NetBackup™ Self Service Installation Guide

11.0

Document version: 1

VERITAS™

NetBackup™ Self Service Installation Guide

Last updated: 2025-08-29

Legal Notice

Cohesity Inc
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Cohesity account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Cohesity community site:

http://www.veritas.com/community/

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Introduction

This chapter includes the following topics:

About Self Service components

The installer consists of the `setup.exe` file.

The installation process installs the following components:

- Panels
- Tasks
- Database

The focus of this guide is the two-server install. A web server that hosts the website and Windows Service, and a database server that hosts the databases.

You can extend your NetBackup Self Service solution by using one of the additional add-ons. You can find more information, as well as download details, on the Veritas Open Exchange (VOX). A link takes you to the specific post.

- Cohesity NetBackup Self Service plug-in for VMware vRealize Automation
  https://tinyurl.com/ybldbpcx
- Cohesity NetBackup Self Service plug-in for VMware vCloud Director
  https://tinyurl.com/y77f68jv

Chapter 2

Prerequisites

This chapter includes the following topics:

About prerequisites

The person who installs NetBackup Self Service needs a working knowledge of SQL Server, Windows Services, and Internet Information Services (IIS).

NetBackup Self Service can be installed on the following Windows platforms:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Note: Apply the latest service packs to the operating system.

The prerequisites for each component are:

Table 2-1

Component	Requirement
Database	■ Microsoft SQL Server 2016, 2017, 2019, or 2022, allowing SQL authentication method ■ Azure SQL database or Microsoft SQL Server on Amazon RDS ■ At least 5 GB free disk space for data and 2 GB for logs

Table 2-1 *(continued)*

Component	Requirement
Website and Windows Service	■ Microsoft .NET Framework version 6.0.32 ■ Microsoft PowerShell version greater than 7.2 (part of standard Windows installation) ■ Access to an SMTP server ■ At least 1 GB free disk space ■ .NET Desktop run-time 6.0.32 ■ IIS run-time support (ASP.NET Core Module v2) ■ Internet Information Services (IIS) ■ Microsoft ODBC driver 17 for SQL Server ■ Microsoft Command Line Utilities 15 for SQL Server **Note:** You can install the prerequisites that are shown with the installer if the internet is available: Microsoft .NET Framework, .NET Desktop run-time, IIS run-time support, IIS, ODBC driver, Command-Line Utilities. If the internet is not available, two batch files are available that can download all the prerequisites and install them once they are copied to the computer without internet connectivity. The batch files are `Download Prerequisites.bat` and `Install Prerequisites.bat` which are located in the Silent Files folder in the setup package.

Chapter 3

Installation

This chapter includes the following topics:

Installation overview

You can install Self Service either with the `.msi` file or through the silent install method. Table 3-1 provides an overview of the process. Additionally, this chapter provides details on where the various Self Service components are installed.

Table 3-1 Installation overview

Step	Additional information
Https	See "About the default HTTPS configuration" on page 28.
Graphical user interface (GUI) install	See "Graphical user interface install" on page 10.
Silent install	See "Silent install" on page 10.
Validation	See "Validation" on page 11.

Graphical user interface install

This section guides you through the installation of NetBackup Self Service.

To install NetBackup Self Service

1. Run *install_path*\setup.exe, which launches the InstallShield Wizard. The installer runs and copies the installation files onto disk. When it completes, the configurator launches.
2. The configurator reviews your local environment for the installation status of NetBackup Self Service.
3. If the configurator doesn't find a NetBackup Self Service installation, it shows you a configuration page with the default values that you can change. Select **Start Installation** to start the installation process.
4. The **Portal Name** field defines the name of the site. Self Service uses it to create the names of the IIS Applications and Windows service the installer creates. You cannot change the portal name once the installer runs. Choose the **Portal Name** carefully.

   On the **Database to be created** dialog, enter the information about the database you want created. The default database name is the same as the **Portal Name**. Cohesity recommends that you keep the default database name.

   System Base Currency defines the currency type that Self Service uses.

