



DocAve® 6 Platform Backup and Restore for NetApp Systems

User Guide

Service Pack 8, Cumulative Update 2

Issued March 2017

Table of Contents

What's New in this Guide.....	4
About Platform Backup and Restore for NetApp Systems.....	5
Submitting Documentation Feedback to AvePoint.....	6
Before You Begin.....	7
AvePoint's Testing Policy and Environment Support.....	7
Configuration.....	8
Agents.....	8
Required Permissions.....	9
Health Analyzer.....	10
Getting Started.....	11
Launching Platform Backup and Restore for NetApp Systems.....	11
User Interface Overview.....	12
Navigating DocAve.....	12
Configuring Devices and Setting up Storage Policies.....	14
About the Verification and Index Policy.....	15
Configuring a Verification and Index Server Profile.....	15
Configuring a Verification and Index Server Group Profile.....	17
About Command with Operation.....	19
Configuring a Command Profile.....	20
Command Arguments Used to Pass Information to the Program or Script.....	22
About Migrator Tools.....	25
Migrate Database.....	25
Migrate Index.....	26
SharePoint Components Supported for Backup.....	28
SharePoint 2016.....	28
SharePoint 2013.....	29
SharePoint 2010.....	29
Using Plan Builder to Back Up Data.....	31
Using Wizard Mode to Create a Backup Plan.....	31

Using Form Mode to Create a Backup Plan	50
Backing up Databases First, and then Index Components	50
Pruning Log Backups from the Shared Folder.....	50
Running a Backup Job Immediately.....	51
Managing Plans.....	52
Configuring the Run Now Interface	52
Generating an Index	58
Checking the Generate Index Job Status.....	60
Configuring the Maximum Number of Snapshots Cloned for Index Generation.....	60
Configuring the Maximum Number of Database Indices to Generate in Parallel.....	61
Performing a Restore.....	62
Building a Restore Plan.....	63
Building a Restore Plan at Database Level.....	65
Building an In Place Platform Granular Restore Plan.....	68
Building an Out of Place Platform Granular Restore Plan	76
Restoring a Database to a Point in Time	85
Restoring from an Alternate Storage Location	85
Cloning Web Applications for Restore	86
Restoring Backed-Up Web Front-End Files.....	89
Restoring Backed-up BLOB Data.....	91
Restoring Backed-up Stub Database.....	92
Restoring Backed-Up Catalog Site Collection.....	92
Restoring Backed-up Database Master Key.....	94
Deselecting the Restore Granular Content Feature	95
Restore Details for Specific Farm Components.....	96
Backup and Restore FAST Search Server for SharePoint 2010 Farms	97
Backing Up the FAST Search Server	97
Restoring the FAST Search Server.....	99
Supported and Unsupported List	100
About Platform Backup and Restore for NetApp Systems for SQL Mirroring Database	102
About Platform Backup and Restore for NetApp Systems for Failover Database	103
Checking a Job Status.....	105

Performing Disaster Recovery	106
About Farm Repair.....	106
About Farm Clone.....	106
Full Farm Rebuild in Primary Site.....	119
Full Farm Recovery in SnapMirror Destination	128
Troubleshooting for Platform Backup and Restore for NetApp Systems	130
Cannot See the Farm in Migrate Index Wizard	130
Cannot Load Remote Backups	130
Appendix A: About Find Site Collection	131
Appendix B: About Advanced Search	132
Appendix C: About Local and Remote Backup Snapshot Retention	136
Scenario 1: Deleting Backup Snapshots via Storage Policy Retention Rule	138
Scenario 2: Deleting Job and Backup Snapshot via Job Monitor	141
Scenario 3: Deleting Remote Snapshots from SnapVault Destination with clustered environments..	143
Appendix D: Supported SharePoint Components.....	155
SharePoint 2010 Components Supported in Platform Backup and Restore for NetApp Systems.....	155
SharePoint 2013 Components Supported in Platform Backup and Restore for NetApp Systems.....	161
SharePoint 2016 Components Supported in Platform Backup and Restore for NetApp Systems.....	164
Platform Restore for NetApp Systems Support Table	166
Appendix E: SharePoint 2013 Social Features Supported in Platform Backup and Restore for NetApp Systems	195
Appendix F: SharePoint Object Security and Property	197
Appendix G: Using Hot Key Mode in Platform Backup and Restore for NetApp Systems.....	198
Backup Tab.....	198
Restore Tab.....	200
Clone Tab.....	201
Plan Manager Tab.....	201
Notices and Copyright Information	203

What's New in this Guide

- Added the Pruning Log Backups from the Shared Folder section.

About Platform Backup and Restore for NetApp Systems

Platform Backup and Restore for NetApp Systems protects your organization from disasters with a comprehensive toolset for backing up and restoring your entire SharePoint environment. Platform Backup and Restore for NetApp Systems backs up all content, customizations, solutions, and features, as well as back-end SQL databases, all configurations, index/job servers, front-end IIS settings, file system resources, and custom application databases. It allows for restore of an entire platform or individual SharePoint environment components.

It is important to fully understand the implications of using NetApp/IBM N seriesstorage volumes and their NetApp FAS LUNs during the backup and restore process. During the backup process, a snapshot backup is created for SharePoint databases and SharePoint index files; these snapshots are stored in a NetApp or an IBM N seriesstorage volume. The backup set can contain one or multiple NetApp Data ONTAP® NetApp FAS LUNs with multiple databases.

During backup, SnapManager for Microsoft SQL Server is used to perform database snapshot backups and SnapDrive is used to perform SharePoint index snapshot backups. The backup data of the other SharePoint components is sent to the configured storage policy and stored together with the backup job metadata and index.

***Note:** If SharePoint databases share a same NetApp FAS LUN with SQL Server system databases, only stream-based backup and restore can be utilized. DocAve 6 does not support this configuration. Always put SharePoint databases on NetApp FAS LUNs separate from the SQL Server system database NetApp FAS LUN.

***Note:** DocAve also supports VMDK disks. These disks interact with DocAve dentially to NetApp FAS LUNs, except that SnapVault integration is not supported on VMDK disks. In the following sections, all the areas that mention NetApp FAS LUNs will also apply to VMDK disks. For more information about VMDK disks, refer to the *SnapDrive Installation and Administration Guide*.

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. Click the following URL to access the [Submit Your Feedback](#) form on our website.

Before You Begin

Refer to the sections for system and farm requirements that must be in place prior to installing and using Platform Backup and Restore for NetApp Systems.

AvePoint's Testing Policy and Environment Support

Supported Software Environments

AvePoint is committed to testing against all major versions and service packs of SharePoint as well as the latest versions of Windows Server and SQL Server, as Microsoft announces support and compatibility.

***Note:** AvePoint does not recommend or support installing DocAve on client operating systems.

Supported Hardware

AvePoint is committed to maintaining a hardware agnostic platform to ensure that DocAve operates on common Windows file sharing and virtualization platforms. To ensure that DocAve is hardware agnostic, AvePoint tests hardware that is intended to support SharePoint and DocAve infrastructure, storage targets, and hardware-based backup and recovery solutions, as supported by AvePoint's partnerships. AvePoint directly integrates with the following platforms: any Net Share, FTP, Amazon S3, AT&T Synaptic, Box, Caringo Storage, Cleversafe, DELL DX Storage, Dropbox, EMC Atmos, EMC Centera, Google Drive, HDS Hitachi Content Platform, IBM Spectrum Scale Object, IBM Storwize Family, Microsoft Azure Storage, NetApp Data ONTAP, NFS, OneDrive, Rackspace Cloud Files, and TSM.

All other hardware platforms that support UNC addressable storage devices are supported.

***Note:** AvePoint has ended the test and development for Caringo Storage and DELL DX Storage in DocAve since DocAve 6 SP7 CU1, as the providers of these two platforms have stopped the platform maintenance.

***Note:** Due to changes in the IBM Tivoli Storage Manager API, DocAve 6 Service Pack 6 and later versions require that TSMClient version 7.1.2 is installed on the Control Service and Media Service servers.

***Note:** Most of the hardware partnerships referenced in this guide are intended to make use of advanced functionality (such as snapshot mirroring, BLOB snapshots, indexing, long-term storage, WORM storage, etc.), and are not indications that any changes to the product are required for basic support. In most cases, hardware can be supported with no change to the product.

Supported Backup and Recovery

DocAve supports BLOB backup storage according to the list of hardware platforms above. BLOB snapshot function, however, is currently only supported on OEM versions and NetApp hardware.

DocAve supports SQL content and Application database backups via the SharePoint Volume Shadow Copy Service (VSS) on all Windows and SQL server platforms listed above. DocAve also supports

snapshot-based SharePoint VSS on all hardware listed above where the hardware partner has certified support with Microsoft.

DocAve supports application and configuration server backups for all the supported software environments listed above. DocAve 6 SP5 or later supports VM backup via Hyper-V/VMWare for the following operating systems: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Microsoft Hyper-V Server 2012 R2.

Configuration

In order to use Platform Backup and Restore for NetApp Systems, the DocAve 6 platform must be installed and configured properly on your farm. Platform Backup and Restore for NetApp Systems will not function without DocAve 6 present on the farm.

Agents

DocAve Agents are responsible for running DocAve 6 jobs and interacting with the SharePoint object model. Platform Backup and Restore for NetApp Systems Agent must be installed on the following servers:

- A Platform Backup and Restore for NetApp Systems Agent must be installed on at least one of the Web front-end servers.
- The Search Service Application server where you want to back up the components of the specified Search Service Application
- The SharePoint Foundation (Help) Search server where you want to back up the components of the SharePoint Foundation (Help) Search
- Each SharePoint server where you want to back up the following object(s): IIS Settings, SharePoint Hive, Global Assembly Cache, Custom Features, SharePoint Site Definitions and Extra File System Folders
- Each FAST Search server where you want to back up the FAST Search server settings
- The server with Microsoft SQL Server installed
- Each node of Microsoft SQL Cluster (Each replica of the Microsoft SQL AlwaysOn Availability Groups if you are using SQL Server 2012)
- The source SQL Server and the failover SQL Server on the SQL mirroring database where you want to perform the Platform Backup and Restore for NetApp Systems job

For Farm Rebuild: Platform Backup and Restore for NetApp Systems Agent installed on each server in the SharePoint farm (including all of the SharePoint servers and SQL Servers)

For instructions on installing the DocAve Platform, DocAve Manager, and DocAve Agents, see the [DocAve 6 Installation Guide](#).

Required Permissions

To install and use Platform Backup and Restore for NetApp Systems properly, ensure that the Agent account has the following permissions.

Agent Account configured on the SharePoint Agents included in the Agent group:

1. Local System Permissions: User is a member of local **Administrator** group.
2. SharePoint Permissions: This permission must be manually configured prior to using DocAve 6 Platform Backup and Restore for NetApp Systems; it is not automatically configured.

- Member of the **Farm Administrators** group

***Note:** For SharePoint 2010, SharePoint 2013, and SharePoint 2016, the Platform Granular Restore requires the Agent account to have Full Control of all zones of the Web application.

When restoring the backed up personal site, the Agent account used to run the Platform Granular Restore job must also have the following permissions:

- Full control to the User Profile Service Application related to the Web application where the personal site resides
 - Security account of the application pool used by the Web application where the personal site resides
3. SQL Permissions: These permissions must be manually configured prior to using DocAve 6 Platform Backup and Restore for NetApp Systems; they are not automatically configured.
 - Database Role of **db_owner** in all of the databases related with SharePoint, including SharePoint configuration database, and Central Administration content database
 - Database Role of **db_owner** in all of the content databases, and service application databases included in the backup plan
 - Database Role of **db_owner** in the destination content databases
 - Server Role of **public** and **securityadmin** in SQL Server
 - Database permission of **View server state** to SQL Server
 - Database permission of **Alter Any Database** or **View Any Definition** to the SQL Server, or Server Role of **dbcreator** in SQL Server
 - Database permission of **Control server** to SQL Server (this permission is only required when you are using the **AlwaysOn Availability Groups** feature in **SQL Server 2012**, **SQL Server 2014**, or **SQL Server 2016**, and this permission must be configured on **all SQL instances** inside the AlwaysOn Availability Group)

Agent Account configured on the Index Server

- Member of the local **Administrators** group in the local system

Agent Account configured on the FAST Search Server

1. Local System Permissions
 - Member of the following local groups:
 - Administrators
 - **FASTSearchAdministrators** (this permission is only required for the Agent Account configured on the **FAST Search Administration** server)
2. SQL Server
 - Server Role of **public** in SQL Server (this permission is only required for the Agent Account configured on the **FAST Search Administration** server)

Agent Account configured on the SQL Server

1. Local System Permissions:
 - Member of the local administrator
2. SQL Server:
 - Database role of **db_owner** in master database.
 - Database role of **db_owner** in all of the databases included in the backup plan.
 - Server role of **processadmin** in SQL Server
 - Database permission of **View Server State** in SQL Server.
 - Database permission of **Control server** to SQL Server (this permission is only required when you are using the **AlwaysOn Availability Groups** feature in **SQL Server 2012**, **SQL Server 2014**, or **SQL Server 2016**, and this permission must be configured on **all SQL instances** inside the AlwaysOn Availability Group)

***Note:** The user who backed up and restores the certificate encrypted by TDE must have the server role of **securityadmin**. The user who restored the SQL logins must have the server role of **securityadmin**.

Refer to the [DocAve 6 Installation Guide](#) for information on the required Platform Backup and Restore for NetApp Systems permissions.

Health Analyzer

AvePoint recommends using Health Analyzer to verify that you meet the prerequisites necessary to use DocAve Platform Backup and Restore for NetApp Systems.

***Note:** Only users in the DocAve **Administrators** group can use Health Analyzer.

For more information about Health Analyzer, refer to [DocAve 6 Installation Guide](#).

Getting Started

Refer to the sections below for important information on getting started with Platform Backup and Restore for NetApp Systems.

Launching Platform Backup and Restore for NetApp Systems

To launch Platform Backup and Restore for NetApp Systems and access its functionality, follow the instructions below:

1. Log in to DocAve. If you are already in the software, click the **DocAve** tab.
2. From the **DocAve** tab, click **Data Protection** to view the backup modules.
3. Click **Platform Backup and Restore for NetApp Systems** to launch this module.

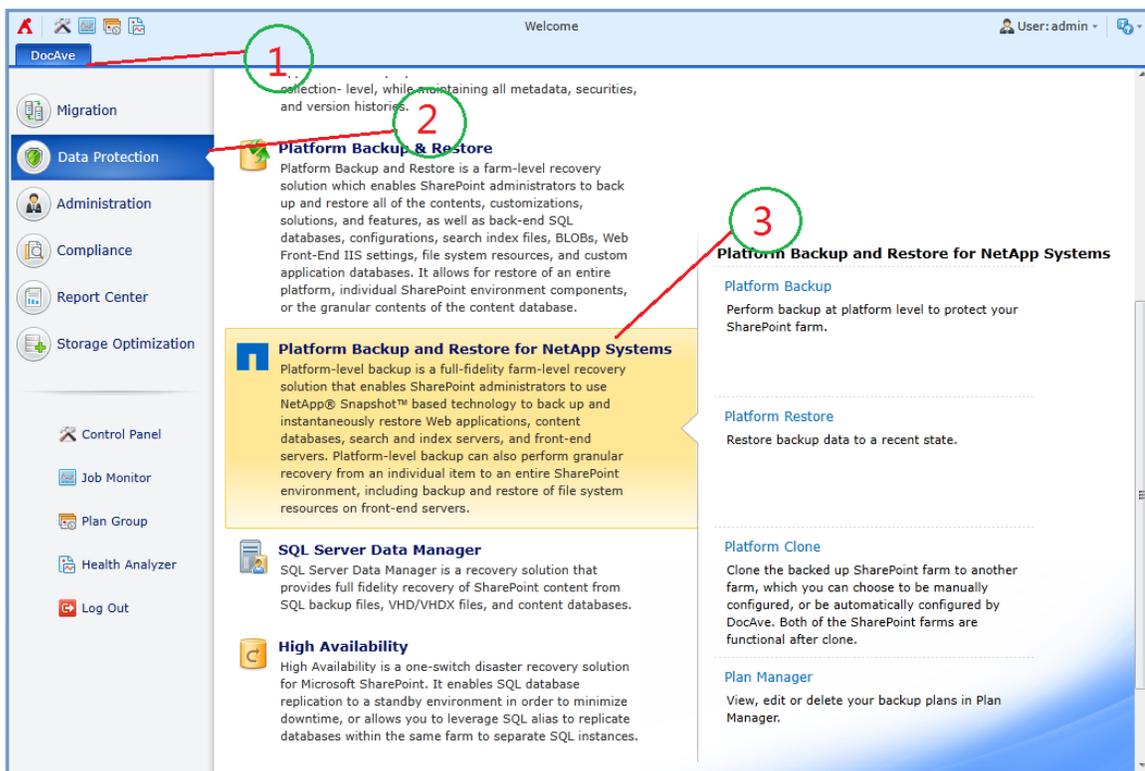


Figure 1: DocAve module launch window.

User Interface Overview

The Platform Backup and Restore for NetApp Systems user interface launches with the **Backup** tab active. This tab displays your farm environment and allows for quick access to a list of Platform Backup and Restore for NetApp Systems features.

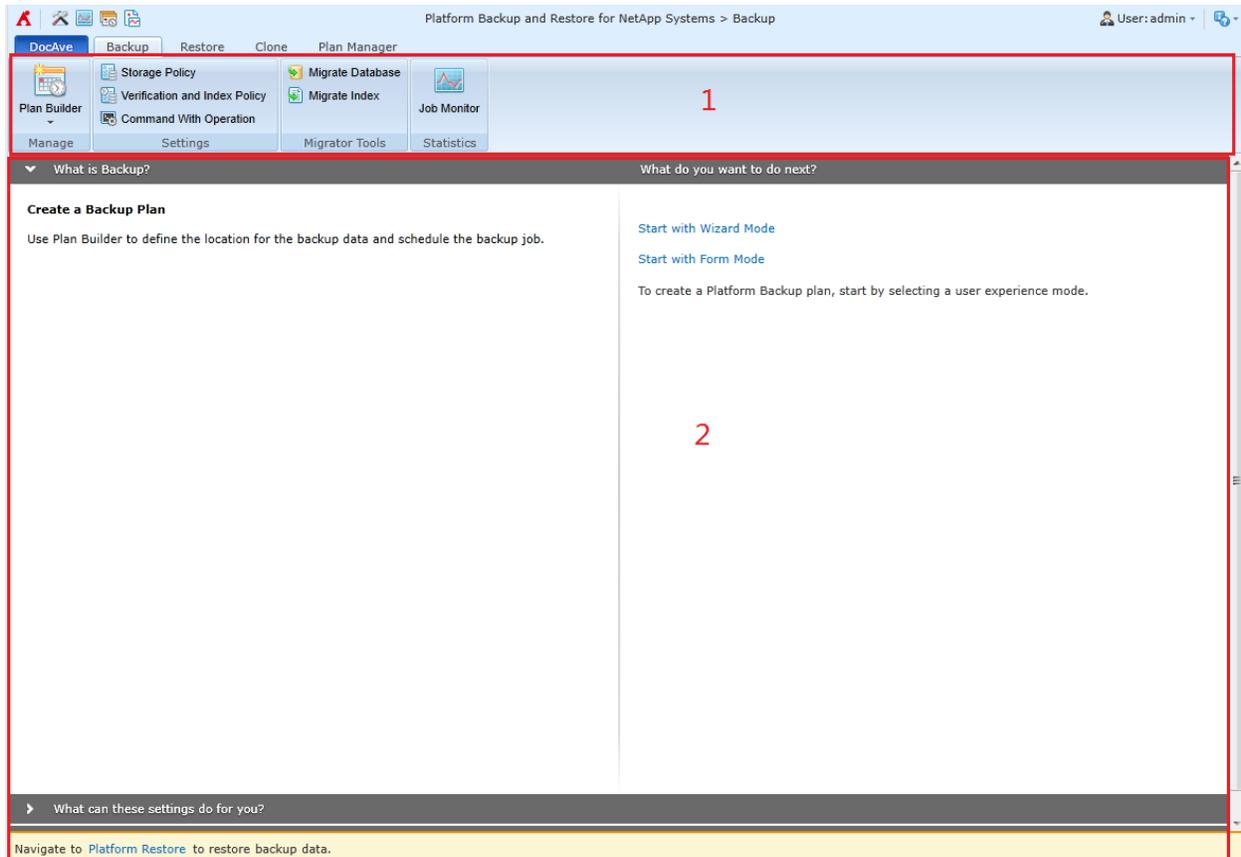


Figure 2: Platform Backup and Restore for NetApp Systems user interface.

