBackup Services** panel.
   - Click on the link **vCloud NetBackup services**.
   - From the next page, click the **Edit** icon, at the top right of the page.
   - Check the **Enabled** field.

   This Service Catalog category contains a list of Services, identified by an icon. Each service links to a request form:
   - **Protect Machine**
   - **Backup Now**
   - **Unprotect Machine**

- **Restore VM**
- **Restore File**
- **Register VM for File Restore** (email notification only)

Services can be found in **Admin > Service Catalog and Notices > Service**.

6 Enable the **vCloud Protected** panel.

- Click the **vCloud Protected** link.
- From the next page, click the **Edit** icon, at the top right of the page.
- Check the **Enabled** field.

This Service Catalog panel references the Integration Setting Panel's URL in the **NetBackup Adapter** section for the URL of the NetBackup Self Service Adapter. **Admin > Settings > Integration Settings**.

7 Enable the **vCloud Unprotected** panel.

- Click the **vCloud Unprotected** link.
- From the next page, click the **Edit** icon, at the top right of the page.
- Check the **Enabled** field.

This Service Catalog panel references the Integration Setting Panel's URL in the **NetBackup Adapter** section for the URL of the NetBackup Self Service Adapter. **Admin > Settings > Integration Settings**.

Appendix H

Glossary

This appendix includes the following topics:

Glossary

Table H-1 Glossary of terms

Term	Definition
Alternate vCloud configuration	When the NetBackup Self Service system is set up with vCloud; vCloud controls management of computers and tenant ownership of them.
Backup Now	A user action in Self Service that creates a temporary Policy on the master server and schedules it for immediate backup. The template policy is deleted afterwards.
Computer	Any physical or any virtual machine that the solution is aware of.
Customer Code	A unique code that is set at the tenant level of integration settings. Used in the policy names that are created for that tenant (Managed estate) and to associate a computer to a tenant.
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**.

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

Term	Definition
Location	A location represents a connection to a NetBackup Master 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.
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.
Policy Modifier	Allows multiple sets of Template Policies on a Master Server, and determines their selection at a computer level. You should use this feature as an exception only. An advanced feature for dashboard configurations only.
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 Master Server.
Refresh NetBackup Data	Computer level manual or automated process to rebuild image data, protection data, and traffic lights.
Register Machine	The process 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 VM	A user action in Self Service that creates a job to restore a virtual machine in NetBackup.
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**.

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

Term	Definition
Service Provider	Refers to the top-level organization administering the Self Service system.
Template Policies	Inactive NetBackup Policies on a master 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.
Unprotect (computer)	A user action in Self Service that results in a computer being removed from a NetBackup Policy.
vCloud 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 DAPI.