   The **System Base Language** defines the language that is displayed in the user interface.
5. The final page of the configurator contains the URL for the website. The credentials for the initial logon are:

   - **User ID**: Admin.
     The user ID is not case-sensitive.
   - **Password**: password.
     The password is case-sensitive.

   You are required to change the password at first logon. Keep a copy of the URL from this screen. Use this URL to connect to the system.

Silent install

Before you attempt to install NetBackup Self Service, confirm that the current computer meets all installation requirements for NetBackup Self Service. These requirements include confirming there is not an older version of NetBackup Self Service already installed.

To install NetBackup Self Service silently:

1. Edit the configuration file `Install.ini`. Be sure to update the `DatabaseServer`, `UserNameForSA` and `PasswordForSA` settings.

   You can set `UseWindowsAuthentication=1` and leave the `PasswordForSA` value empty if you want to use windows authentication to log on SQL Server.

2. Right click the *`install_directory`*`\SilentInstall.bat` and select **Run as administrator**. The installation starts and the command-line window displays the installation progress. The command-line window closes after the installation completes.

   You can also launch the silent install directly from the command line. Open a command prompt, change to the directory that contains the `SilentInstall.bat` file, and then run `SilentInstall.bat`.

An installation log file, *`timestamp`*`_install.log`, is generated in the same directory as the `SilentInstall.bat` file. Review this file to see the installation results. If the installation succeeded, you can visit `https://`*`domainname`*`/NetBackupSelfService` for testing. If the installation failed, troubleshooting information is found in the installation log.

Validation

When the installation completes, log into to the website with the URL and credentials from the final screen of the portal installation. More information on how to validate the installation and perform the initial setup is available.

See "About post-installation validation" on page 20.

Installed components

This section shows the results of a default installation of NetBackup Self Service. It shows the components that are installed and where they are installed.

File System

The portal and the adapter are installed under `C:\Program Files\Cohesity\NetBackup Self Service` *`version_number`*.

IIS

In this configuration, an IIS public website is created to host the web pages.

Windows Service

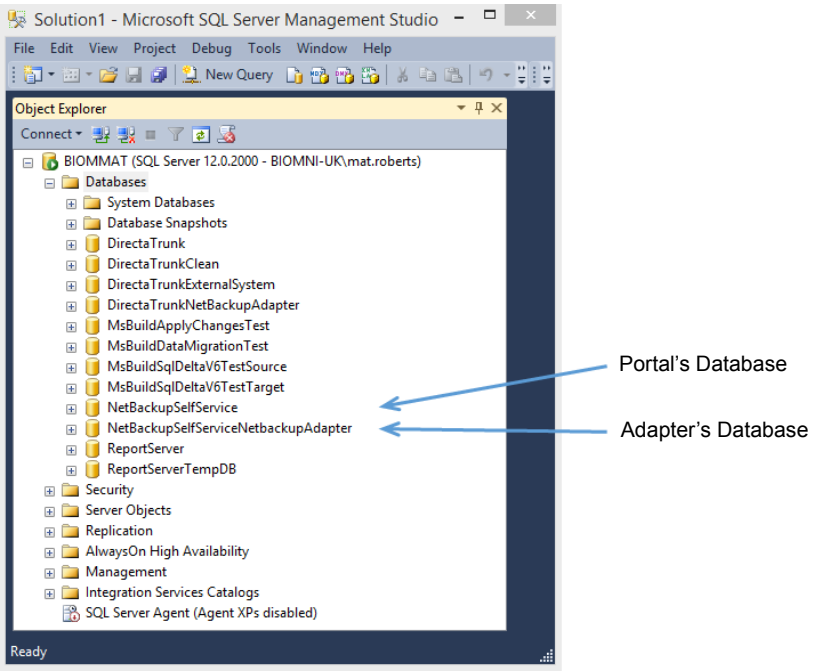
The portal installs a Windows Service.

Database

Two databases are created:

- Portal's database: **NetBackup Self Service**
- Adapter's database: **NetBackupSelfServiceNetBackupAdapter**

Figure 3-1 Self Service Databases



Soap service

The Soap Service URL has changed to `https://domain:httpsport/NetBackupSelfServicePublicWebService`. The endpoint for automation against the soap service is available in the `wsdl` file at the able location at the very end of the document and appears as follows:

The **Location** value is your endpoint for automation purposes. Note that the URL ends with `DirectaApi`.