1. The **ribbon** shows the available actions and wizards for the selected nodes. This content is dynamic; it will often change depending on what is selected on the SharePoint tree.
2. The **workspace** shows all form-based content that is used during the configuration of actions performed in DocAve products.

***Note:** Maintenance jobs are not counted into the **Dashboard** of the **Backup** tab or **Restore** tab.

Navigating DocAve

DocAve mimics the look and feel of many Windows products, making for an intuitive and familiar working environment. While there are many windows, pop-up displays, and messages within DocAve products, they share similar features and are navigated in the same ways.

Below is a sample window in DocAve. It features a familiar, dynamic ribbon, and a searchable, content list view.

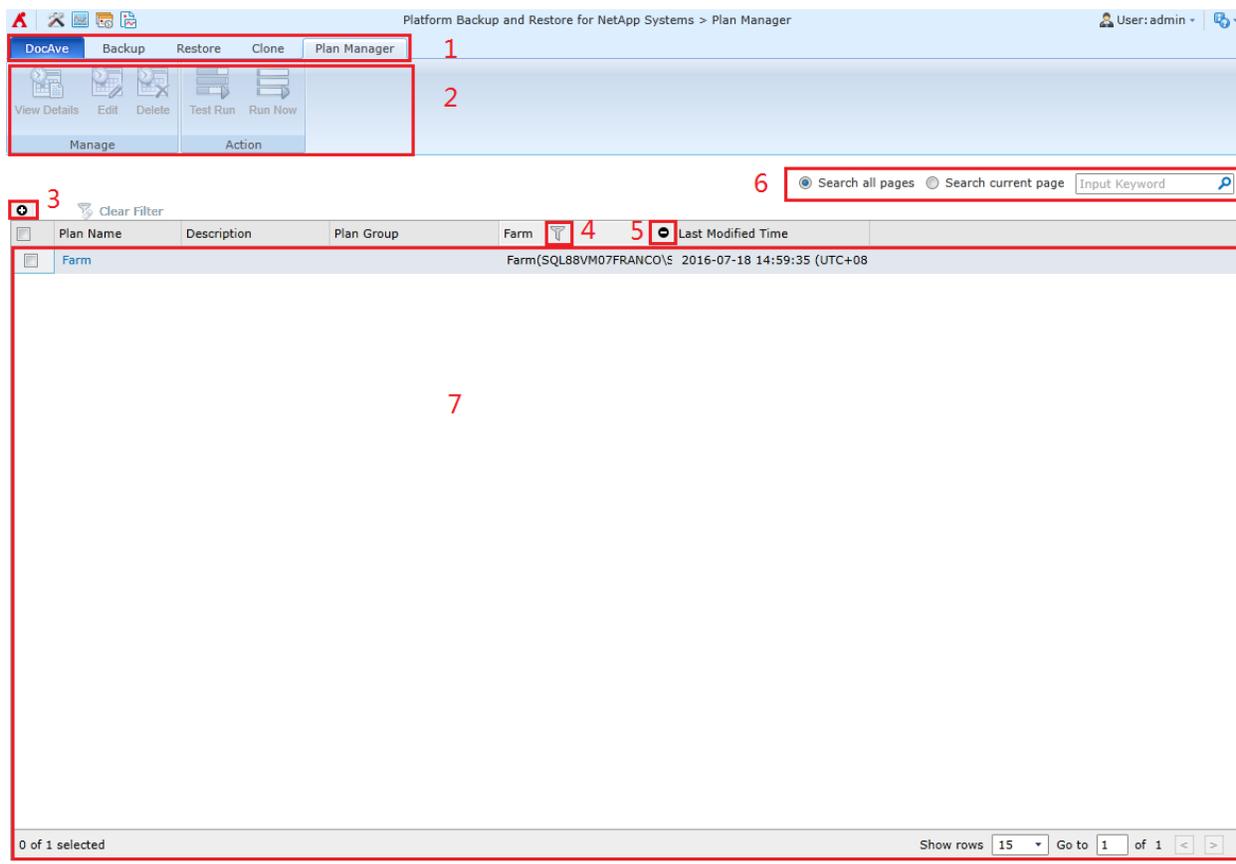


Figure 3: Navigating DocAve.

1. Ribbon Tabs— Allows users to navigate to the DocAve Welcome page and within the active module.
2. Ribbon Panes – Allows users to access the functionality of the active DocAve module.
3. Manage columns (⊕) – Allows users to manage which columns are displayed in the list. Click the manage columns (⊕) button, and then select the checkbox next to the column name in the drop-down list.
4. Filter the column (🔍) – Allows users to filter the information in the List View. Click the filter the column (🔍) button next to the column and then select the checkbox next to the column name.
5. Hide the column (⊖) – Allows users to hide the selected column.
6. Search – Allows users to search the List View pane for a keyword or phrase. You can select **Search all pages** or **Search current page** to define the search scope.
***Note:** The search function is not case-sensitive.
7. Management Pane – Displays the actionable content of the DocAve module.

Configuring Devices and Setting up Storage Policies

In order to perform a backup job using Platform Backup and Restore for NetApp Systems, it is necessary to first configure one or more physical/logical devices and then set up a storage policy.

DocAve has the ability to treat multiple NetApp FAS LUNs or NetApp FAS CIFS shares as a single logical unit when saving backup data. This is especially useful for very large backup plans, as many small drives can be combined. A storage policy must be defined before creating a backup plan. In addition, you can define the retention rules to manage your backup data in the storage policy.

Platform Backup and Restore for NetApp Systems can only write to a NetApp Data ONTAP device.

For instructions on defining devices and setting up storage policies, refer to the [DocAve 6 Control Panel Reference Guide](#). For details on retention, refer to [Appendix C: About Local and Remote Backup Snapshot Retention](#).

About the Verification and Index Policy

If you do not want to use the default SQL Server for backup verification and index generation, you can set up a verification and index policy to use one or more SQL Servers.

Configuring a Verification and Index Server Profile

To configure a verification and index server profile, complete the steps below:

1. Click **Verification and Index Policy** in the **Settings** group on the **Backup** or **Restore** tab. The **Verification and Index Policy Configuration** window appears.

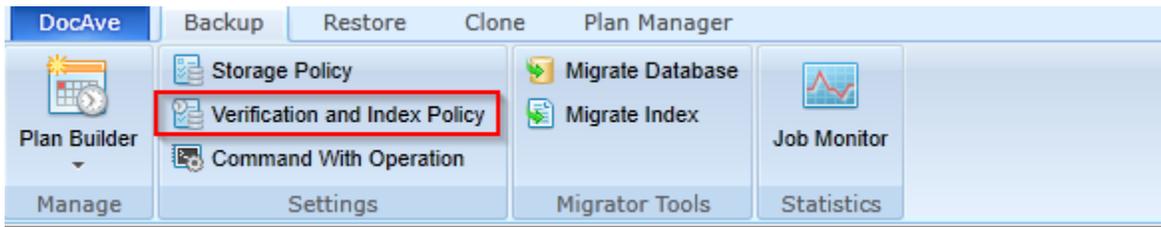


Figure 4: Selecting Verification and Index Policy from the Backup tab.

2. Click **Create** from the **Manage** group, and then select the **Verification and Index Server** from the drop-down list. The **Verification and Index Policy Configuration** page appears. Configure the following settings:

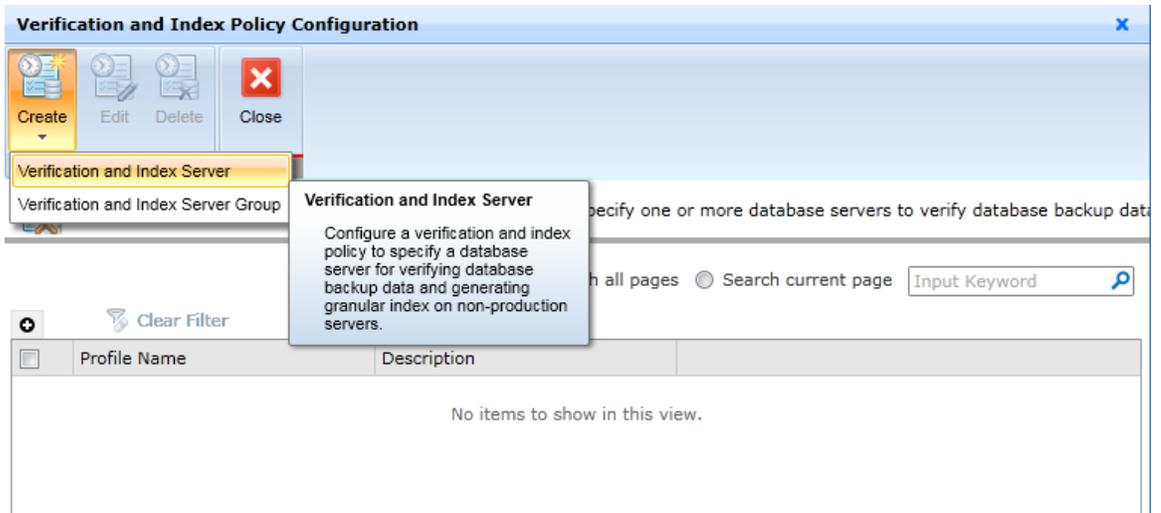


Figure 5: Selecting Verification and Index Server from the drop-down list.

Verification and Index Policy Configuration

OK Cancel Commit

Verification and Index Server Profile Name
Create a name for the verification and index server profile. A description is optional.

*Profile Name: [Text Box]
Description: [Text Box]

Server Name
Specify the server that you want to use to verify backups by entering the server name.
Example:
Server or Server\Instance

*Server name: [Text Box]

Database Access Credentials
Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials of the connecting database.

Database authentication (for accessing database within SharePoint)
 Windows authentication (recommended)
 SQL authentication

Account: [Text Box]
Password: [Text Box]

Create a New Verification and Index Server Profile OK Cancel

Figure 6: Configuring the Verification and Index Server profile.

- a. **Verification and Index Server Profile Name** – Enter a **Name** and optional **Description** for the verification and indexserver profile.
- b. **Server Name** – Enter a SQL Server name or instance to be used as the server for verification and index generation in the **Server Name** field. The format is **Server** or **Server\Instance**.

*Note: **SnapManager for SQL Server** must be installed on the verification server.
- c. **Database Access Credentials** – Select the authentication method used to create the database.
 - **Windows authentication (recommended)** (the default option) – Use this method to confirm the user identity using Windows.
 - **SQL authentication** – SQL Server confirms the user identity according to the selected Managed Account. The designated account must be added to the **sysadmin** role in SQL Server.
- d. **Allow all Farms to Use this Server** – By default, all farms are allowed to use the specified server for the backup verification and indexgeneration. To choose the farms

where you want to use this verification and index server, click the **Farm** drop-down list and select the specified farms.

3. Click **OK** to save the configured verification and index server profile. Otherwise, click **Cancel**.

Configuring a Verification and Index Server Group Profile

Verification and index server group enables you to use more than one SQL Server for database backup verification and index generation. To configure a verification and index server group, complete the steps below:

1. Click **Verification and Index Policy** in the **Settings** group on the **Backup** or **Restore** tab. The **Verification and Index Policy Configuration** window appears.
2. Click **Create** from the **Manage** group, and then select the **Verification and Index Server Group** from the drop-down list. The **Verification and Index Policy Configuration** page appears. Configure the following settings:

Verification and Index Policy Configuration

OK Cancel

Commit

Verification and Index Policy Group Name
Create a name for the verification and index server group. A description is optional.

*Profile Name:
VI Server Group Profile for Farm27

Description:

Farm
Select a farm to load and create verification and index servers.

* Select a farm:
Farm(VM6710SQL27:SHAREPOI)

Database Server Mappings
Database Server Mappings

<input checked="" type="checkbox"/>	* SQL Server	* Verification and Index Server Profile	Assign Mount Point
<input checked="" type="checkbox"/>	VM6710SQL27	ddd	Enter Mount Point Path

Create a New Verification and Index Server Group

OK Cancel

Figure 7: Configuring the Verification and Index Server Group profile.

- a. **Verification and Index Server Group Profile Name** – Enter a **Name** and optional **Description** for the verification and index server group profile.

- b. **Farm** – Select a farm from the drop-down list to load and create the verification and index servers.
 - c. **Database Server Mappings** – Configure the mappings for the SQL Servers and verification and index servers. The verification and index server specified for the corresponding SQL Server will mount the temporary database to the specified mount point directory to verify the backed up database and generate the granular index. Complete the steps below:
 - i. In the **Database Server Mappings** field, click **Add** on the left-corner to add a mapping into the table.
 - ii. Select a SQL Server from the **SQL Server** drop-down list, and then select a verification and index server profile from the **Verification and Index Server Profile** drop-down list. Enter the mount point directory for mounting the temporary database on the specified verification and index server. You can perform the following actions on the configured mappings:
 - **Delete** – Delete the selected mappings.
 - **Clear Selection** – Clear all of the selections.
3. Click **OK** to save the configured verification and index server group profile. Otherwise, click **Cancel**.

About Command with Operation

For a DocAve 6 database backup, restore, or verification operation, you have the option to automatically run a command before the operation starts or after the operation completes. Enabling the **Run command with operation** option prompts you to select a command profile, which must be configured before the backup, restore, or verification operation can begin.

A command profile contains the following information:

- The type of the command, which is either a **Pre-Operation command** or **Post-Operation command**
- The host system from which the command is to be run
- The full path of the command that you want DocAve 6 to run before or after the database backup, restore, or verification operation
- Any parameters that are to be passed to the command
- Because the command (your own program or script) is invoked from within the context of a specific database backup, restore, or verification, you can pass the command information about the components of that operation. In your script, any occurrence of the text string %1 corresponds to the first parameter passed; the text string %2 corresponds to the second parameter, and so on.

After you have completed configuring the command and parameters, the database backup, restore, or verification operation can be started.

***Note:** The **Post-Operation** command or script will run only after a successful backup, restore, or verification. If the backup or restore is not completed successfully, or if the verification fails, then the **Post-Operation** command or script is not run.

Configuring a Command Profile

To configure a command profile:

1. Click **Command With Operation** in the **Settings** group on the **Backup** tab. The **Command With Operation** window appears.
2. Click **Create** from the **Manage** group. The **Create a New Command Profile** window appears.

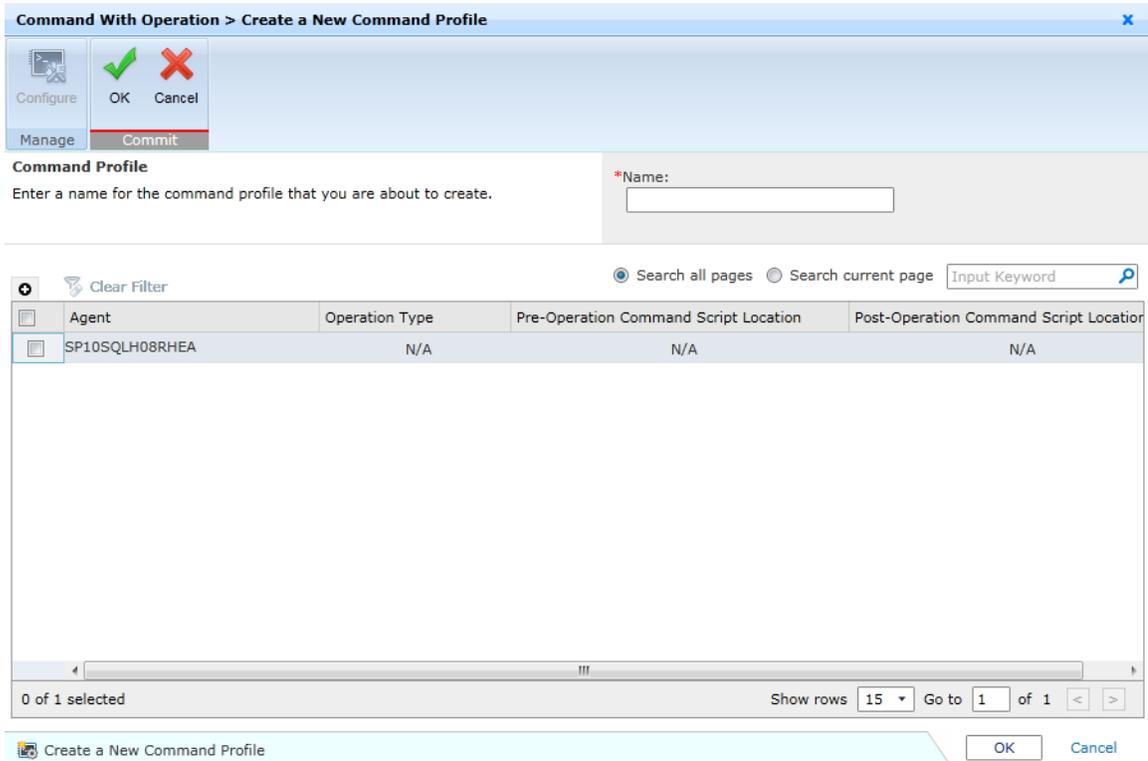


Figure 8: Create a New Command Profile window.

3. Enter a **Name** for the command profile and select one or more Agents where you want to **Run command with operation**. Then, click the **Configure** button on the ribbon. You can also click the **Configure** link following the Agent name in the **Agent** column to configure the detailed settings for only that Agent.
4. Select the **Operation Type** for the command profile. The operation type specifies when this command profile can be loaded.
5. If desired, configure the **Pre-Operation Command** settings.
 - a. **Run Pre-command or Script** – Select the **Run pre-command or script before the SnapManager Operation starts** checkbox to enable the pre-operation function.
 - b. **Pre-command Errors** – If the **Treat pre-command errors as fatal by stopping the remaining SnapManager operations** option is selected, the backup, restore, or verification operation will not run if the pre-command does not complete successfully.

- c. **Specify a Computer** – Specify the hostname or IP address of one computer where you want to run the command (your own program or script) in the **Specify a computer to run command** textbox.
 - d. **Specify a Program or Script** – Specify the full path to the command in the Specify a program or script you want to run textbox.
 - e. **SnapManager Variables and Command Arguments** – Select the sequence of SnapManager variables that you want to pass to the command in the **SnapManager variables** field, and then click **Add to Command Arguments** to add the selected variables to the **Command arguments** field.
6. If desired, configure the **Post-Operation Command** settings.
 - a. **Run Post-command or Script** – Select the **Run post-command or script after the SnapManager Operation completes** checkbox to enable post-operation function.
 - b. **Post-command Errors** – If the **Treat post-command errors as fatal by stopping the remaining SnapManager operations** option is selected, the backup, restore, or verification operation will be considered failed if the post-command does not complete successfully.
 - c. **Specify a Computer** – Specify the hostname or IP address of one computer where you want to run the command (your own program or script) in the **Specify a computer to run command** textbox.
 - d. **Specify a Program or Script** – Specify the full path to the command in the Specify a program or script you want to run textbox.
 - e. **SnapManager Variables and Command Arguments** – Select the sequence of SnapManager variables that you want to pass to the command in the **SnapManager variables** field, and then click **Add to Command Arguments** to add the selected variables to the **Command arguments** field.
7. Click **Save** to save the configuration; you will be redirected to the **Create a New Command Profile** page.
8. Click **Save** to save the configured command profile; you will be redirected to the **Command With Operation** page.
9. In the **Command With Operation** page, you can edit the created command profiles or delete the command profiles that are no longer useful.

Command Arguments Used to Pass Information to the Program or Script

The **Run command with operation** feature supports the following variables, which can pass operation-specific information to your program or script.

Variable	Description
\$SqlSnapshot	<p>Expands to the name of a SQL Server database Snapshot copy. This argument is used for backup and verification operations.</p> <p>Examples: <code>sqlsnap winsrvr201-31-2005_15.03.09</code> <code>sqlsnap_winsrvr_recent</code></p> <p>*Note: The number of database Snapshot copies in a SnapManager backup set depends on the number of volumes used to store the databases included in the backup.</p> <p>For a restore operation, this argument specifies the name of the Snapshot copy to be restored.</p> <p>Example: <code>sqlsnap winsrvr201-31-2005_15.03.09</code> <code>sqlsnap winsrvr2 recent</code></p>
\$InfoSnapshot	<p>Expands to the name of a SnapInfo directory Snapshot copy.</p> <p>Examples: <code>sqlinfo winsrvr201-31-2005_15.03.09</code> <code>sqlinfo winsrvr2 recent</code></p>
\$SnapInfoName	<p>Expands to the name of the SnapInfo directory.</p> <p>Examples: <code>WINSRV2recent</code> <code>WINSRV2_11-23-2004_16.21.07 Daily</code></p> <p>*Note: If you use this variable, you must also provide the correct path to the directory.</p>
\$SnapInfoPath	<p>Expands to the name of the SnapInfo subdirectory. This argument is used in backup and verification operations.</p>

Variable	Description
	<p>Example: I:\SMSQL_SnapInfo\SQL WINSRVR2\DB North wind</p> <p>For restore operation, this argument specifies the path to the Snapshot copy information metadata that is being used for the database restore.</p> <p>Example: U:\SMSQL_SnapInfo\VDISK E\FG\05-14-2010_15.33.41\SnapInfo 05-14-2010_15.33.41.sml</p>
\$LogBackupFile	<p>Expands to the full path name of the transaction log backup file.</p> <p>Example: I:\SMSQL_SnapInfo\SQL WINSRVR2\DB North wind\LogBackup\ 11-01-2004_13.34.59 Northwind.TRB</p>
\$Database	<p>Specifies the logical name of the database processes.</p> <p>*Note: To prevent PowerShell from interpreting the value of this parameter, be sure to enclose the entire parameter value with single quotes. For example, PreCmdArg '\$Database \$ServerInstance'</p> <p>Example: DatabaseAccounting</p> <p>If you want to have more than one database expanded, repeat the parameter as many times as you want.</p> <p>Example: AccountingDB1 AcmeServer1/SqlInst1 FinanceDB2 AcmeServer1/SqlInst2</p>
\$OperationStatus	<p>Provides the status of the SMSQL operation.</p> <p>Example: 5234</p>

Variable	Description
\$PreCommandStatus	<p>Provides the pre-command status to the post-command if the post-command is executed based on the status of the earlier pre-command.</p> <p>Example: 5234</p>

***Note:** Several parameters like the **\$SnapInfoPath** and **\$LogBackupFile** variables are automatically enclosed within double quotes so that the actual path name can contain spaces without affecting the script invocation on the Windows command line. If you do not want the double quotes to appear in your command line, remove them from the **Command arguments** field.

The following are some helpful notes on the **Command with Operation** function:

- The machine specified in the **Specify a computer to run command** textbox must have SMSQL installed to run the command.
- If SMSQL 5.2P1 or higher is on a machine running a database backup, restore, or verification job, both the pre-command and the post-command are executed.

About Migrator Tools

SharePoint databases/indexes must be located on storage systems running NetApp Data ONTAP (NetApp FAS LUNs and NetApp FAS CIFS shares) for them to be backed up by DocAve. If SharePoint databases/indexes are not located on storage systems running NetApp Data ONTAP, then they must be migrated to these storage systems.

Use SnapManager for Microsoft SQL Server (SMSQL) to migrate SQL Server databases from a local disk to storage systems running NetApp Data ONTAP, as well as separate the database files and log files onto separate NetApp FAS LUNs.

The DocAve's **Migrate Index** tool can be used to facilitate the index migration process. You can find the Migrate Index tool by navigating to **DocAve > Data Protection > Platform Backup and Restore for NetApp Systems**.

The DocAve Migrate Index tool provides a way of moving SharePoint indexes to NetApp FAS LUNs. Clicking the **Migrate Index** button on the ribbon will lead you to the Migrate Index Wizard.

Migrate Database

The Migrate Database tool migrates SharePoint databases to NetApp Data ONTAP storage systems (NetApp FAS LUNs). Such databases include the SharePoint Configuration database, service application database, or Web application content database. With this feature you can also move a database from local disk to an SMB share.

***Note:** The Migrate Database tool does not support the migration of the databases in the AlwaysOn Availability Group and the SQL Mirroring Databases.

***Note:** SharePoint services on all servers in the farm will be automatically stopped during the migration process. Services are restarted after completion of the migration. For servers in the farm that do not have DocAve Agents installed, you must stop the services before you click **Start** and then restart the services manually after the migration job is finished.

To access the **Migrate Database** tool, click **Migrate Database** in the **Migrator Tools** group on the **Backup** tab. To use the **Migrate Database** tool, complete the steps below:

1. **Migrate Database** – In the **Farm Selection** field, select the farm that contains the SharePoint databases you want to migrate. All of the DocAve Agents installed on the SQL Servers of the specified farm are loaded in the **Agent Selection** field. Choose one Agent from the **Agent selection** drop-down list to migrate the databases on the specified Agent server.
2. Click **Next**. The **Database Association** page appears.
3. **Database Association** – Select the checkbox of the database or the database file that you want to migrate. The **To (Available Disk)** field becomes enabled. Select a NetApp FAS LUN from the **To**

2. **Migrate Index** – In the **Farm Selection** field, select the farm that contains the SharePoint indexes you want to migrate. All DocAve Agents installed on the SharePoint Foundation Help Search index server and Search Service Application index server are loaded in the **Agent Selection** field. Choose one Agent from the **Agent selection** drop-down list to migrate the indexes on the specified Agent server.

***Note:** SharePoint Foundation farms will not be loaded in the **Farm Selection** drop-down list, as the Migrate Index tool does not support migrating SharePoint Foundation farm index files.

3. Click **Next**. The **Index Association** page appears.
4. **Index Association** – Select the checkbox of the index you want to migrate. The **To (Available Disk)** field becomes enabled. Select a NetApp FAS LUN from the **To (Available Disk)** drop-down list. The selected index will be migrated from the location displayed in **From (Location)** to the NetApp FAS LUN specified in the **To (Available Disk)** field.
5. Click **Next**. The **Notification** page appears.
6. **Notification** – To inform specified users of the index migration job, configure the **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list, or create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.
7. After you are satisfied with the configuration, click **Start** to start the index migration job.

***Note:** To create a new content database, create a new empty SQL database using the **LATIN1_General_CI_AS_KS_WS** collation and move it onto the storage system that is running NetApp Data ONTAP. Next, in Microsoft SharePoint, choose to create a new content database and point it to the pre-created databases. For more information regarding this option, consult Microsoft SharePoint documentation. This is the recommended approach when storage admins and SharePoint admins are different people/teams. For more information, refer to Microsoft article [Deploy by using DBA-created databases \(SharePoint Foundation 2010\)](#).

SharePoint Components Supported for Backup

See below for SharePoint 2016/2013/2010 components supported for backup.

***Note:** Some components have multiple related sub-components that must be backed-up together. For example, the service application must be backed up with its connection type in order to perform a successful restore of these components.

***Note:** Platform Backup and Restore for NetApp Systems does not include system backups such as AD backup and System State backup. Therefore, the SharePoint customizations' external dependencies are not backed up. Typically, such customizations are deployed through an installer or configured manually and require the use of binaries, registry entries and so on.

SharePoint 2016

DocAve Platform Backup and Restore for NetApp Systems supports backup for the following SharePoint 2016 components:

- All SharePoint databases – The configuration database, SharePoint Central Administration content database, content databases, State Service database, Shared Service Application Database, Session State Service database, and Usage and Health Service database are supported. These databases are backed up by the SQL Agent.
***Note:** Only the databases in the state of **ONLINE** are supported for backup.
- Database master key – When backing up the database, only the database master key encrypted by the service master key will be backed up with the database.
- SharePoint search index – This includes the Server Search index. The search index files are backed up on DocAve Agent.
- SharePoint components and settings – This includes Web applications, InfoPath Forms Services, License to Feature Mappings, State Service, Subscription Service, Global Search Settings, Workflow Service, Microsoft SharePoint Server Diagnostics Service, Microsoft SharePoint Foundation Diagnostics Service, Shared Service Applications, Shared Service Proxies, Usage and Health Service, and Global Site Template.
- SharePoint solutions – This includes any SharePoint customizations deployed to SharePoint in the form of solutions. These solutions and their deployment statuses are backed up.
- SharePoint front-end resources – This includes the IIS settings (both metadata and files), SharePoint site definitions, SharePoint hive files, Global Assembly Cache files, custom features, and extra file system folders.

SharePoint 2013

DocAve Platform Backup and Restore for NetApp Systems supports backup of the following SharePoint 2013 components:

- All SharePoint databases – The configuration database, SharePoint Central Administration content database, content databases, State Service database, Application Registry Service Database, Shared Service Application Database, Session State Service database, Usage and Health Service database, and Help Search database can be fully backed up. These databases are backed up by the SQL Agent.
***Note:** Only the databases in the state of **ONLINE** are supported for backup.
- Database master key – When backing up the database, only the database master key encrypted by the service master key will be backed up with the database.
- SharePoint search index – This includes the Server Search index. The search index files are backed up on DocAve Agent.
- SharePoint components and settings – This includes Web applications, InfoPath Forms Services, State Service, Microsoft SharePoint Foundation Sandboxed Code Service, Microsoft SharePoint Server Diagnostics Service, Microsoft SharePoint Foundation Diagnostics Service, Shared Service Applications, Shared Service Proxies, Global Search Settings, and Managed Metadata Service.
- SharePoint solutions – This includes any SharePoint customizations deployed to SharePoint in the form of solutions. These solutions and their deployment statuses are backed up.
- Nintex databases – This includes Nintex workflow 2013 configuration database, content database, and solutions.
- NewsGator – This includes the Enrich Service, News Stream Service, Social Platform Service, and Video Stream Service (including corresponding databases), proxies, and solutions.
***Note:** Social Sites (NewsGator) 4.0 and Social Sites (NewsGator) 5.0 for SharePoint 2013 are supported in DocAve 6 SP8 or later.
- SharePoint front-end resources – This includes the IIS settings (both metadata and files), SharePoint site definitions, SharePoint hive files, Global Assembly Cache files, custom features, and extra file system folders.

SharePoint 2010

DocAve 6 Platform Backup and Restore for NetApp Systems supports backup of the following SharePoint 2010 components:

- All SharePoint databases – The configuration database, Central Administration content database, content databases, State Service database, Application Registry Service

Database, Shared Service Application Database, Session State Service database, Usage and Health Service database, and Help Search database can be fully backed up. These databases are backed up by the SQL Agent.

***Note:** Only the databases in the state of **ONLINE** are supported for backup.

- Database master key – When backing up the database, only the database master key encrypted by the service master key will be backed up with the database.
- SharePoint search index – This includes the Server Search index. The search index files are backed up on DocAve 6 Agent.
- SharePoint components and settings – This includes Web applications, InfoPath Forms Services, State Service, Microsoft SharePoint Foundation Sandboxed Code Service, Microsoft SharePoint Server Diagnostics Service, Microsoft SharePoint Foundation Diagnostics Service, Application Registry Service, Shared Service Applications, Shared Service Proxies, Global Search Settings, and Managed Metadata Service.
- SharePoint solutions – This includes any SharePoint customizations deployed to SharePoint in the form of solutions. These solutions and their deployment statuses are backed up.
- Nintex databases – This includes Nintex workflow 2010 configuration database, content database, and solutions.
- NewsGator – This includes NewsGator Social Platform Services (including corresponding databases), NewsGator Social Platform Services Proxy, and solutions.

***Note:** Social Sites (NewsGator) 1.2 and 2.5 for SharePoint 2010 are supported by DocAve 6.

- KnowledgeLake – This includes KnowledgeLake Imaging Data, KnowledgeLake Service Application, KnowledgeLake Proxy, and solutions.
- SharePoint front-end resources – This includes the IIS settings (both metadata and files), SharePoint site definitions, SharePoint hive files, Global Assembly Cache files, custom features, and extra file system folders.
- FASTSearch Server Farms – FASTSearch Server Farms backup is supported.

Using Plan Builder to Back Up Data

Use the **Plan Builder** to schedule a backup job.

***Note:** By default, DocAve backs up databases and index components in parallel. To modify this behavior, you must manually edit a configuration file. For details, refer to [Backing up Databases First, and then Index Components](#).

To use Plan Builder:

1. Click **Plan Builder** from the **Backup** tab.
2. From the drop-down menu, select [Wizard Mode](#) for step-by-step guidance during configuration, or select [Form Mode](#) (recommended for advanced users only) to set up a plan quickly.

See the section below applicable to your choice.

Using Wizard Mode to Create a Backup Plan

Wizard Mode provides you with step-by-step guidance on how to configure a new plan. Follow the instructions below to configure a plan using Wizard Mode. Note that a red * in the user interface indicates a mandatory field or step.

1. Enter a **Plan Name** and optional **Description**, if desired. Then choose whether to **Create a new plan** or **Copy saved plan settings from template** to start from a previously saved plan template.
2. In the **Scope Selection** field, select a farm from the **Farm** drop-down list, and then select the Agent group that will execute the backup job.

***Note:** If your environment has a DMZ, make sure all of the Agents in the Agent group are in the same LAN as DocAve Manager, and can communicate with SQL Server and Media Server.

3. In the **Backup Components Selection** field, choose the scope of data for backup.
 - **Back up selected components** – In the **Data Selection** step, you can expand the farm tree and select any specific components in the farm you want to back up.
 - **Back up the whole farm** – All of the farm components will be automatically selected for backup in the farm tree of the **Data Selection** step; however, you can also deselect the components you do not want to include in this plan, except for the SharePoint configuration database and administration database.

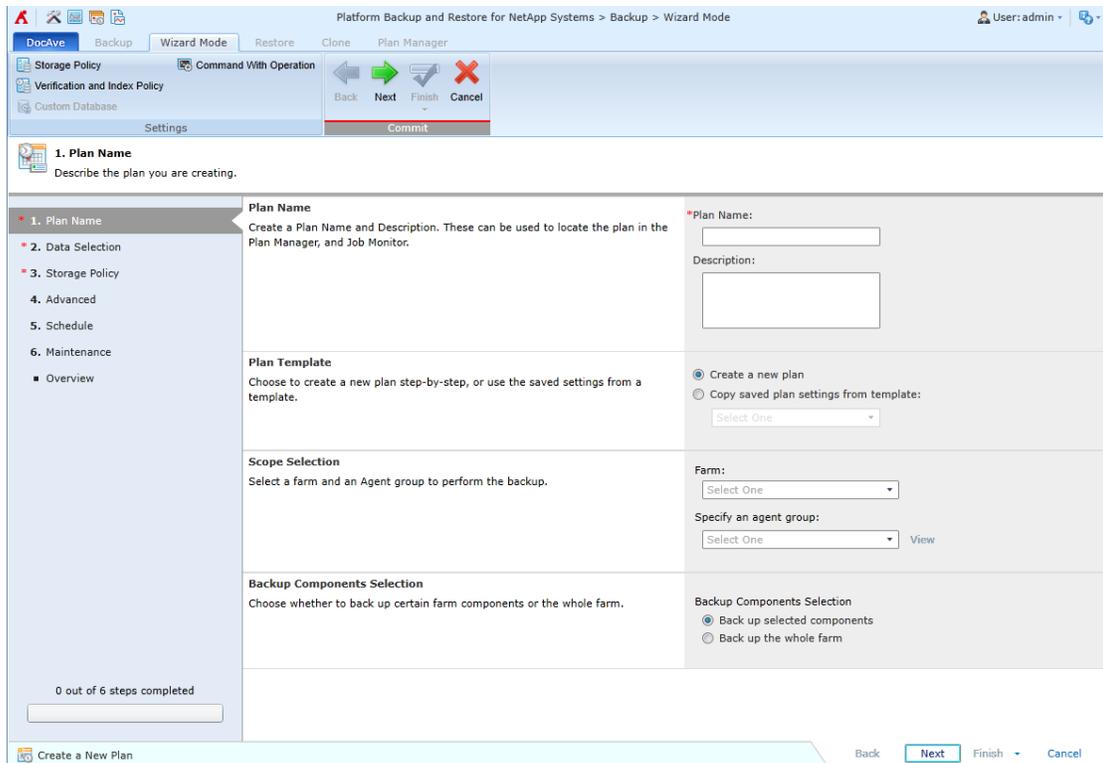


Figure 10: Creating a plan in Wizard Mode.

4. In the **Data Selection** step, select or deselect the farm components to include or exclude from this backup plan.

To select content to back up, complete the following steps:

- a. Click the farm node to expand the tree and display all the SharePoint components (databases, services, solutions, index components, etc.) that can be backed up.

***Note:** If the databases are in AlwaysOn Availability Group, the AlwaysOn Availability Group Listener name will be displayed next to the database name.

***Note:** You cannot select nodes on both a SharePoint 2010 tree and SharePoint 2013 tree simultaneously.

- By default, the **Verify Storage Layout** option is selected, which means that DocAve tries to obtain information for all databases and indexes regarding storage from SnapManager for Microsoft SQL Server and SnapDrive, respectively. This process may take some time to complete, depending upon the number of databases on the SQL Servers.
- When the **Verify Storage Layout** option is not selected, DocAve will retrieve only the farm tree structure from SharePoint, which means that the farm tree loads faster. However, because the storage layout is unknown in this case, you must ensure that all components are correctly configured on the NetApp FAS LUN.

- If the **Verify Storage Layout** option is selected, certain icons are displayed to indicate the storage status, as shown in the following table.

Type	Database	Index
In NetApp FAS LUN or on SMB 3 Share with SnapMirror and SnapVault enabled		
In NetApp FAS LUN or on SMB 3 Share with SnapMirror enabled		
In NetApp FAS LUN or on SMB 3 Share with SnapVault enabled		
In NetApp FAS LUN or on SMB 3 Share		
Invalid. No database or index in NetApp FAS LUN, no database on SMB 3 Share, or database is on snapshot copied NetApp FAS LUN or NetApp FAS CIFS of cloned volumes.		
Browse the tree without selecting the Verify Storage Layout option, or unknown error occurs while browsing		
No Agent is installed, the database cannot be backed up		

***Note:** If any newly created SharePoint objects are not displayed in the tree, right-click the root **Farm (Farm name)** node and click **Refresh** to refresh the tree.