Chapter 4

Upgrade

This chapter includes the following topics:

Review current environment configuration

Before you begin the upgrade, review your existing installation. Self Service has six components that are typically distributed across two servers.

Table 4-1 Typical Self Service configuration

Location	Component
IIS server	■ NetBackupSelfService ■ NetBackupSelfServicePubilcWebService
Windows services	■ Portal Windows service ■ Adapter Tasks (Self Service 9.1 and later)

Table 4-1 Typical Self Service configuration *(continued)*

Location	Component
SQL server	■ Portal database ■ Adapter database

You can identify the components in your environment from within NetBackup Self Service.

- Identify the IIS components.
  Log on to the web server and open **Internet Information Services (IIS) Manager**.
  Browse the sites and identify the two IIS components that are listed in Table 4-1.
- Identify the Windows service.
  Log on to the server with the Windows Service. In a default installation of Self Service, the service is located on the web server.
  Open **Services** and locate the **Portal Windows Service**.
- Identify the databases.
  Open Microsoft SQL Server Management Studio, and connect to the database server.
  Identify the two databases that are listed in Table 4-1.
  See "Installed components" on page 11.

Upgrade preparation

You must perform several steps to prepare for an upgrade.

To prepare for an upgrade

1 Back up the databases

You should back up both Self Service databases before you start the upgrade. The default names for the databases are **NetBackupSelfService** and **NetBackupSelfServiceNetBackupAdapter**. Perform these steps in **SQL Server Management Studio**.

- Make a note of the **NetBackupSelfService** database recovery model.
- Set the database recovery model to **Simple**.
- Back up the database.
- Make a note of the **NetBackupSelfServiceNetBackupAdapter** database recovery model.
- Set the database recovery model to Simple.

- Back up the database.

2 Take the portal offline.

Cohesity recommends that you prevent user logon and user activity while the upgrade is active. The best way to prevent user logon and user activity is to use **Internet Information Services (IIS) Manager** to stop the application pool for the portal website.

If a user attempts to connect to the website when the application pool is stopped, they receive an `HTTP Error 503. The service is unavailable` error in their web browser.

Do not stop the other application pools during the upgrade. If you stop the application pools with the suffix **PublicWebServiceAppPool** then the upgrade fails. The public web service is used for the upgrade.

Graphical user interface (GUI) upgrade

To upgrade NetBackup Self Service

1 Run the installer *`install_directory`*`\setup.exe`.

The installer runs and copies the installation onto the computer. When the installation completes, a configurator launches.

2 The original configuration parameters are filled automatically. Select **Start Upgrade** to start the upgrade.

3 After successful completion of the upgrade, verify that your machine currently uses the latest versions of Microsoft .NET Runtime 6.0 and Microsoft Windows Desktop Runtime 6.0. If it uses earlier versions of those applications, go to the Microsoft download site to obtain the latest version of each one, and then install them.

Silent upgrade

Before you attempt to upgrade NetBackup Self Service, confirm that NetBackup Self Service is installed on the current computer.

To upgrade NetBackup Self Service silently:

1. Create back up copies of the NetBackup Self Service databases. By default, they are named `NetBackupSelfService` and `NetBackupSelfServiceNetBackupAdapter`. Create backups from either the command line or from SQL Management Server.
2. The silent upgrade can collect all required information from the existing NetBackup Self Service installation. You do not need to configure anything before you launch the upgrade.

   Right click the *`install_directory`*`\Silent Upgrade.bat` and select **Run as administrator**. The upgrade starts and a command-line window displays the upgrade progress. The command-line window closes after the upgrade completes.

   You can also launch the silent upgrade directly from the command line. Open a command prompt, change to the directory that contains the `SilentUpgrade.bat` file, and then run `SilentUpgrade.bat`.