- If desired, select the **Include New** node to include any newly created SharePoint objects (child nodes) in the Platform Backup for NetApp Systems plan. By default, the **Include New** node is selected for each Web application. The nodes that support the **Include New** function are:
 - Farm
 - Solutions
 - Microsoft SharePoint Foundation Web Application and the Web Application nodes below it
 - Shared Service Applications
 - Shared Service Proxies
 - InfoPath Form Services
 - Data Connections
 - Form Templates

- Exempt User Agents
- c. In the screenshot below, the following SharePoint objects will be backed up by the Platform Backup for NetApp Systems plan:
 - Newly created Web applications under the **Microsoft SharePoint Foundation Web Application** node (because **Include New** is selected)
 - Any existing or newly added content databases of the selected/newly created Web applications under the **Microsoft SharePoint Foundation Web Application** node

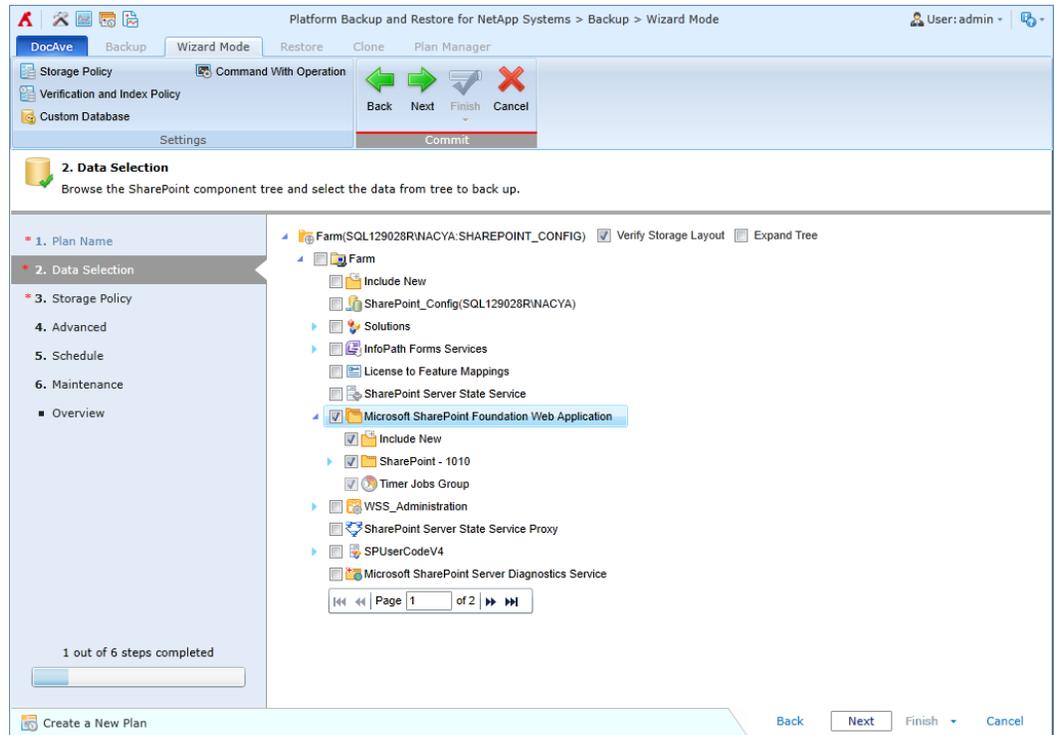


Figure 11: The objects for backup.

In addition, you can use the **Custom Database** feature to manually add custom databases that are not listed to the SharePoint component tree. Such databases include solution databases, third-party software databases, and so on.

It is required that custom databases be on NetApp FAS LUNs or SMB 3 Share in order for them to function properly with DocAve. A custom database can be on a SQL Server that is separate from the one that the farm uses, as long as the servers have DocAve Agents installed on them and the database is on a NetApp FAS LUN or a SMB 3 Share.

Complete the steps below to add a custom database to a backup plan.

- a. In the **Data Selection** step, click **Custom Database** on the ribbon. The **Custom Database** window appears.

- b. In the **Custom Database** window, click the **Custom Database** node on the right panel to expand the tree. All custom databases on all of the SQL Servers that have DocAve Agents are listed under the corresponding SQL instance node and the AlwaysOn Availability Group listener node (if the SQL instance is a replica of one or more AlwaysOn Availability Groups) in the tree. If you choose to verify the storage layout for adding the custom databases, as to AlwaysOn Availability Group, DocAve will verify if the databases are on NetApp FAS LUN in the preferred replica of the AlwaysOn Availability Group.

***Note:** If the database is selected from AlwaysOn Availability Group, it cannot be selected from the regular SQL instance of the same SQL Server, and the backup of this database will be defined by the [Backup Replica Settings](#) configured in the backup schedule or **Run Now** interface. If a database is selected from both the regular SQL instance and AlwaysOn Availability Group listener of different SQL Servers, DocAve will choose one AlwaysOn Availability Group replica at random to back up the database, and skip the backup on the regular SQL instance.

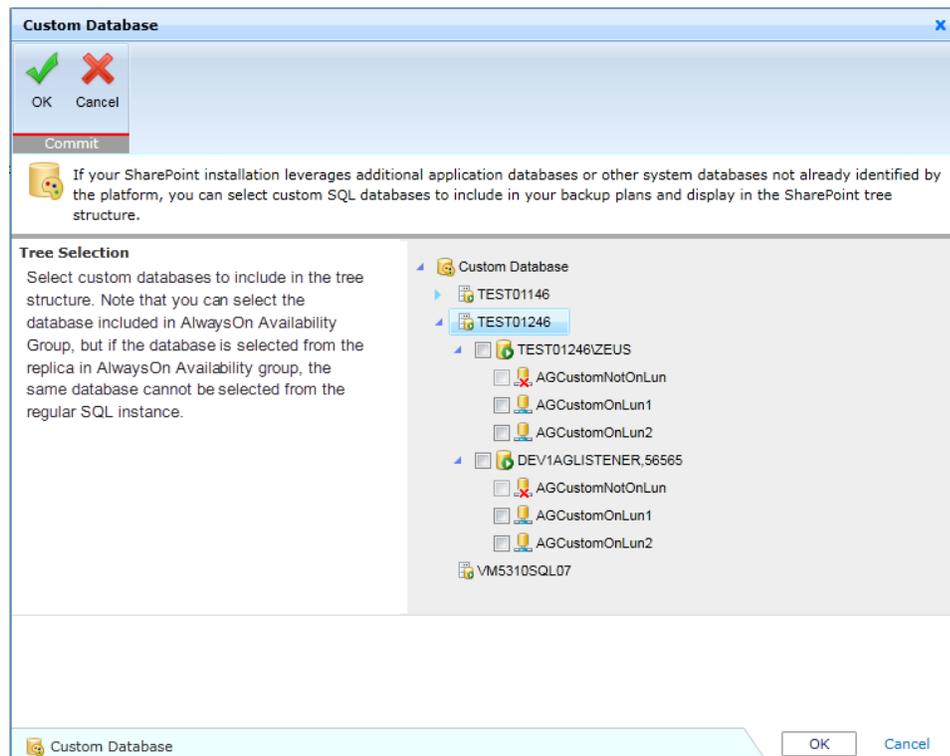


Figure 12: The Custom Database tree.

- c. Select the databases that you want to be displayed on the backup tree by selecting the checkbox next to the database.

***Note:** Databases that have **Restoring** status cannot be backed up and are not displayed in the tree.

- d. When finished, click **OK**. The selected databases are now shown on the backup tree under the **Custom Database** node.
5. Click **Next**. The **Storage Policy** page appears.
6. Select a **Storage Policy** from the drop-down list, or choose to set up a new storage policy by clicking the **New Storage Policy** link. Click the **here** link to display detailed information of the **Primary Storage, Total Space, Free Space, and The number of physical device(s) attached** in the area below.

***Note:** Please make sure the user credentials designated for the Storage System Profile have the following permissions before performing a Platform Backup for NetApp Systems job:

- A member of the local **Administrators** group, if the storage system is NetApp Data ONTAP 7.X or 7 mode of NetApp Data ONTAP 8.X.
- A member of **Ontapi admin** group, if the storage system is NetApp Data ONTAP 9.x or Cluster mode of NetApp Data ONTAP 8.X.

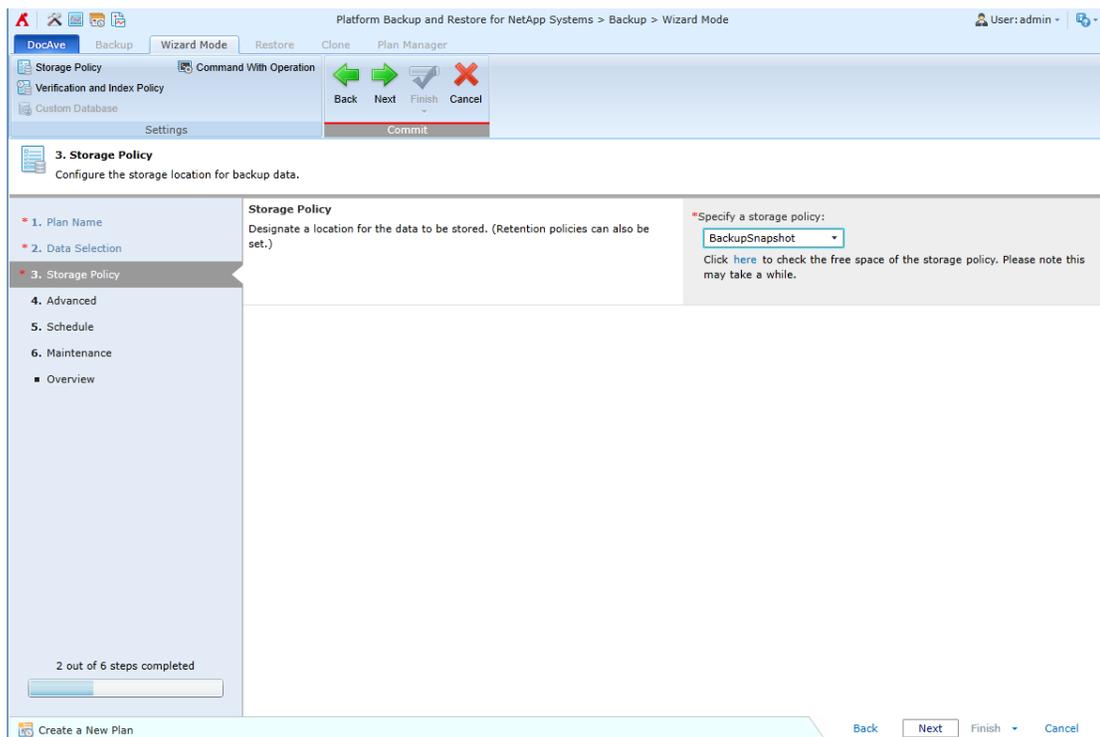


Figure 13: Selecting a Storage Policy.

7. Click **Next**. The **Advanced** page appears.

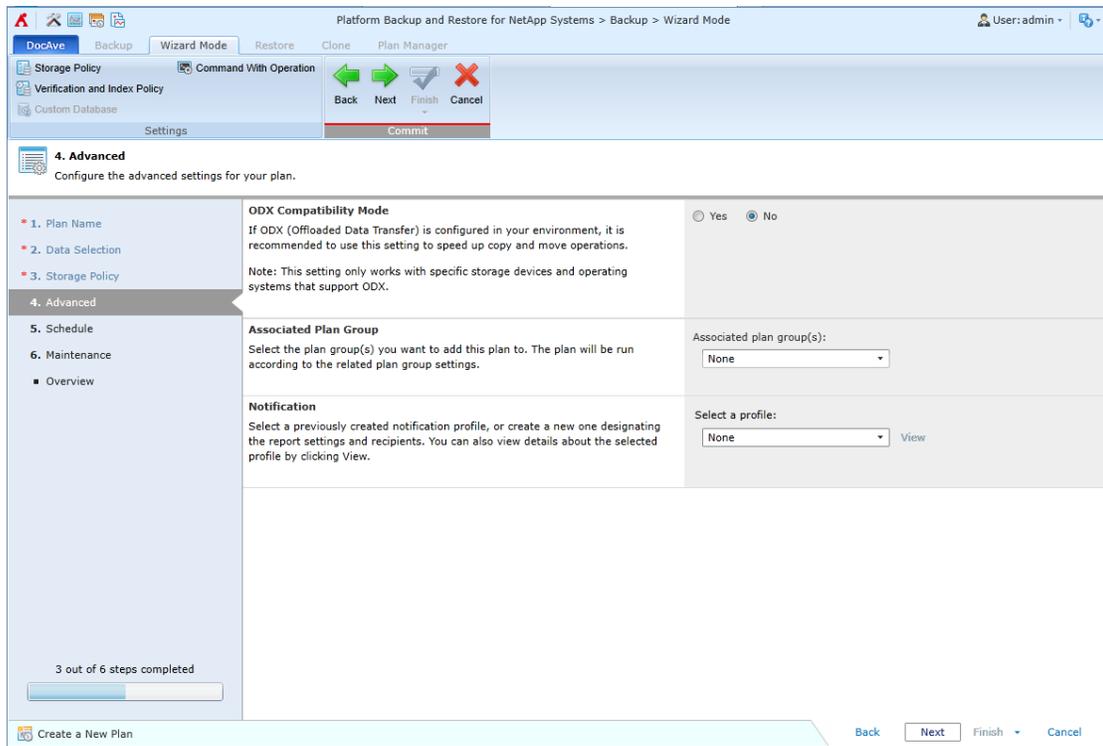


Figure 14: Configuring the Advanced page.

- a. **ODX Compability Mode** – Choose whether or not to enable **ODX Compability Mode** to speed up copy and move operations. To enable ODX compability mode, select **Yes**; otherwise, select **No**. For more details on ODX Compability Mode, refer to <http://msdn.microsoft.com/en-us/library/windows/hardware/hh833784.aspx>.

***Note:** ODX Compability Mode (Offloaded Data Transfer) supports Web front-end data and the FAST Search data (the FAST Search data stored in NetApp FAS LUN is not supported), but ODX does not support data in a database snapshot. For details on these limitations, refer to Microsoft’s [“Offloaded Data Transfers”](#) article.

- b. **Associated Plan Group** – Select the plan groups from the drop-down list to add the plan to the corresponding groups. The added plan will run according to the related plan group settings. You can also choose to create a new plan group by clicking the **New Plan Group** link in the drop-down list. For more information on plan groups, refer to the [DocAve 6 Control Panel Reference Guide](#).
- c. To inform users of the Platform Backup for NetApp Systems job, configure the **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list, or choose to create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.

8. Click **Next**. The **Schedule** page appears.

9. Define the **Schedule type** selection:

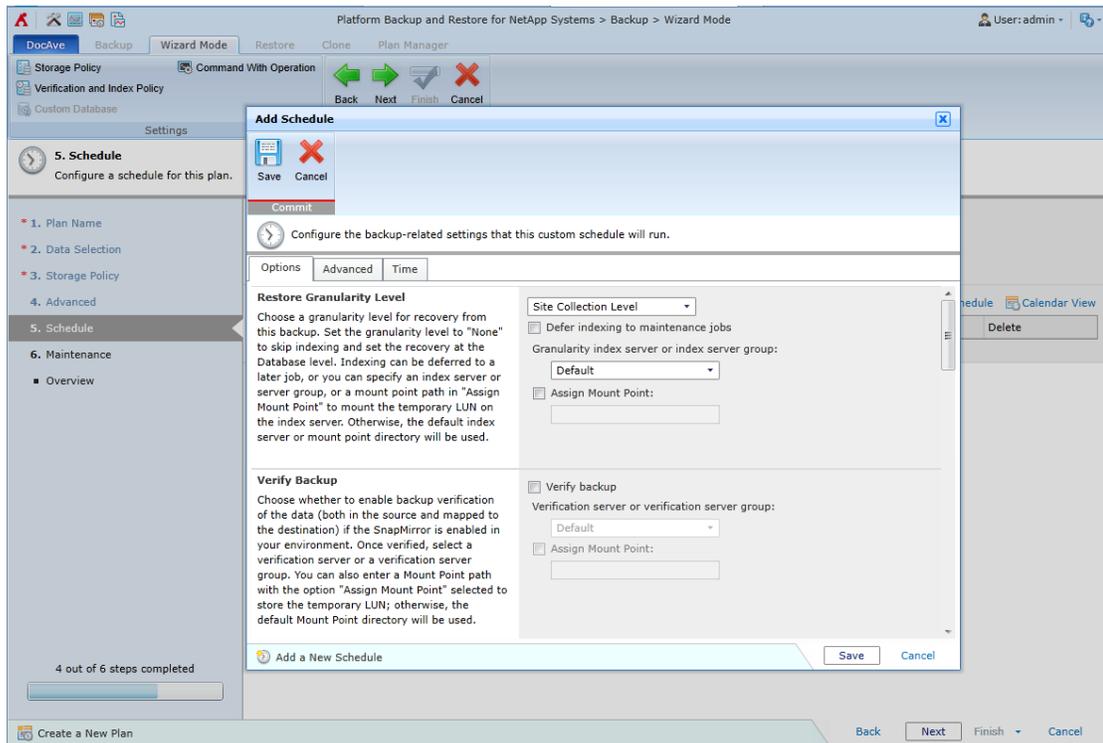


Figure 15: Configuring a schedule.

- **No schedule** – Select this option to run the plan manually, and the plan will be saved in Plan Manager.
- **Configure the schedule myself** – Select this option to configure a customized schedule, and run the backup job by schedule. Click **Add Schedule** to set up a schedule. The **Add Schedule** window appears. Configure the settings in the **Options**, **Advanced** and **Time** tabs according to the detailed information in each section. Refer to [Backup Schedule](#) for more information on adding a schedule.

After configuring the schedule for the Platform Backup for NetApp Systems, click **Calendar View** to view the scheduled jobs by **Day**, **Week**, or **Month**. All of the schedules will be displayed in the **Summary** table. Click **X** to delete a schedule.

10. Click **Next**. The **Maintenance** page appears.
11. Configure the **Maintenance Options** to be performed on the snapshots during the maintenance.
12. **Index last ... deferred indexing** – This option generates indexes for backup jobs that have the **Defer Indexing to maintenance jobs** option selected. After selecting this option, enter the number of jobs for which indexes will be generated. For example, setting this option to **Index last 3 deferred indexing** will generate the indexes for the most recent three backup jobs that have a **Finished/Finished with Exception** status.
 - a. **Clone database on SnapMirror destination** – Use this option to clone a database based upon the Snapshot copy on the SnapMirror destination volume.

- b. **Clone database on SnapVault destination** – Use this option to use the remote backup to perform the clone operation. Snapshots saved in SnapVault primary storage are considered Local Backups and snapshots saved in SnapVault secondary storage are considered Remote Backups.
 - c. **Granularity index server or index server group** – Choose the index server or server group used for generating the granular level restore index. To generate the granular level index, DocAve uses the SQL Server that contains the data to be backed up by default. You can click the **New Index Server or Index Server Group** link in the drop-down list to create a new index server. For more information, refer to [About the Verification and Index Policy](#).
 - d. **Assign Mount Point** – If you do not want to use the default mount point directory, use this option to specify the mount point directory on which a backup set will be mounted during generating the granular level restore index. For example: **C:\mountpoint**.