An upgrade log file, *`timestamp`*`_upgrade.log`, is generated in the same directory as the `SilentUpgrade.bat` file. Review this file to see the upgrade results. If you see `Upgrade succeeded` at the end of the file, the upgrade was successful. If you see `Upgrade failed`, the upgrade was not successful. If the upgrade failed, troubleshooting information is found in the upgrade log.

Validation

To validate the upgrade:

1. Start the portal application pool to bring the website online.
2. Log into the portal.
3. Perform the validation steps to confirm correct installation.

   See “About post-installation validation” on page 20.

Post upgrade resynchronization

After the upgrade, manually resynchronize the data between NetBackup and vCloud Director, if Cloud is used. Two scheduled tasks run once per day: System Sync and Asset Import. System Sync imports any new backup images from all backup servers, expires old backup images, and calculates usage. Until these tasks are run, the data that is displayed to the user may be incomplete.

To resynchronize the data

1. Log in to the website as an administrator, and navigate to the **Monitoring** tab. The left side of the screen shows scheduled tasks.
2. Click the cog next to the **System Sync** task and select **Run Now**.
3. (Conditional) If you use vCloud Director, click the cog next to the **Asset Import** task, and select **Run Now**.
4. The **Activity** section on the right side of the screen monitors the progress of these tasks.

If you do not perform these steps manually, the tasks run automatically overnight.

Post upgrade steps

After the upgrade finishes, complete a connectivity check for all primary servers.

Cohesity also recommends that you re-synchronize all data.

As part of the upgrade, the two databases were backed up and the recovery model was set to **Simple**. Revert the database's recovery model to its initial value.

To revert the database to its initial value:

1. Shrink both databases.
2. Set the recovery model of the databases back to its original value.

When an upgrade is performed a new set of code is placed in a new location on the server. Once the upgrade is complete, remove the old installation.

To remove old installation code

1. Go to **Add/Remove Programs**.
2. Uninstall any previous versions of:
   - **NetBackup Self Service Portal**
   - **NetBackup Self Service Adapter**

Rollback

To revert back to the previous version, a restore of the two NetBackup Self Service databases is required. Additionally, you must reinstall the previous portal and adapters or restore their web server from a backup).

If you reinstall the portal and the adapters, ensure **Database** is not selected on the **Select Components** dialog box during install. In both cases the database is restored and does not need to be reinstalled.

During the portal reinstallation, when prompted for an application key, enter the application key from the previous installation. This application key is the key used to encrypt third party passwords in the restored databases and was recorded when the previous version was deployed.

Chapter 5

Post-installation validation

This chapter includes the following topics:

About post-installation validation

When you complete the installation, you can validate the installation with a series of checks.

Table 5-1 NetBackup Self Service validation checklist

Validation	Additional details
Perform a visual check of the website main screen.	See "Visual Check" on page 20.
Confirm the Windows service is configured correctly.	See "Windows Service" on page 21.

Visual Check

After installation it is important to check that the system has installed correctly. Log on to the portal website. The main screen of the website should display correctly.

IIS configuration check

After installation, check that IIS is configured correctly. Search for **Internet Information Service** in the **Start** menu.

- Under **Internet Information Service > Sites > Default website > Bindings**, confirm that the installer created an SSL certificate.
- Under **Internet Information Service > Sites > Default website > Bindings**, confirm the binding for port 443 is created and the certificate is assigned to that port.

Windows Service

After an install, it is advisable to check that the Windows service is running correctly. On the server where the Windows service is installed:

- Open Event Viewer, and navigate to the Application Log.
- Find messages with a source of **DirectaService11.0$NetBackupSelfService**. The name may vary slightly - the naming convention is **DirectaService11.0$*SiteName***, where *SiteName* is the name of the website.
- If the Windows service has logged any errors then it is possible there is a configuration problem. Examine the detail of the error.

A common configuration problem is the Windows service cannot connect to the database. The Windows service checks to confirm that connectivity to the database is defined in the configuration file. If the service cannot connect to the database it logs an error in the Windows Event Log.

Chapter 6

Uninstallation

This chapter includes the following topics:

Uninstalling NetBackup Self Service

The uninstallation process removes the Windows service that is connected to the installation location. It then deletes the software on the hard disk.