***Note:** A volume mount point is a drive or volume in Windows that is mounted to a folder that uses the NTFS file system. A mounted drive is assigned a drive path instead of a drive letter. Volume mount points enable you to exceed the 26 drive letter limitation. By using volume mount points, you can mount a target partition onto a folder on another physical disk.
 - e. **Granular Index Method** – Choose how to generate the granular index. **Sequential** will generate the index one database at a time on each SQL Server, minimizing the resource requirements. **Parallel** will generate the index for multiple databases simultaneously on each SQL Server. If you select **Parallel**, by default, there will be at most five databases generating index at the same time on a SQL Server. You can change the maximum number for the parallel index generation. For details, refer to [Configuring the Maximum Number of Database Indices to Generate in Parallel](#).
 - f. **BLOB Settings** – Select which options to perform on the device that stores the original BLOB data after the BLOB backup completes. The SnapMirror/SnapVault destination of the device that stores the original BLOB data will be updated.
 - g. **Storage Policy Settings** – Select which options to perform on the device configured in the storage policy after the backup operation completes. The SnapMirror/SnapVault destination of the device configured in the storage policy will be updated.
13. **Verify last ... unverified backup(s)** – Select this option to specify how many unverified backup jobs to verify. Enter a positive integer in the provided field.
- a. **Verification server or Verification server group** – Select the server or server groups used for verifying the backed-up database. By default, the default verification server is used. You can click the **New Verification Server or Verification Server Group** link in the drop-down list to create a new verification server or server group. For more information, refer to [About the Verification and Index Policy](#).

- b. **Assign Mount Point** – If you do not want to use the default mount point directory, use this option to specify the mount point directory on which a backup set will be mounted during database verification. For example: **C:\mountpoint**.

***Note:** If you are using a clustered instance of SQL, the mount point NetApp FAS LUN needs to be a shared NetApp FAS LUN in the SQL cluster.

- c. **Scripts** – If you selected the **Run command with operation** option, the **Verify** operation type command profile will be listed in the drop-down list. Select a command profile from the drop-down list to run the commands according to the command profile you selected. You can also click the **New Command Profile** link in the drop-down list to create a new command profile. For more information, refer to [About Command with Operation](#).
- d. **BLOB Settings** – Select which options to perform on the device that stores the original BLOB data after the BLOB backup **completes**. The SnapMirror/SnapVault destination of the device that stores the original BLOB data will be updated.
- e. **Farm Component Settings** – Configure the **SnapMirror-/SnapVault**-related settings for the backed-up databases and index components.

- **SnapMirror** – Choose the operations to perform on the SnapMirror destination after completion of the database backup and index components.

- **Update SnapMirror after operation** – Use this option if you are using backups that reside on volumes configured as SnapMirror sources. This option updates the SnapMirror destination after the backup operation is complete.
- **Verify on available SnapMirror destination volumes** – Use this option to verify the database and index components on the SnapMirror destination volume.

- **SnapVault** – Choose the operations to be performed on the SnapVault storage system after completion of the database and index components backup.

***Note:** Prior to using this option in a backup plan, the SnapVault datasets must have already been created by SMSQL and in a conformant state. For more information on configuring the SnapVault datasets, refer to the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

- **Verify archive backup on secondary storage** – Use this option to verify the database and index components archived on the secondary storage system.
- **Archive backup to secondary storage** – With this option selected, you can retain backups at the archived location on an **Hourly, Daily, Weekly, Monthly, or Unlimited** basis.

- f. **Storage Policy Settings** – Select which options to perform on the device configured in the storage policy after the backup operation completes. The SnapMirror/SnapVault destination of the device configured in the storage policy will be updated.
- *Note:** If you select a **Maintenance Option**, you must configure a schedule for running the maintenance jobs.
- *Note:** You can also perform maintenance jobs manually in Job Monitor. For more information, refer to [Manual Maintenance](#).
14. **Maintenance Schedule** – Define the **Schedule type selection** for scheduled maintenance jobs. Note that you can only perform a maintenance job on **Finished** and **Finished with Exception** backup jobs whose **Index Status** is not **Successful**.
- **No schedule** – Run the maintenance job manually. Select this option if you want to run the maintenance job manually in Job Monitor after the corresponding backup job completes.
 - **Configure the schedule myself** – Select this option to configure a customized schedule, and run the maintenance job by schedule. Click **Add Schedule** to create a schedule. The **Add Schedule** window appears. After configuring the schedule for the maintenance job, click **Calendar View** to view the scheduled jobs by **Day**, **Week**, or **Month**. All the schedules will be displayed in the **Summary** table. Click **X** to delete a schedule.
15. **Maintenance Notification** – To inform users of a maintenance job, configure a notification. Select a previously configured notification profile from the **Select a profile** drop-down list, or create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.
16. When finished, click **Next**. The **Overview** screen appears.
17. Review and edit the plan selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
18. Select the **Save current plan as plan template** checkbox to save the current plan as a template. Enter the template name in the textbox; after this plan template is saved, you can select it when creating a new plan.
19. On the lower-right section of the screen or on the ribbon, perform the following actions:
- Click **Finish** to save the configuration of the plan without running it. The Backup plan will be now listed in **Plan Manager**.
 - Click **Finish and Test Run** to save the configuration and then perform a test run job, based on the plan, immediately. The backup job is now listed in **Plan Manager**.
 - Click **Finish and Run Now** to save the configuration and then run the saved plan immediately. The backup plan is now listed in **Plan Manager**.

Backup Schedule

Configure the following settings in each tab to build a new backup schedule.

1. **Options tab** – Choose backup options for the scheduled backup job.

Add Schedule

OK Cancel

Commit

Configure the backup-related settings that this custom schedule will run.

Options Advanced Time

Restore Granularity Level

Choose a granularity level for recovery from this backup. Set the granularity level to "None" to skip indexing and set the recovery at the Database level. Indexing can be deferred to a later job, or you can specify an index server or a Mount point path in "Assign Mount Point" to mount the temporary LUN on the index server. Otherwise, the default index server or mount point directory will be used.

Site Collection Level

Defer indexing to maintenance jobs

Granularity index server:

Default

Assign Mount Point:

Verify Backup

Choose whether to enable backup verification of the data (both in the source and mapped to the destination) if the SnapMirror is enabled in your environment. Once verified, select a verification server. You can also enter a Mount Point path with the option "Assign Mount Point" selected to store the temporary LUN; otherwise, the default Mount Point directory will be used.

Verify backup

Verification server:

Default

Assign Mount Point:

Add a New Schedule

OK Cancel

Figure 16: Configuring backup options.

2. **Restore Granularity Level** – Select the restore granularity level for the scheduled backup job. Note that the more detailed restore granularity level you select, the more detailed the granular restore index will be. Because a detailed granular restore index requires more storage space than a less detailed one, ensure that there is enough space to store the generated granular restore index. You can view the size of the data backed up by each Platform Backup for NetApp Systems plan and the available space of each logical device used by the corresponding storage policy when viewing the detailed information of the plan's storage policy in **Control Panel > Storage Configuration > Storage Policy**. After selecting the Restore Granularity Level, you can expand the tree to the level you selected when running a restore job.

If you select **None**, no granular restore index is generated. However, you can still restore the backup data of this job through a Platform granular restore by using the **Browse the index from backup data** option. The granular restore index makes it easier to search for contents to be restored from a backup.

- **Defer indexing to maintenance jobs** – Selecting this option does not generate a granular restore index for the backup data in the corresponding logical device. The index can be generated using a scheduled or manual maintenance job that is run after the backup job completes.
 - **Granularity index server or index server group** – Choose one or more index servers used for generating the granular level restore index. By default, the SQL server whose data you want to back up is used. You can click the **New Index Server or Index Server Group** link in the drop-down list to create a new index server or group. For more information, refer to [About the Verification and Index Policy](#).
 - **Assign Mount Point** – If you do not want to use the default mount point directory, use this option to specify the mount point directory on which a backup set will be mounted during generating the granular level restore index. For example: **C:\mountpoint**.
3. **Verify Backup** – Configure settings for verifying the backed-up database.
- **Verify Backup** – Select this option to enable the verification of the backed up database. Note that not all backups have to be verified, but it is recommended that you perform at least one verified backup per day. Also, verifications can be performed through scheduled maintenance jobs after the backup job is completed.
 - **Verification server or verification server group** – Specify the server or server group used for verifying the backed-up database. By default, the default verification server is used. You can click the **New Verification Server or Verification Server Group** link in the drop-down list to create a new verification server. For more information, refer to [About the Verification and Index Policy](#).

***Note:** If the version of SnapManager for SQL Server is 7.2 or later, the verification for the database backups in different SQL instances will be performed in parallel concurrently.
 - **Assign Mount Point** – If you do not want to use the default mount point directory, use this option to specify the mount point directory on which a backup set will be mounted during database verification. For example: **C:\mountpoint**.
4. **Check Old Backups to Be Deleted** – If a retention rule is enabled for the selected storage policy and the **Check Old Backups to Be Deleted** function is enabled, DocAve looks to see if former snapshots from this plan have been manually deleted by the user accidentally. For those accidentally deleted snapshots, DocAve ensures that deleted snapshot data cannot be selected to restore in the **Data Selection** interface of the **Restore** wizard. Note that DocAve does not clean up snapshot metadata.
5. **Transaction Log Backup & Truncation** – If the **Run transaction log backup after full database backup** option is selected, this option backs up and truncates the **transaction** log after a Full database backup. By default, this option is selected. Note that the transaction log backup is skipped for databases in simple recovery mode.
6. **Back up Stub Database for Selected Scope** – Choose whether or not to back up the stub database along with the contents you have selected to back up. This option allows users to perform granular-level restores of stubs from a backed-up stub database.

7. **Back up BLOB for Selected Scope** – This option backs up BLOB content generated by Storage Manager and files in the connected path of Connector. Select the corresponding checkboxes if you wish to back up this BLOB data.

***Note:** If you want to back up the BLOB data generated through the **Leave a stub in SharePoint for each document (uses Storage Manager)** feature of Archive Manager, select **Back up Storage Manager BLOB** option. In the same way, if you have BLOB data generated through Archive Manager in the backup scope, selecting **Back up Storage Manager BLOB** option will also back up the Archive Manager BLOB data together with the Storage Manager BLOB data during the backup job.

8. **Back up Web Front-End Servers in Parallel** – Choose whether or not to back up the Web front-end servers in parallel. Backing up the Web front-end servers in parallel may cause overload of the Media service. If you select the **Back up Web Front-End servers in parallel** option, you are required to specify the maximum number of the Web front-end servers you want to back up in parallel.

***Note:** The following recommendations assume that your network bandwidth is 60 MB/s:

If the content under the **Extra File System Folder** node exceeds **1 GB**, **3** or **4** is a recommended maximum number.

If the content under the **Extra File System Folder** node does not exceed **1 GB**, the maximum number can be larger because the average backup rate is less than **1 MB/s**.

9. **Refresh SharePoint Farm Topology** – Choose whether or not to refresh the SharePoint farm topology before starting to run the backup job and to update the backup scope in the Platform Backup for NetApp Systems plan. Leverage this option if you have strict change management policies for SharePoint. Refreshing the farm topology will use the current state of the farm, as indicated by SharePoint Central Administration, to define the scope of the selected nodes in this backup plan. The plan will assume any changes to a farm's services, server layout, or Web applications and databases from the previous job are expected and will not log these changes as exceptions in the job details. After selecting this option, the **Verify Storage Layout** option appears. Choose whether or not to select this option to verify the storage layout before backup.

***Note:** Leveraging this option will not reveal VMs in your farm topology.

10. **Granular Index Method** – Choose how to generate the granular index. Sequential will generate the index one database at a time on each SQL Server, minimizing the resource requirements. **Parallel** will generate the index for multiple databases simultaneously on each SQL Server. If you select **Parallel**, by default, there will be at most five databases generating index at the same time on a SQL Server. You can change the maximum number for the parallel index generation. For details, refer to [Configuring the Maximum Number of Database Indices to Generate in Parallel](#).

11. **Check Agent Account Permissions for Backup** – Select **Yes** to check the Agent account permissions for backup in the backup job. If you are sure that your Agent Account has the required permissions for using Platform Backup and Restore for NetApp Systems, select **No** to

skip this process. Skipping this process may result in faster job times. If the job fails because of insufficient permissions for the Agent account, the backup job report will show the details.

12. **Job Report** – Choose the level of reporting for the backup job. **Simplified** creates a summary of the backup data. **Detailed** creates a full list of all backup objects, but at the cost of performance. If you select Storage Manager or Connector BLOB data for backup, the **BLOB Details** tab will be shown in the Job Monitor **Job Details** interface.

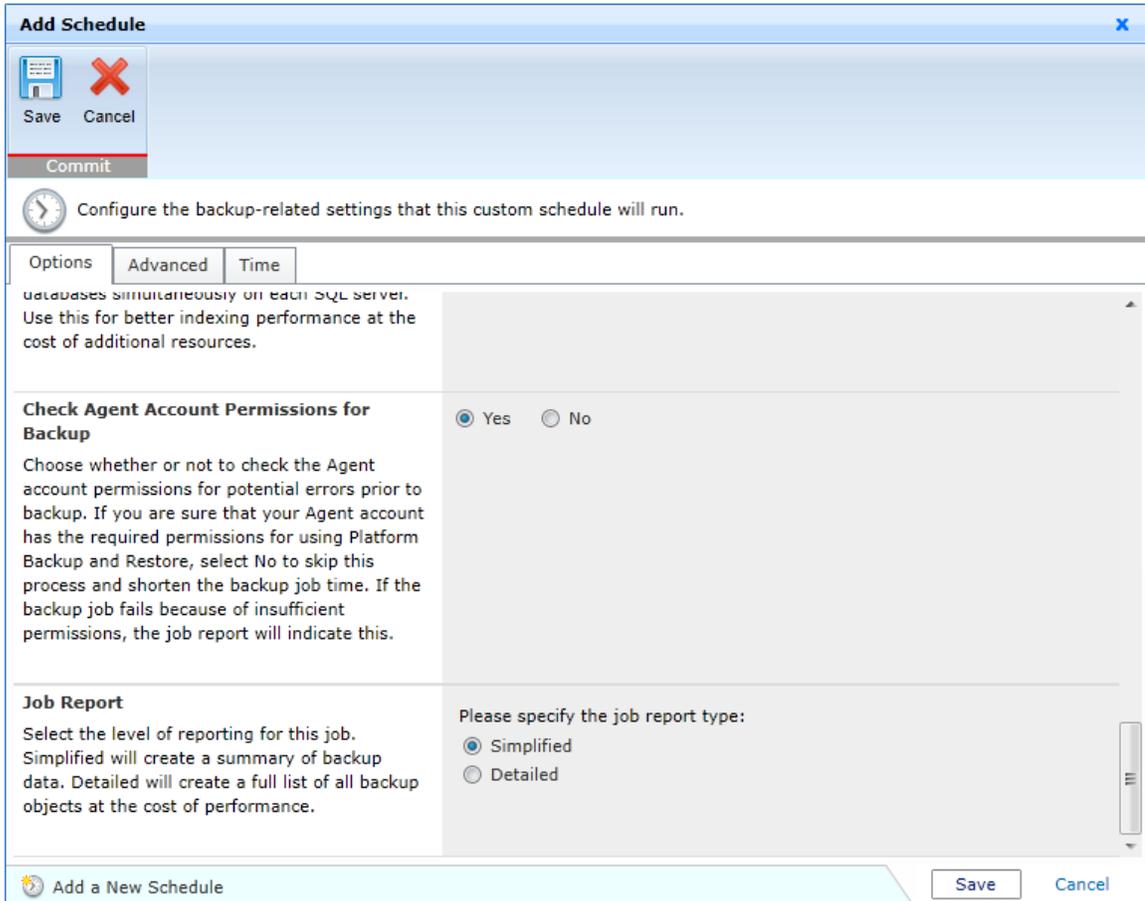


Figure 17: Selecting the job report type.

13. **Advanced tab** – Configure the advanced settings for the scheduled backup job.

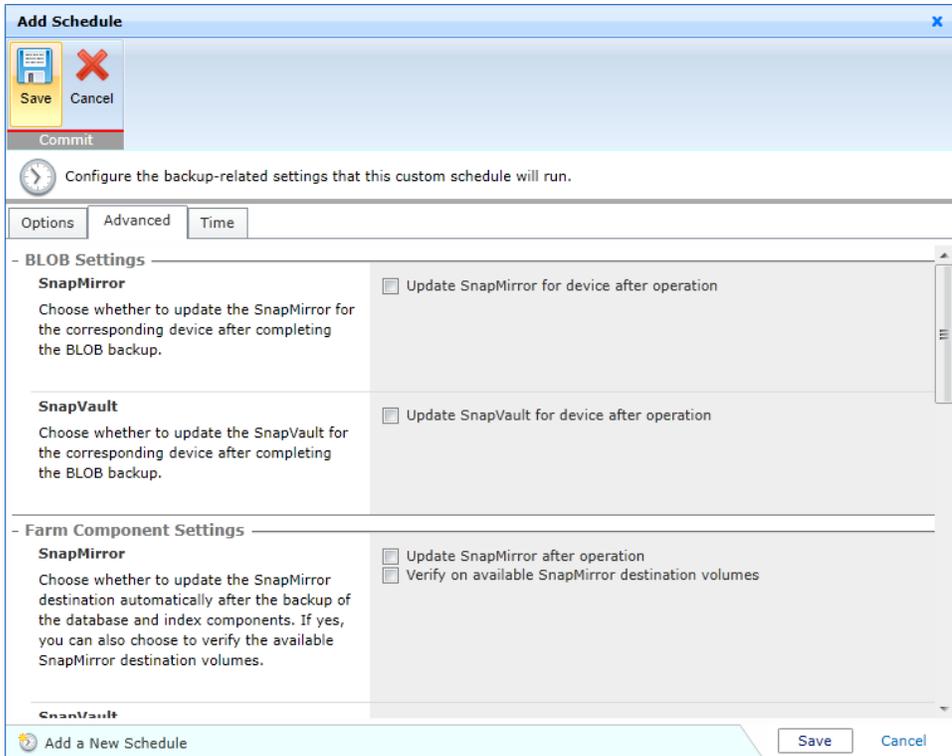


Figure 18: Configuring advanced backup settings (1).

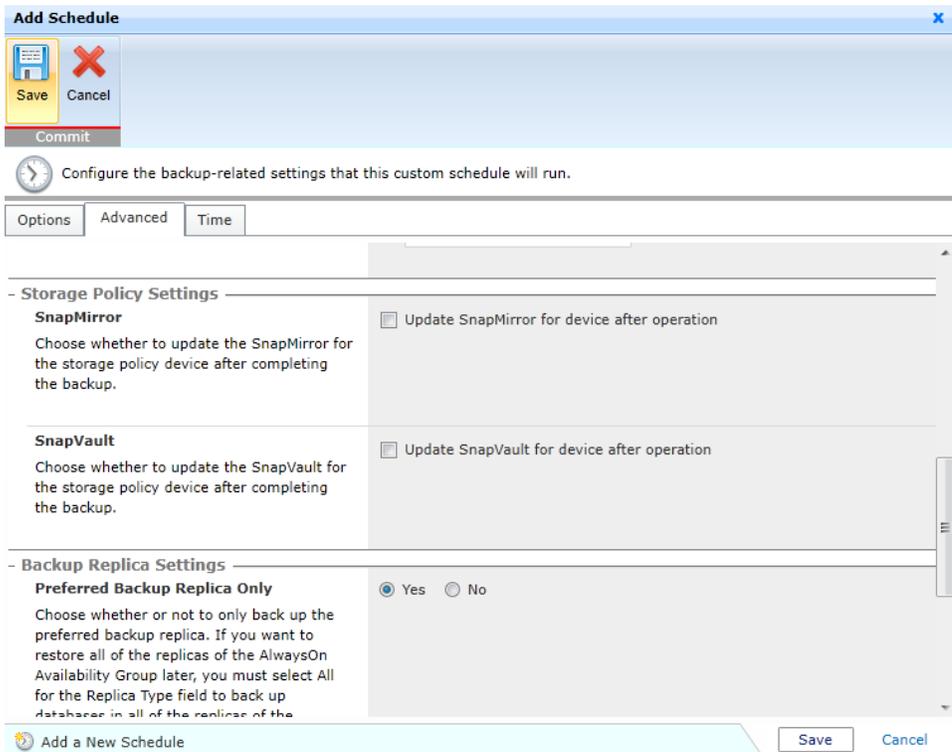


Figure 19: Configuring advanced backup settings (2).

14. **BLOB Settings**– Select which options to perform on the device that stores the original BLOB data after the BLOB backup completes. The SnapMirror/SnapVault destination of the device that stores the original BLOB data will be updated.
15. **Farm Component Settings**– Configure the SnapMirror-/SnapVault-related settings for the backed-up databases and index components.
 - a. **SnapMirror** – Choose the operations to perform on the SnapMirror destination after completion of the backup of the databases and index components.
 - **Update SnapMirror after operation** – If you are using backups that reside on volumes configured as SnapMirror sources, this option updates the SnapMirror destination after the backup operation is complete.
 - **Verify on available SnapMirror destination volumes** – Use this option to verify the data on the SnapMirror destination volume.
 - b. **SnapVault** – Choose the operations to be performed on the SnapVault storage system after completion of the backup of the databases and index components.

***Note:** SnapVault is an option of NetApp Data ONTAP; if you are using the SMSQL 6.x, ensure that you have set up the Protection Manager Datasets via SMSQL 6.x.

***Note:** Prior to using this option in a backup plan, the SnapVault datasets must have already been created by SMSQL and in a conformant state. For more information on configuring the SnapVault datasets, refer to the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

***Note:** If you are using clustered NetApp Data ONTAP 8.2 or later, you can directly configure SnapVault on the clustered storage devices through SMSQL 7 to make it available for DocAve 6. If you are using 7-Mode of NetApp Data ONTAP 8.2 or earlier (for example, NetApp Data ONTAP 7.x), you must use DFM to configure SnapVault for availability in DocAve 6.

 - **Archive backup to secondary storage** – With this option selected, you can retain backups at the archived location on an **Hourly, Daily, Weekly, Monthly, or Unlimited** basis.
 - **Verify archive backup on secondary storage** – Use this option to verify the database archived at the secondary storage system.
 - c. **Scripts** – If you select the **Run command with operation** option, the **Backup** operation command profile type will be listed in the drop-down list. Select a command profile from the drop-down list; the commands will be run according to the command profile you selected. You can also click the **New Command Profile** link in the drop-down list to create a new command profile. For more information, refer to [About Command with Operation](#).
16. **Storage Policy Settings**– Select which options to perform on the device configured in the storage policy after the backup operation completes. The SnapMirror destination of the device configured in the storage policy will be updated.

17. **Backup Replica Settings** – Configure the backup settings for replicas in AlwaysOn Availability Groups.

- **Preferred Backup Replica Only** – Select **Yes** if you want to back up only preferred backup replica.

If you select **No**, proceed to designate the replica type and backup priority of the replicas you want to back up:

- **Replica Type** – Choose to back up all of the replicas, all of the primary replicas, or all of the secondary replicas in the AlwaysOn Availability Group. Select **All**, **Primary**, or **Secondary** from the **Replica Type** drop-down list.
- **Backup Priority** – Configure the Minimum and Maximum value of the backup priority to back up the replicas whose backup priority falls within the range.

18. **Time tab** – Configure the detailed schedules for the scheduled backup job.

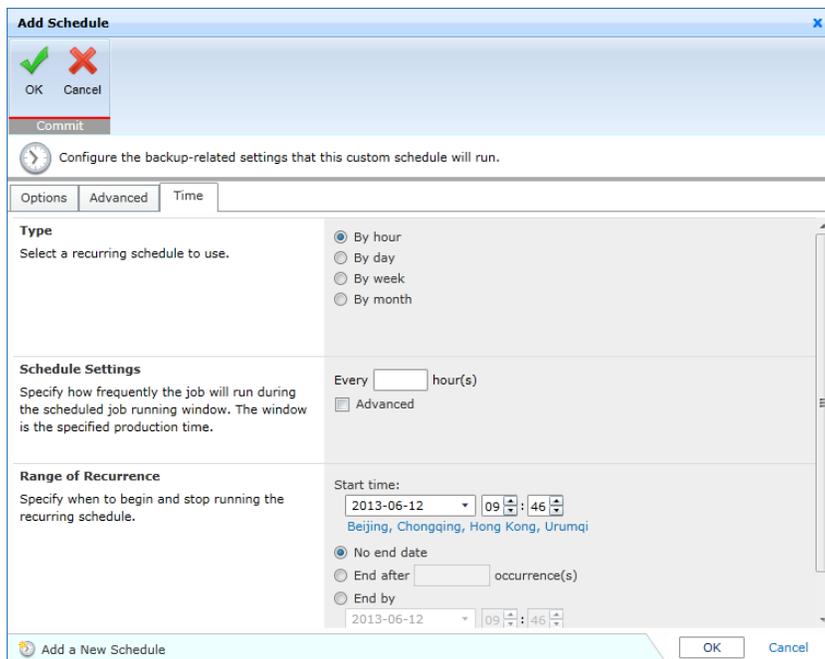


Figure 20: Configuring schedule backup settings.

- a. **Type** – Select the recurring schedule. You can select **By hour**, **By day**, **By week**, or **By month**.
- b. **Schedule Settings** – Set up the frequency for the scheduled backup job. If you select the type as **By hour**, **By week**, or **By month**, set up the **advanced** settings for the frequency. For more scheduling options, select the **Advanced** checkbox to reveal additional options.
 - Advanced settings for **By hour**:
 - **Specify production time** – Select the production time range for the running jobs from the drop-down lists. The start time will be the time in

the **From** field. The backup job will run hourly until the time entered in the **to** field.

- **Select time below** – Select a start time from the drop-down list. The backup job will start at the entered time. You can click **Add** to specify more than one start time.
- Advanced settings for **By week** – Enter an integer greater than zero into the **Run every: _ week(s)** text box and then select the days of the week from the **on: _** drop-down list.
- Advanced settings for **By month:**
 - **On day _ of _** – Runs the backup job on the month and date you select.
 - **Day: _ of every _ month(s)** – For example, if you enter **Day: 1 of every 2 months**, the backup job will run on the first day of this month, and on the first day of the month after next month, and so until the entered end time.
 - **The: __ of every _ month(s)** – For example, if you enter **The: Second Monday of every 2 months**, the backup job will run on the second Monday every 2 months.
 - **The: __ of _** – For example, if you enter **The: Second Monday of February, March, and April**, the backup job will run on the second Monday of February, second Monday of March, and second Monday of April.
- c. **Range of Recurrence** – Select the start time and end time for the schedule.

Manual Maintenance

In addition to a scheduled maintenance job (which can be configured in the backup plan), you can manually perform a maintenance job, which generates a granular level index on **Finished/Finished with Exception** jobs whose **Index Status** is not **Successful**. The Manual Maintenance options will configure the SnapMirror/SnapVault settings in Job Monitor.

For detailed information on each option, refer to [Maintenance Options](#).

To inform designated users that a maintenance job is about to be run, configure a **Maintenance Notification**. Select a previously configured notification profile from the **Select a profile** drop-down list, or create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.

Maintenance jobs can be viewed in Job Monitor by selecting **Filter group > Module > Platform Maintenance Manager for NetApp Systems**. For more information, refer to the [DocAve 6 Job Monitor Reference Guide](#).

Using Form Mode to Create a Backup Plan

Form Mode is recommended for users who are familiar with building DocAve 6 backup plans. To build a backup plan in Form Mode, click **Plan Builder > Form Mode**, and then select the content to be backed up. Refer to [Using Wizard Mode to Create a Backup Plan](#) for detailed information regarding each option.

***Note:** If this is your first time building a plan, or if you think you would benefit from descriptions of each plan component, it is recommended you use the Wizard Mode.

Backing up Databases First, and then Index Components

Find the **SP2010PlatformConfiguration.xml** file in the Agent installation directory (...*AvePoint \DocAve 6\Agent\data\SP2010\Platform*) on the SQL Server that contains the databases and index components. Configure the **NativeBackupParallelConfig BackupParallel** attribute; otherwise, the customized configuration will not take effect and the default configuration will be used.

To specify whether or not to back up the databases and index components in parallel that reside on the same server, configure the following attribute:

```
<NativeBackupParallelConfig BackupParallel="true"/>
```

The default value is “**true**”, which indicates that the databases and index components on this server that are included in the backup plan will be backed up in parallel. If the value is set to **False**, the databases on this server will be backed up at first before backing up the index components.

***Note:** The index component here refers to that from Search Service Application or SharePoint 2010 Help Search.

Pruning Log Backups from the Shared Folder

The SMSQL log backups stored in the shared folder are used to ensure the successful restore of the databases in AlwaysOn Availability Group. If you want to prune the log backups from the shared folder, configure the log backup retention settings in the **SP2010PlatformConfiguration.xml** configuration file on each SQL Server Agent. The Platform Backup for NetApp Systems jobs that starts afterwards will automatically prune the log backups from the shared folder according to the settings in the configuration file, and retention settings configured in the configuration file will be returned with the – **RetainShareBackupDays** parameter in the SMSQL new-backup cmdlet.

***Note:** This feature only functions when the following options are met:

- The databases for backup are in the AlwaysOn Availability Group.
- The storage policy used by backup plans has retention rule enabled.

Complete the steps below to modify the **SP2010PlatformConfiguration.xml** file:

1. Go to the `...Agent\data\SP2010\Platform` directory on each SQL Server Agent.
2. Find the `SP2010PlatformConfiguration.xml` configuration file and open it with Notepad.
3. Locate the `JobRetentionRetainShareBackupDays` attribute within the `JobRetentionDeletedSnapshotRuleConfig` node.
***Note:** The default value of the `JobRetentionRetainShareBackupDays` attribute is `-1`, which represents that the log backups will not be deleted from the shared folder.
4. If you want to prune the log backups from the shared folder, designate a proper value for the `JobRetentionRetainShareBackupDays` attribute. The Platform Backup for NetApp Systems job will prune the log backups whose backup time is out of the designated days from the shared folder. To set a proper value, note the following:
 - The time unit of this value is **Day**.
 - The number of the days you set for this attribute must be greater than the days of the backup data retained within the storage policy; otherwise, Platform Restore for NetApp Systems job may fail when using the incomplete backup data to restore. You can get an approximate number in this way:
 - i. Look over your retention rules configured for each storage policy and find the greatest number of the days for keeping full backups.
***Note:** If your retention rule is set to keep the specified number of last full backups, you can figure out when the earliest backup in the retained backups was performed according to your backup schedule.
 - ii. If you did not figure out the value in the last step and your retention rules' actions include removing the job, you can go to **Job Monitor** and use the **Plan Name** to filter out the backup jobs. You will see the date when the earliest backup job was performed.
5. Save the configuration and close this file.

Running a Backup Job Immediately

If setting up a plan using [Wizard Mode](#), you can run the backup job immediately by clicking **Finish and Run Now** when saving the plan; the plan is saved and the job is run immediately.

If setting up a plan using [Form Mode](#), click **Save and Run Now** when saving the plan; the plan is saved and the job is run immediately.

***Note:** A backup job cannot be run at the same time as a restore job. However, you can perform simultaneous backup and restore actions if the actions are on separate SQL instances.

***Note:** DocAve Platform Backup for NetApp Systems plans do not lock up the SharePoint databases and index files when backing up, and therefore can be scheduled to run during normal production hours.

Managing Plans

Use **Plan Manager** to manage created Platform Backup for NetApp Systems plans. After launching the **Platform Backup and Restore for NetApp Systems** interface, click **Plan Manager** next to the **Clone** tab. In the **Plan Manager** interface, all of the previously created plans are displayed in the main display pane.

To change the number of the plans displayed per page in this interface, select the desired number from the **Show rows** drop-down menu in the lower right-hand corner. To sort the plans by heading, click the column heading such as **Plan Name**, **Description**, **Plan Group**, **Farm**, and **Last Modified Time**.

Perform the following actions in the **Plan Manager** interface:

- **View Details** – Select a plan and click **View Details**. The backup scope and the plan settings are displayed on the **View Details** interface. When you want to change the nodes you selected or want to modify the settings, click **Edit** on the ribbon.
- **Edit** – Select a plan and click **Edit** on the ribbon to change the configurations for the selected plan. You can change the nodes you selected and modify the plan settings. Besides, you can click **Storage Policy**, **Verification and Index Policy**, **Custom Database**, or **Command with Operation** to perform the corresponding actions.
- **Delete** – Select the plans that you want to delete and click **Delete** on the ribbon. A confirmation window will pop up and ask whether you are sure that you want to proceed with the deletion. Click **OK** to delete the selected plans, or click **Cancel** to return to the **Plan Manager** interface without deleting the selected plans.
- **Test Run** – Click **Test Run** to perform a test run job that simulates the real Platform Backup for NetApp Systems job. By viewing the job report of the test run, you can find whether the source contents can be backed up successfully, and then adjust the plans or optimize the settings.
- **Run Now** – Click **Run Now** to go to the **Run Now** interface. For more information on the **Run Now** interface settings, see [Configuring the Run Now Interface](#).

Configuring the Run Now Interface

In the **Run Now** interface, the **Options** tab and the **Advanced** tab are available for configuring backup job settings. Refer to the section below for details on the **Options** tab:

1. **Restore Granularity Level** – Select the restore granularity level for the backup job. Note that the more detailed restore granularity level you select, the more detailed the granular restore index will be. A detailed granular restore index requires more storage space than a less detailed one, so ensure that your storage has enough free space for the generated granular restore index. You can view the size of the data backed up by each Platform Backup for NetApp Systems plan and the available space of each logical device used by the corresponding storage policy when viewing the detailed information of the plan's storage policy in **Control Panel > Storage Configuration > Storage Policy**. After selecting the Restore Granularity Level, you can expand the tree to the level you selected when running a restore job.

If you select **None**, no granular restore index is generated. However, you can still restore the backup data of this job through a Platform granular restore by using the **Browse the index from backup data** option. The granular restore index makes it easier to search for contents to be restored from a backup.

- **Defer indexing to maintenance jobs** – Selecting this option does not generate a granular restore index for the backup data in the corresponding logical device. The index can be generated using a scheduled or manual maintenance job that is run after the backup job completes.
 - **Granularity index server or index server group** – Select one or more index servers used for generating the granular level restore index. By default, the SQL server whose data you want to back up is used. You can click the **New Index Server or Index Server Group** link in the drop-down list to create a new index server or index server group. For more information, refer to [About the Verification and Index Policy](#).
 - **Assign Mount Point** – If you do not want to use the default mount point directory, use this option to specify the mount point directory on which a backup set will be mounted during generating the granular level restore index. For example: **C:\mountpoint**.
2. **Verify Backup** – Configure settings for verifying the backed-up database.
- **Verify Backup** – Select this option to enable the verification of the backed up database. Note that not all backups have to be verified, but it is recommended that you perform at least one verified backup per day. Also, verifications can be performed through scheduled maintenance jobs after the backup job is completed.
 - **Verification server or verification server group** – Select one or more database server used for verifying the backed-up database. By default, the SQL Server whose data you want to back up is used. You can click the **New Verification Server or Verification Server Group** link in the drop-down list to create a new verification server or verification server group. For more information, refer to [About the Verification and Index Policy](#).

***Note:** If the version of SnapManager for SQL Server is 7.2 or later, the verification for the database backups in different SQL instances will be performed in parallel concurrently.
 - **Assign Mount Point** – If you do not want to use the default mount point directory, use this option to specify the mount point directory on which a backup set will be mounted during database verification. For example: **C:\mountpoint**.
3. **Check Old Backups to Be Deleted** – If a retention rule is enabled for the selected storage policy and the **Check Old Backups to Be Deleted** function is enabled, DocAve 6 looks to see if former snapshots from this plan have been manually deleted by the user accidentally. For those accidentally deleted snapshots, DocAve 6 ensures that deleted snapshot data cannot be selected to restore in the **Data Selection** interface of the **Restore** wizard..
4. **Transaction Log Backup & Truncation** – If the **Run transaction log backup after full database backup** option is selected, this option backs up and truncates the **transaction** log after a Full

database backup. By default, this option is selected. Note that the transaction log backup is skipped for databases in simple recovery mode.

5. **Back up Stub Database for Selected Scope** – Choose whether or not to back up the stub database along with the contents you have selected to back up. This option allows users to perform granular-level restores of stubs from a backed-up stub database.
6. **Back up BLOB for Selected Scope** – This option backs up BLOB content generated by Storage Manager and files in the connected path of Connector. Select the corresponding checkboxes if you wish to back up this BLOB data.

***Note:** To back up BLOB data generated through the **Leave a stub in SharePoint for each document (uses Storage Manager)** feature of Archive Manager, select the **Back up Storage Manager BLOB** option. If BLOB data generated through Archive Manager is selected in the backup scope, selecting the **Back up Storage Manager BLOB** option will also back up Archive Manager BLOB data with Storage Manager BLOB data during the backup job.

7. **Back up Web Front-End Servers in Parallel** – Note that backing up Web front-end servers in parallel may overload the Media service. If you select the **Back up Web Front-End servers in parallel** option, you are required to specify the maximum number of Web front-end servers to back up in parallel.

***Note:** The following recommendations assume that your network bandwidth is 60 MB/s):

If the content under the **Extra File System Folder** node exceeds **1 GB**, **3** or **4** is a recommended maximum number.

If your content under the **Extra File System Folder** node does not exceed **1 GB**, the maximum number can be larger because the average backup rate is less than **1 MB/s**.

8. **Refresh SharePoint Farm Topology** – This feature refreshes the SharePoint farm topology before starting a backup job and updates the backup scope in the Platform Backup for NetApp Systems plan. Leverage this option if you have strict change management policies for SharePoint. Refreshing the farm topology causes DocAve 6 to use the current state of the farm, as determined by SharePoint Central Administration, to define the scope of the selected nodes in this plan. The plan assumes that any changes to a farm's services, server layout, or Web applications and databases from the previous job are expected, so these changes are not logged as exceptions in the job details. After selecting the **Refresh SharePoint farm topology before starting backup job** option, the **Verify storage layout** option appears. Select this option to verify the storage layout before running a backup plan.

***Note:** Leveraging this option will not reveal VMs in your farm topology.

9. **Granular Index Method** – Choose how to generate the granular index. Sequential generates the index one database at a time on each SQL Server, thereby minimizing the resource requirements. **Parallel** generates the index for multiple databases simultaneously on each SQL Server. If you select **Parallel**, DocAve 6 will by default generate (at most) five database indices at the same time on a SQL Server. To change the maximum number of indices to generate simultaneously, refer to [Configuring the Maximum Number of Database Indices to Generate in Parallel](#).

10. **Check Agent Account Permissions for Backup** –Select **Yes** to check the Agent account permissions for backup in the backup job. If you are sure that your Agent Account is granted the required permissions for using Platform Backup and Restore for NetApp Systems, select **No** to skip this process. Skipping this process may result in faster job times. If the job fails because of insufficient permissions of Agent account, the backup job report will show the details.
11. **Job Report** – Choose the level of reporting for the backup job. **Simplified** creates a summary of the backup data. **Detailed** creates a full list of all backup objects at the cost of performance. If you select Storage Manager or Connector BLOB data for backup, the **BLOB Details** tab will be shown in the Job Monitor **Job Details** interface.
12. **Remember these settings** – Select **Yes** to remember these settings for the future usage when the current user performs any backup jobs. Otherwise, select **No**.