The uninstallation does not delete the two databases that were created. The databases must be deleted manually.

To uninstall a NetBackup Self Service

1. Determine the version of NetBackup Self Service you want to uninstall.
2. Locate and stop the service **Cohesity Front Office Service 11.0 (NetBackupSelfService)**.
3. In Windows open **Programs and Features**.
4. Locate **NetBackup Self Service *version***, and select uninstall.

When the uninstall process finishes, delete the databases from within SQL Server Management studio. From **Object Explorer**, expand the **Databases** node. Right-click on each of the relevant databases and select **Delete**.

Appendix A

Software requirements

This appendix includes the following topics:

NetBackup software requirements for Self Service

NetBackup 8.0 or later with the latest service pack is required. With a Windows primary server, only US English operating system and code page installations of NetBackup are supported. NetBackup language packs are not supported.

With a UNIX primary server, the character encoding of the primary server operating system must be UTF-8. Multiple locales are supported. NetBackup language packs are supported.

NetBackup appliances are supported.

Software requirements for Self Service

The Self Service software requirements are

- If using a vCloud Director Integrated configuration, check the Software Compatibility List for supported API versions.
  http://www.netbackup.com/compatibility
- NetBackup Self Service works on any virtual platform, such as Hyper-V or vSphere, provided one of the supported operating systems is installed.

The lists that are shown define the supported operating systems, SQL servers, and web browsers. The latest service pack should always be used.

Note: Any version of operating system, SQL server, and web browser that is not listed as **Supported** is considered unsupported.

Supported operating systems:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Supported SQL server:

- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL Server 2022
- Azure SQL database
- SQL Server on Amazon RDS

Supported browsers:

- Internet Explorer
- Edge
- Firefox
- Chrome
- Safari (supported, but not recommended)

Appendix B

Troubleshooting

This appendix includes the following topics:

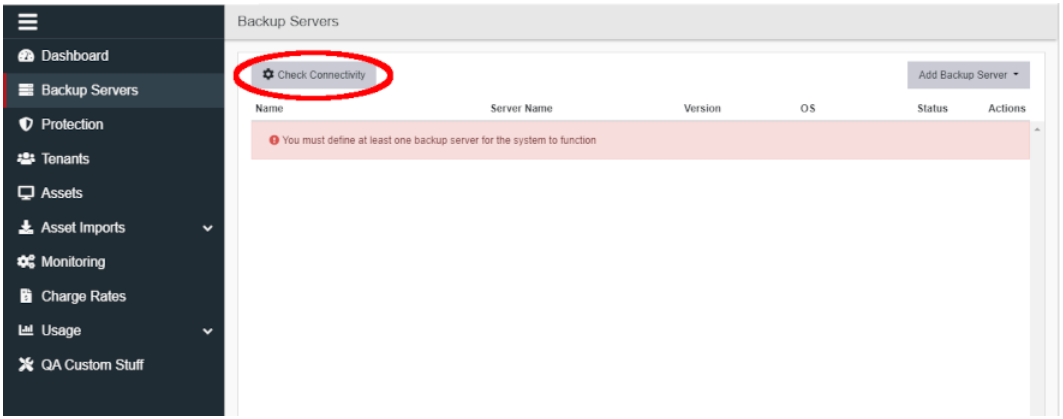
About PowerShell execution policy

The PowerShell execution policy determines if PowerShell can run scripts. The installer sets the execution policy to **Remote Signed** which allows scripts to run. Problems are encountered if this step of the installer fails or the execution policy is changed after install. This appendix describes diagnosing and solving execution policy issues.

Diagnosis

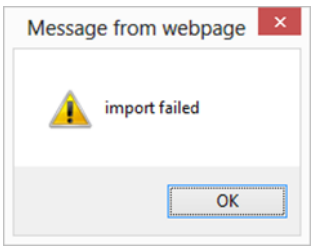
- Log on to the website
- Click the **Backup Servers** tab.
- Click the **Check Connectivity** icon

Figure B-1 Check connectivity



If you receive the error message shown, there may be an execution policy issue. If **Check Connectivity** does not generate an error, the execution policy is set correctly.

Figure B-2 Import failed pop-up box



To confirm there is an execution policy issue, navigate to the error log. Select `%ProgramData%\Veritas\NetBackupSelfService` and examine the errors. An example of an execution policy issue is shown.

```
"CreateRequest failed with error:
File C:\Temp\NetBackupAdapter\NetBackupAdapterServices\PowerShellScripts\
ValidationHook\Initial.p s1 cannot be loaded because running scripts is
disabled on this system. For more information, see about_Execution_Policies
at http://go.microsoft.com/fwlink/?LinkID=135170. File C:\Temp
\NetBackupAdapter\NetBackupAdapterServices\PowerShellScripts\ValidationHook\
Initial.p s1 cannot be loaded because running scripts is disabled on this
system. For more information, see about_Execution_Policies at
http://go.microsoft.com/fwlink/?LinkID=135170."
```

Solution

1. Log on to the web server
2. Open a PowerShell command prompt as administrator.
3. Type: `Get-ExecutionPolicy -List`

   The list of the current execution policies is shown
4. If the **Local Machine Scope** is not set to **Remote Signed**, type the command:

   ```
   Set-ExecutionPolicy -Scope LocalMachine -ExecutionPolicy
   RemoteSigned
   ```

Execution policy scope treats items higher up the list as higher priority, overriding those lower in the list. If the scope **MachinePolicy** is set to **Restricted**, then even though **LocalMachine** is set to **RemoteSigned** you are still unable to run scripts. This Stack Overflow post describes how to solve such problems.

http://stackoverflow.com/a/27755459

Recovering a lost application key

The application key is critical to the correct operation of the system. If the application key is lost it is not possible to recover the third-party passwords. Logging on is unaffected but passwords for adapters and integration settings must be re-entered.

In practice, there are two ways the application key can be lost:

- The web server fails.
- The website is uninstalled.

To mitigate the first issue, a backup of the web server should be kept.

An example of the second issue is the need to move the web server to a different physical computer. The application key should be copied from the configuration file on the old server and the new website should be installed using the application key. Test that the new server works correctly and verify that there is a valid backup of the server. Once the installation is complete, uninstall the website from the old server.

The application key, as well as the database connections strings, are stored in a configuration file named `appsettings.json` for the components.

Appendix C

Default HTTPS configuration

This appendix includes the following topics:

About the default HTTPS configuration

The installation configures the site to use HTTPS by default. The installation adds the self-signed certificate by default and creates an HTTPS binding.

Appendix D

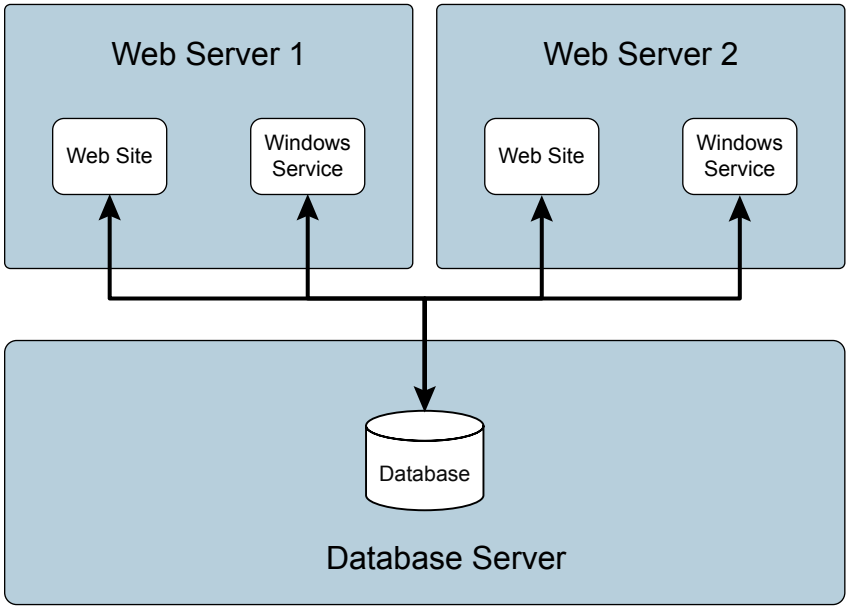
Load balanced installation

This appendix includes the following topics:

About load-balanced installation

A load-balanced installation has a single database server and database, but multiple instances of the web site and Windows service. This configuration provides load balancing and redundancy.