Refer to the section below for details of the settings on the **Advanced** tab:

1. **BLOB Settings**– Select which options to perform on the device that stores the original BLOB data after the BLOB backup completes. The SnapMirror/SnapVault destination of the device that stores the original BLOB data will be updated.
2. **Farm Component Settings**– Configure the SnapMirror-/SnapVault-related settings for the backed-up databases and index components.
 - a. **SnapMirror** – Choose the operations to perform on the SnapMirror destination after completion of the database and index components backup.
 - **Update SnapMirror after operation** – If you are using backups that reside on volumes configured as SnapMirror sources, this option updates the SnapMirror destination after the backup operation is complete.
 - **Verify on available SnapMirror destination volumes** – Use this option to verify the database and index components on the SnapMirror destination volume.
 - b. **SnapVault** – Choose the operations to be performed on the SnapVault storage system after completion of the database and index components backup.

***Note:** SnapVault is an option of NetApp Data ONTAP; if you are using the SMSQL 6.x, ensure that you have set up the Protection Manager Datasets via SMSQL 6.x.

***Note:** Prior to using this option in a backup plan, the SnapVault datasets must have already been created by SMSQL and in a conformant state. For more information on configuring the SnapVault datasets, refer to the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

***Note:** If you are using clustered NetApp Data ONTAP 8.2 or later, you can directly configure SnapVault on the clustered storage systems through SMSQL 7 to make it available for DocAve. If you are using 7-Mode of NetApp Data ONTAP 8.2 or earlier (for example, NetApp Data ONTAP 7.x), you must use DFM to configure SnapVault for availability in DocAve.

- **Archive backup to secondary storage** – Select whether you want to retain backups at the archived location on an **Hourly, Daily, Weekly, Monthly, or Unlimited** basis.

- **Verify archive backup on secondary storage** – Use this option to verify the database and index components archived at the secondary storage system.
 - c. **Scripts** – If you select the **Run command with operation** option, the **Backup** operation command profile type will be listed in the drop-down list. Select a command profile from the drop-down list; the commands will be run according to the command profile you selected. You can also click the **New Command Profile** link in the drop-down list to create a new command profile. For more information, refer to [About Command with Operation](#).
3. **Storage Policy Settings** – Select which options to perform on the device configured in the storage policy after the backup operation completes. The SnapMirror/SnapVault destination of the device configured in the storage policy will be updated.
 4. **Backup Replica Settings** – Configure the backup settings for the replicas in the AlwaysOn Availability Group.

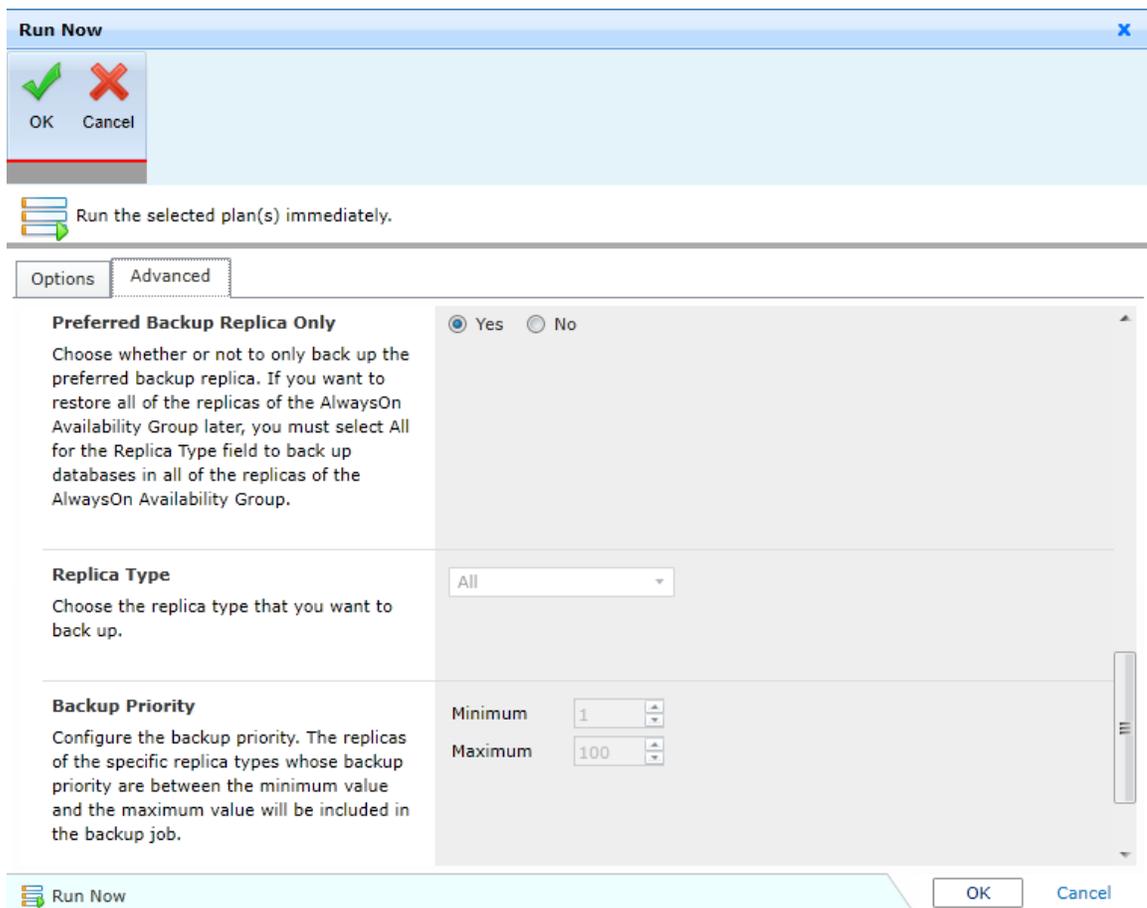


Figure 21: Configuring Backup Replica Settings.

- **Preferred Backup Replica Only** – Select **Yes** if you want to back up only preferred backup replica.

If you select **No**, proceed to designate the replica type and backup priority of the replicas you want to back up:

- **Replica Type** – Choose to back up all of the replicas, all of the primary replicas, or all of the secondary replicas in the AlwaysOn Availability Group. Select **All**, **Primary**, or **Secondary** from the **Replica Type** drop-down list.
 - **Backup Priority** – Configure the Minimum and Maximum value of the backup priority to back up the replicas whose backup priority is in between.
5. **Remember these settings** – Select **Yes** to remember these settings for the future usage when the current user performs any backup jobs. Otherwise, select **No**.

Generating an Index

Use the **Generate Index** feature to generate for the first time a granular index for a selected database, or to replace an existing corrupted index. You can mount the temporary database to one or more index servers during index generation.

***Note:** The default maximum number of snapshots that can be cloned as a group for index generation is **5**. The default maximum number of databases to generate index in parallel is **5**. To configure a desired maximum number for cloning snapshots or generating index, refer to [Configuring the Maximum Number of Snapshots Cloned for Index Generation](#) and [Configuring the Maximum Number of Database Indices to Generate in Parallel](#).

To generate index, complete the steps below:

1. Select the **Restore** tab and click **Generate Index** in the **Manage** group. The **Generate Index** tab appears.

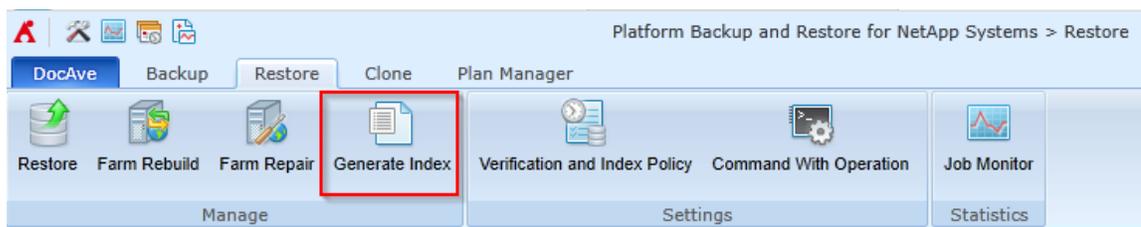


Figure 22: Selecting the Generate Index button on the Restore tab.

2. Configure the options in the **Filter By** area to limit the scope of backup data. By default, all of the backup jobs that were run within the last 7 days are displayed.
 - a. **Filter by Plan** – Filter the backup data by plan information using the drop-down list.
 - **Farm** – Select a farm from the drop-down list to display all plans for that particular farm. Select **All Farms** to display all plans for all farms.
 - **Plan Name** – Select the plan that you want to display from the drop-down list. Select **All Plans** to display all plans.
 - **Restore Granularity Level** – Select the restore granularity level from the drop-down list; only the backup jobs that support the selected restore granularity levels are displayed. Select **All Levels** to list backup jobs for all levels.
 - b. **Filter by Time Range** – Filter backup data by **completion** time range using the drop-down list.
 - **All Jobs** – Select this option to display all **Finished/Finished with Exception** Platform Backup for NetApp Systems jobs.
 - **Backup jobs start within ...** – Select this option to select a time period. All of the **Finished/Finished with Exception** Platform Backup for NetApp Systems jobs whose start time is in the entered time period are displayed.

3. After selecting the filters, click the **Filter** button in the **Filter By** area or on the ribbon. All backup jobs that meet the selected filter rules are listed in the calendar. If desired, click **Reset** in the **Filter By** area or click **Reset** on the ribbon to clear all filters and display all **Finished/Finished with Exception** Platform Backup for NetApp Systems jobs.
4. Select the backup job that contains the desired databases. Additional actions that can be performed:
 - Place the mouse cursor over a backup job to display job information such as the **Plan Name, Job ID, Restore Granularity Level, Index Status, Job Status** and **Data Import**. Click **Day, Week, or Month** to change the view to see all the available jobs during that time period.
 - Click the page turning button   on the top-left corner of the calendar to turn the page.
5. Click **Next**. The **Data Selection** interface appears.
6. Expand the **Backup Data** tree to select the desired Web application or content database. The current index level is displayed beside the corresponding database. Select the content databases to generate granular index.
7. Click **Next**. The **Index Settings** interface appears.
8. **Index Level** – Select from the drop-down list the granular index level.
9. **Clone Database Option** – Choose to use non-production resources for creating the database clone by leveraging either the SnapMirror destination or SnapVault destination.
 - **Clone database on SnapMirror destination** – Select this option to clone a database based upon the Snapshot copy on the SnapMirror destination volume.
 - **Clone database on SnapVault destination** – Select this option to use a remote backup to perform the cloning operation. Snapshots saved in SnapVault primary storage are considered Local Backups, and snapshots saved in SnapVault secondary storage are considered Remote Backups.
10. **Index Conflict Resolution** – Select an index conflict resolution. If generating a more granular-level index than your current index level, DocAve 6 will automatically re-index the database. If the selected index level is less granular than the current index level:
 - **Skip** keeps the current index level.
 - **Replace** removes the existing index and generates a new granular index for the database.
11. **Granular Index Method** – Choose how to generate the granular index. **Sequential** generates the index one database at a time on each SQL Server, minimizing the resource requirements for generating an index. **Parallel** simultaneously generates the indices for multiple databases on each SQL Server. If you select **Parallel**, by default, there will be at most five databases generating index at the same time on a SQL Server. To change the maximum number of indexes you can generate simultaneously, refer to [Configuring the Maximum Number of Database Indices to Generate in Parallel](#).

12. **Index Policy**– You can use the SQL Server where the database resides to mount a temporary database for index generation, or you can use a configured index server or index server group to mount the temporary database for the index generation. Select **New Index Policy** from the drop-down list to create a new verification and index server or group to mount temporary database for index generation. For details, refer to [About the Verification and Index Policy](#).
13. **Assign Mount Point** (Optional) – If you do not want to use the SQL Server default mount point or the mount point directory of the selected index server or group, you can manually enter a desired mount point path here.
14. Click **Next**. The **Notification** interface appears.
15. **Notification** – Configure the e-mail **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list, or create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.
16. When finished, click **Next**. The **Overview** page appears.
17. Review and edit the job selections as needed. To make changes, click **Edit** in the middle of the row.
18. Click **Finish** to save the configuration and run the job immediately.

Checking the Generate Index Job Status

The Generate Index job can be found in the **Platform Maintenance Manager for NetApp Systems** module with a Job ID that starts with **PM**. For details on managing and viewing job information and details, refer to [DocAve 6 Job Monitor Reference Guide](#).

After generating a granular index using the **Generate Index**, the **Index Status** of the applicable backup job will be **Regenerated** or **Successful**.

- **Regenerated** – If you selected to generate an index for at least one of the successfully backed-up databases in this backup job, and at least one index was successfully generated, the **Index Status** for this backup job will be **Regenerated**.
- **Successful** – In this case, the Generate Index job must have the following requirements.
 - All of the databases that were successfully backed up in this backup job are selected to generate an index whose level is equal to or more granular than the current index level.
 - All of the selected databases have successfully generated the granular index.

Configuring the Maximum Number of Snapshots Cloned for Index Generation

Use the **SP2010PlatformConfiguration.xml** file to configure the maximum number of snapshots cloned for index generation.

***Note:** Both the SharePoint 2010 environment, SharePoint 2013 environment, and SharePoint 2016 environment use this same configuration file.

On the SQL Server that contains the database, find the **SP2010PlatformConfiguration.xml** file in the Agent installation directory (...*AvePoint\DocAve 6\Agent\data\SP2010\Platform*). Then, configure the following attribute:

```
<MaxCloneCountConfig MaxCloneCount="5"/>
```

The default value is “5”, which indicates that at most five snapshots will be cloned in sequential order as a group to generate index. After the index generation completes, the cloned snapshots are deleted. The next five snapshots will be cloned and will go through the same process for the next index generation.

Configuring the Maximum Number of Database Indices to Generate in Parallel

Use the **SP2010PlatformConfiguration.xml** to configure the maximum number of databases to generate index in parallel.

***Note:** Both SharePoint 2010 environments, SharePoint 2013 environments, and SharePoint 2016 environments use this same configuration file.

On the SQL Server that contains the database, find the **SP2010PlatformConfiguration.xml** file in the Agent installation directory (...*AvePoint\DocAve 6\Agent\data\SP2010\Platform*). Then, configure the following attribute:

```
<GenerateIndexConfig GenerateIndexMaxThreadCount="5"/>
```

The default value is “5”, which indicates that at most, five databases will be simultaneously performing index generation.

Performing a Restore

A Platform restore can be performed only on snapshots backed up using DocAve Platform Backup and Restore for NetApp Systems. Note that if you configured your storage volume to automatically delete older Snapshot copies, deleted backups cannot be selected to perform a restore.

Before building a restore plan, refer to [Restore Details for Specific Farm Components](#) for important information regarding the restore of farm components.

***Note:** A restore job cannot be run at the same time as a backup job. However, you can perform simultaneous backup and restore actions if the actions are on separate SQL instances.

There are two restore levels available:

- **Database Level** – Under the **Backup Data** pane, the SharePoint farm structure is displayed. Multiple farm components, such as Web applications, content databases, service applications, or even the entire farm and its settings, can be selected for restoration.
- **Granular Restore Level** – If granular indexing options were selected during backup, individual site collections, sites, libraries, lists, folders, items, or file/item versions can be restored from the content databases after clicking the **View Details** link on the top-right corner of the **Backup Data** pane. You can also search for the content to be restored by clicking **Advanced Search** on the ribbon and search using the entered criteria.

The following are the types of restore that can be performed:

1. **In place restore** (at [database level](#) or [granular restore level](#)) – Restores the selected backed-up data to its original location in SharePoint.
2. **Out of place restore** (at [granular restore level](#)) – Restores the selected backed-up data to another location in the original SharePoint farm or another SharePoint farm (other than the original location).

***Note:** Before performing an out of place restore of granular content to another location in the same SharePoint farm, make sure the SQL alias points to the same SQL instance in the backup and restore process. If you are about to perform an out of place restore of granular content to another SharePoint farm, make sure there is no SQL alias in the destination that has the same name as the source SQL alias. Ensure that the destination SQL alias points to a different SQL instance.

If you perform an out of place restore using the **Restore from alternate storage location** restore type, use the `clone-backup` cmdlet in SnapManager for SQL Server to clone the temporary database to the desired SQL instance, and make sure the destination farm can successfully connect to the database using the designated SQL alias name.

***Note:** For information regarding the SharePoint components supported in Platform Backup and Restore for NetApp Systems, refer to [Appendix D: Supported SharePoint Components](#).

***Note:** The account of the Platform Backup and Restore for NetApp Systems Agent that is installed on the SharePoint Central Administration server must be the **Administrator** of a selected site collection in order to restore the corresponding site administration-level search scope.

Building a Restore Plan

The procedure for building in place and out of place restore plans is identical for both until the **Restore Type** step. Follow the instructions below for all restore types, and then skip to the section appropriate to your plan type.

1. Select the **Restore** tab and click **Restore** in the **Manage** group. The **Time-based Restore** tab appears.
2. Configure the options in the **Filter By:** area to limit the scope of backup data. By default, all backup jobs started within the last 7 days are displayed.
 - a. **Filter by Plan** – Filter the backup data by plan information using the drop-down list.
 - **Farm** – Select a farm from the drop-down list to display all plans for that particular farm. Select **All Farms** to display all plans for all farms.
 - **Plan Name** – Select the plan that you want to display from the drop-down list. Select **All Plans** to display all plans.
 - **Restore Granularity Level** – Select the restore granularity level from the drop-down list; only the backup jobs that support the selected restore granularity levels are displayed. Select **All Levels** to list backup jobs for all levels.
 - b. **Filter by Time Range** – Filter backup data by **completion** time range using the drop-down list.
 - **All Jobs** – Select this option to display all **Finished/Finished with Exception** Platform backup jobs.
 - **Backup jobs start within ...** – Select this option to select a time period. All of the **Finished/Finished with Exception** Platform backup jobs whose start time is in the selected time period are displayed.
3. After selecting the filters, click the **Filter** button in the **Filter By:** area or on the ribbon. All backup jobs that meet the selected filter rules are listed in the calendar. If desired, click **Reset** in the **Filter By:** area or click **Reset** on the ribbon to clear all filters and display all Finished/Finished with Exception Platform backup jobs.
4. Select the backup job that you want to restore by clicking the job. Additional actions that can be performed:
 - Place the mouse cursor over a backup job to display job information such as the **Plan Name, Job ID, Restore Granularity Level, Index Status, Job Status** and **Data Import**. Click **Day, Week, or Month** to change the view to see all the available jobs during that time period.

- Click the page turning button   on the top-left corner of the calendar to turn the page.
5. Find the desired site collections in the farm using the **Find Site Collection** feature. Enter the keywords of the site collection URL or combine the keywords with wildcards.
 6. Now that you selected a backup job containing data you want to restore, click the link applicable to your type of restore to continue with instructions on building the job:
 - [Building a Restore Plan at Database Level](#)
 - [Building an In Place Platform Granular Restore Plan](#)
 - [Building an Out of Place Platform Granular Restore Plan](#)
 - [Restoring from an Alternate Storage Location](#)
 - [Cloning Web Applications for Restore](#)
 - [Restoring Backed-Up Web Front-End Files](#)
 - [Restoring Backed-up BLOB Data](#)
 - [Restoring Backed-up Stub Database](#)
 - [Restoring Backed-Up Catalog Site Collection](#)
 - [Restoring Backed-up Database Master Key](#)

Building a Restore Plan at Database Level

To build and run an in place restore job at the database level:

1. Follow the instructions given in [Performing a Restore](#) to begin building the plan.
2. **Data Selection** – Expand the farm tree, and select the content you want to restore. The content in the tree will vary depending upon the type of backup selected. In this case, select a content database to restore. You can use the **Find Site Collection** feature to search for your desired site collections. For more details, refer to [Appendix A: About Find Site Collection](#).
3. **Restore Type** – Choose how the content will be restored.
 - **Restore Type** – Select one restore type from the three types below.
 - **Restore to original farm** – Use this option to restore the databases to the original farm with the specified configurations.
 - **Restore from alternate storage location** – Use this option to restore the databases from the alternate storage location by manually restoring the databases in SMSQL. For more information, refer to [Restoring from an Alternate Storage Location](#).
 - **Clone to another farm** – Use this option to clone the selected databases with the associated BLOB data and stub database. Select a destination farm from the **Destination Farm** drop-down list. For more information, refer to [Cloning Web Applications for Restore](#).
 - **Agent Group** – Select the Agent group that will perform the restore job. Click **View** to view the details of the selected Agent group.