Figure D-1 Load-balanced installation example



You can run the installation on any web server or application server. The installation process copies all of the required files onto the server.

When you create a load-balanced installation, all configuration files on each web server should keep consistent. That means all servers need the same application key, same connection strings, and so on. To achieve this consistency, you must install NetBackup Self Service on each web server without regard for load balance. Then copy first server's configuration and paste it to all other servers with the NetBackup Self Service command tools. Use the steps that are shown for this configuration:

For a load-balanced installation

1. Run a new install on each web server. For the database name option, use the same name as the original server, but add a trailing number.
2. On the original server, open the command prompt window and run the command shown. This command prints the configuration as a string. Copy the string and paste it on all the other servers.

   ```
   install_directory\Cohesity\NetBackup Self Service 11.0\Install Files\nsscmd.exe -getconfig
   ```

3. On the other servers, open the command prompt window and run the command shown.

   ```
   install_directory\Cohesity\NetBackup Self Service 11.0\Install Files\nsscmd.exe -setconfig configuration string from the original web server
   ```

   This command pastes the configuration from the original web server to the new server. The new web server is now connected to same database as the original server.
4. Delete any unused databases the installation process created on the new web servers.

See “Recovering a lost application key” on page 27.

Appendix E

Customizing image upload

This appendix includes the following topics:

About Customizing Image Upload

Image upload is configured automatically. The uploaded images are stored in `C:\inetpub\Veritas\Images` by default. In a load-balanced installation, all of the web servers need to share any images that users may upload to the system. You must configure the uploaded images to reside on a common network storage area. This section describes how to change the storage location.

To change the storage location

1. Go to *`install_location`*`\Website\appsettings.json`
2. In the **PathForUploadedImages** text box enter the path where any uploaded images are stored. The path can either be a path on the local server, such as `C:\uploadedimages`, or a UNC share, such as `\\myshare\uploadedimages`.

To verify that the image upload works correctly

1. Log on to the website as Admin.
2. Go to **Admin > Settings > Notice**, then select the **New** icon, and then the **Upload** icon.
3. Browse to an image file and upload. If the image is successfully uploaded, it should appear in the image manager dialog box.

Appendix F

Reduced Database Permissions for Database Upgrade

This appendix includes the following topics:

Reduced Database Permissions for Database Upgrade

When you upgrade the database it is necessary to choose a database logon to perform the database upgrade. The simplest choice is to use a user that has the 'sysadmin' role.

If your database administrator (DBA) is unwilling to grant the sysadmin role to you, you can do a database upgrade with a reduced permission set. This appendix describes the upgrade process with reduced permissions.

The following SQL script creates a logon **UpgradeUser** which is suitable for upgrading the database.

To create a reduced permissions user for upgrade

1. Run this script in SQL Management Studio, to create a logon and user suitable for upgrading the database
2. When you run the configurator and select the database to upgrade, choose:
   - Authentication Mode: **Sql**
   - DB User: **UpgradeUser**

- DB Password: ***password***

3 Once install is complete you can disable or delete the **UpgradeUser**, since it is only used during the upgrade process.

```
-- Create a login for upgrading the database
use master
Create Login UpgradeUser WITH PASSWORD = 'password', Check_Policy = OFF
GO

-- Make a database user for the login
-- and give them db_owner role on the target database
USE NetBackupSelfService
CREATE USER UpgradeUser FOR LOGIN UpgradeUser
GO
ALTER ROLE db_owner ADD MEMBER UpgradeUser
GO

-- Allow ownership of database to be transferred to sa.
-- The sa login can be disabled as per good dba practice,
-- and everything will still work ok.
use master
GRANT IMPERSONATE ON LOGIN::sa to UpgradeUser
```