***Note:** If your environment has a DMZ, make sure all of the Agents in the Agent group are in the same LAN as DocAve 6 Manager, and can communicate with SQL Server and Media Server.
4. **Snapshot Selection** – Click **Load Remote Backups** on the ribbon to load the remote snapshots in SnapVault. After the remote backups are loaded in the tree, select local or remote snapshots for the selected content database. Click **View Details** next to the snapshot to view the content databases. Make sure that all of the selected content databases have the corresponding local or remote snapshots selected.

***Note:** Databases, BLOB data, and granular data can be restored from the remote snapshot in SnapVault secondary storage. Web front-end data cannot be restored from the remote snapshot in SnapVault secondary storage.
5. **Restore Settings** – Choose detailed settings for the restore job.
 - a. **Restore Database to Most Recent State** – With this option enabled, the database is restored together with any recent modifications that were made after the latest database backup. DocAve 6 first restores the backed-up database, and then modifies the database to its most recent status by applying all of the backed-up transaction logs to the restored database. Select **No** to restore only the backed up database.

To use this option, you must select the most recent backup data. If this option is not used, a point-in-time restore is performed, which creates multiple recovery paths for the database. A later up-to-the-minute restore using the same backup data will fail. In that case, the SnapManager for Microsoft SQL Server interface can be used for up-to-the-minute restores. For more information, refer to [Restoring a Database to a Point in Time](#).

- b. **Restore Database Only** – If **Yes** is selected, the selected databases are restored with no attempt to connect them to the SharePoint environment. This is useful when a SharePoint environment has not yet been set up (for example, during a whole farm restore). This can also be useful when performing manual steps to bring up or down a specific environment after the database has been restored. If you select **No**, the database is connected to the SharePoint farm normally after the restore.

***Note:** Configuration databases and Central Administration databases can only be restored when this option is selected.

- c. **Replica Restore Options** – Choose to restore only one of the backed up replicas at random, or to restore all of the replicas of the AlwaysOn Availability Group.
 - **Only restore one replica** – With this option selected, only one of the backed up replicas will be used at random for restore. This replica will be connected while databases are accessed from SharePoint after this restore job.
 - **Restore all of the replicas** – With this option selected, all of the backed up replicas will be restored and the databases will be synchronized across the replicas in the AlwaysOn Availability Group. The original availability group listener will still be connected while databases are accessed from Share Point. To select the **Restore all of the replicas**, you must have backed up all of the replicas of the AlwaysOn Availability Group.

***Note:** If the Primary replica of the AlwaysOn Availability Group is not backed up, the AlwaysOn Availability Group will fail over during the restore. At random, one of the Secondary replicas will be set to Primary, which will be connected while database s are accessed from SharePoint.

- d. **Conflict Resolution** – Select whether or not to overwrite the database contents if there is a conflict between the original database name and that of the backed-up database.
 - **Skip** – If a selected database in the backup has the same name as a database in the original farm, then the selected database in the backup is not restored.
 - **Overwrite** – If a selected database in the backup has the same name as a database in the original farm, then the original database is deleted first and the database in the backup is then restored.
- e. **Verify Backup Data Before Restore** – Choose whether to verify the backup data before a restore operation and then configure the corresponding settings.

- **Verify Backup** – This option enables you to verify backup data before restoring it to ensure that the restore is successful. Select this option enables the following settings.
 - **Verification server or verification server group** – Select one or more verification servers used for verifying the backed up database. By default, the SQL Server whose database you want to restore is used. You can click the **New Verification Server or Verification Server Group** link in the drop-down list to create a new verification server or server group. For more information, refer to [About the Verification and Index Policy](#).

***Note:** If the version of SnapManager for SQL Server is 7.2 or later, the verification for the database backups in different SQL instances will be performed in parallel concurrently.
 - f. **Run Command With Operation** – If you select the **Run command with operation** option, the command profile of the **Restore** operation type will be listed in the drop-down list. Select a command profile from the drop-down list. The commands will be run according to the command profile you selected. You can also click the **New Command Profile** link in the drop-down list to create a new command profile. For more information, refer to [About Command with Operation](#).
 - g. **Notification** – Configure the e-mail **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list, or create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.
6. When finished configuring **Restore Settings**, click **Next**. The **Schedule** page appears.
 7. **Schedule** – Choose whether or not to run the restore job based on a schedule.
 - Select **Restore immediately after wizard finishes** to run the job immediately after finishing the restore wizard.
 - To configure the schedule yourself, select **Configure the schedule myself** and input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.
 8. When finished, click **Next**. The **Overview** page appears.
 9. Review and edit the job selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
 10. Click **Finish** to save the job's configuration.
 - If the restore job does not have a schedule, **Finish** runs the job immediately.
 - If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Building an In Place Platform Granular Restore Plan

1. Follow the instructions given in [Performing a Restore](#) to begin building the plan.
2. **Data Selection** – Expand the farm tree, and configure the following settings:
 - a. Select the database that includes the granular content you wish to restore.
 - b. Click the **View Granular Contents** link next to the selected content database to view backup details about the selected database. For details on searching granular data using the **Advanced Search** feature, refer to [Appendix B: About Advanced Search](#).
3. You can navigate directly to the **Backup Data** tab to expand the granular data tree; the backup tree's stored index will be used to load the backup data tree. Select your desired granular level nodes to restore. If no stored index is detected, DocAve will instruct you to select the **Browse the index from backup data** option to continue loading the tree.

Alternatively, you can click the **Global Setting for Restoring Content, Property and Security** link at the top of the **Data Selection** interface and configure the **Item Level Settings**:

View the backup details of the selected database: WSS_Content_1700_a(ZEN13SQLC0404)
You can switch [back](#) to view the SharePoint components tree.

^ [Global Setting for Restoring Content, Property, and Security](#)

- Item Level Settings	
Restore Granular Content Choose whether or not to restore granular content (from the site collection level down to the item version level).	<input checked="" type="checkbox"/> Restore Granular Content
Browse Method Browse the index from backup data: Use the stored index of the backup data to browse the tree. Select a previously created index policy. The SQL instance you have configured in the selected index policy will be used for backup data. Select Default to use the SQL instance whose databases will be backed up. Choose to use non-production resources for creating the database clone by leveraging either the SnapMirror destination or SnapVault destination. Granularity of the stored index data: None Level	<input checked="" type="checkbox"/> Browse the index from backup data Specify an index policy for browsing the tree: Default <input type="checkbox"/> Clone database on SnapMirror destination <input checked="" type="checkbox"/> Clone database on SnapVault destination
Container Selection Check the checkbox to enable the container restore selection, and then choose to restore the container's property or security.	<input type="checkbox"/> Global settings for container configuration <input type="radio"/> Restore container <input type="radio"/> Only restore security
Content Selection Check the checkbox to enable the content restore selection, and then choose whether to restore the content's security.	<input type="checkbox"/> Global settings for content configuration <input type="radio"/> Restore content <input type="radio"/> Only restore security

Backup Data

Farm(ZEN13SQLC0404:SHAREPOINT_CONFIG_13SP1)

Figure 23: The Global Setting for Restoring Content, Property and Security link.

- **Restore Granular Content** – Select this option to restore granular content. If you are browsing the tree to load content under site collections, the **Restore Granular Content** option is automatically selected to enable the restore of the granular contents under the site collection level. If you deselect the **Restore Granular Content** option, the tree is reloaded and you can only browse the tree to the site collection level. For details, refer to [Deselecting the Restore Granular Content Feature](#).

***Note:** Restoring granular content will change the GUIDs of files and items. To keep the original GUIDs of the files and items intact, run a restore job at the database level or run a site collection-level restore job with the **Restore Granular Content** option deselected.

- **Browse Method** – Choose whether or not to browse the tree from the index generated from the backup data. The current granular level of your stored index is displayed in bold on the left side of the interface.

- **Browse the index from backup data** – A SharePoint content database backup snapshot will be mounted as a temporary database. Users can then browse and restore specific granular content. Note that the tree is generated in real time and can be displayed down to the item version level regardless of the database's original restore granularity.

By default, the mounted temporary database is stored on the default index server. To choose another index server, select a pre-defined index policy from the drop-down list, or click the **New Index Policy** link in the drop-down list to create a new index server or server group. For more information, refer to [About the Verification and Index Policy](#).

Additionally, you can use non-production resources for mounting the temporary database for indexing. This is done by leveraging either the SnapMirror destination or SnapVault destination storage. If the index policy is set to **Default**, the SnapMirror/SnapVault destination will be used to mount the temporary database. If you selected a custom index policy, the temporary database is generated from the SnapMirror/SnapVault destination and will be mounted to the selected index server.

- **Container Selection** – Select the **Global setting for container configuration** checkbox to enable the container's global settings.
 - **Restore container** – Select this option to restore the containers in the selected backup data. Select the **Security** checkbox if you want to restore the container's security settings, and/or select the **Property** checkbox if you want to restore the container's property settings. For more information, refer to Appendix A.
 - **Only restore security** – Select this option to restore only the container's security settings. You can select the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security of the container in the backup to the conflict container in the destination. **Replace** will delete the security of the conflict container in the destination first, and then add the security of the container in the backup to the conflict container in the destination.

***Note:** The **Only restore security** feature takes effect only if the selected nodes do not inherit security from their parent nodes.

***Note:** Once you select the **Only restore security** option, the **Container level conflict resolution** configuration field in the **Restore Settings** page will only

display **Skip** and you will not be able to configure the other Container level conflict resolutions through that page.

- **Content Selection** – Select the **Global setting for content configuration** checkbox to enable the content’s global settings.
 - **Restore content** – Select this option to restore content in the selected backup data. Select the **Security** checkbox to restore the content’s security settings as well.
 - **Only restore security** – Select this option to restore only the content’s security settings. You can select the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security settings of the content in the backup into the conflict content in the destination. **Replace** will delete the security settings of the conflict content in the destination first, and then add the security of the content in the backup to the conflict content in the destination.

***Note:** The **Only restore security** feature takes effect only if the selected nodes do not inherit security from their parent nodes.

***Note:** Once you select the **Only restore security** option, the **Content level conflict resolution** configuration field in the **Restore Settings** page will display **Skip** only. You will not be able to configure other Content level conflict resolutions through that page.

4. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the popped up **Item Browser** window. Select the configuration of the container/content being restored.

- a. **Security** – Refer to [Appendix F: SharePoint Object Security and Property](#).
- b. **Property** – Refer to [Appendix F: SharePoint Object Security and Property](#).

5. When finished, click **Next**. The **Stub and BLOB Configuration** page appears.

***Note:** The **Stub and BLOB Configuration** page is available when the selected backup data for a granular level restore contains stubs. Configure the **Stub Database Settings** and **BLOB Settings** to choose to restore granular data from the backed-up stub database/BLOB data or from the original Storage Manager/Connector devices.

6. **Stub Database Settings** – Choose whether or not to restore the granular data from the backed-up stub database in the **Use Backed up Stub Database** field.

- Select **Yes** to restore the granular data from the backed-up stub database. If you select **Yes**, you are required to select which backup method you used.
 - **Default Platform Backup** – Use the stub database that has been backed up by a Platform Backup for NetApp Systems job.

- **Other/Third Party Backup** – Select this option if the stub database was backed up by other/third party tools, and you must manually restore and stage the stub database onto the destination SQL Server.
 - **Database Access Credentials** – Enter the SQL instance name where the stub database resides and the stub database name. Select the database authentication to use to access the customer backed up stub database.
 - Select **No** to restore the stubs from the original Storage Manager/Connector devices.
7. **BLOB Settings** – Choose whether or not to restore the granular data from the backed up BLOB data.
- Select **Yes** to restore the granular data from the backed up BLOB data. If you select **Yes**, you are required to select which backup method you used.
 - **Default Platform Backup** – Use the BLOB data that has been backed up by Platform Backup job to restore.
 - **Other/Third Party Backup** – Select this option if the BLOB data was backed up by other/third party tools, and you must manually restore the BLOB data to a location that must be configured as a logical device.
 - **Logical Device** – Select the logical device where the BLOB data has been staged from the Logical device drop-down list.
 - Select **No** to restore the granular data from the original Storage Manager/Connector devices.
8. Click **Next**. The **Restore Type** page appears.
9. **Restore Type** – Choose how the content will be restored.
- a. **Restore Type** – Select the location where to restore the backup data. In this case, select **In place restore** to restore the selected content to its original SharePoint location.
 - b. **Restore From Alternate Storage Location** – Use this option to restore the data from an alternate storage location by manually cloning the databases in SMSQL. For more information, refer to [Restoring from an Alternate Storage Location](#).
 - c. **Agent Group** – Select the Agent group that will perform the restore job. Click **View** to view the details of the selected Agent group.
- *Note:** If your environment has a DMZ, make sure all of the Agents in the Agent group are in the same LAN as DocAve 6 Manager, and can communicate with SQL Server and Media Server.
10. Click **Next** when finished. The **Restore Settings** page appears.

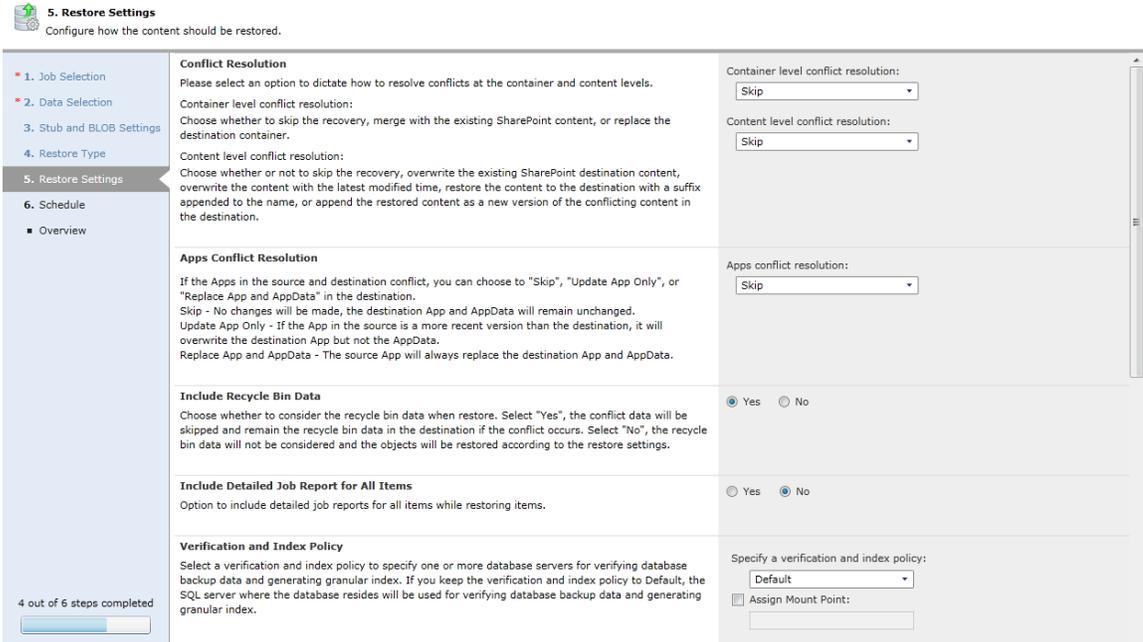


Figure 24: Configuring restore settings (1).

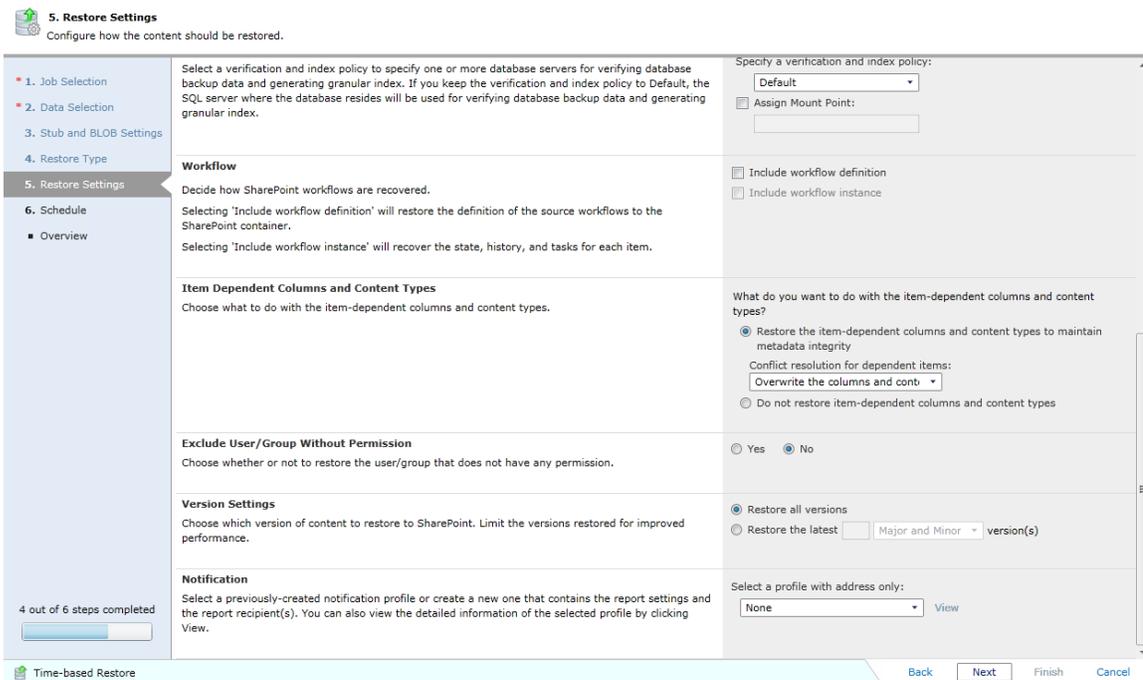


Figure 25: Configuring restore settings (2).

11. Restore Settings – Configure how the content will be restored.

- a. **Conflict Resolution** – Select the action to dictate how to resolve the container level and content level conflicts that arise during a Platform granular restore for NetApp Systems.

- **Container level conflict resolution** – Set the conflict resolution on the site collection, site, list, and folder levels.
 - **Skip** – Ignores the source container that conflicts with the destination one.
 - **Merge** – Combines the configuration of the source and destination containers. If there is a conflict, the source configuration overwrites the destination’s configuration.
 - **Replace** – Deletes the destination container and then restores the source container to the destination. If the selected container is a top-level site, Replace function empties the top-level site instead of deleting it and restores the source top-level site to the destination. This option can only be used at folder/list/library/site/site collection level.

***Note:** As the **Replace** conflict resolution deletes the destination container before performing the restore, make sure the destination container is no longer needed before performing the restore using this conflict resolution.
- **Content Level Conflict Resolution** – Set the conflict resolution on the item level.
 - **Skip** – Ignores the source item/document that has the same item ID/document name as the destination item/document.
 - **Overwrite** – Copies the source item/document to the destination by overwriting the destination item/document with same item ID/document name.
 - **Overwrite by Last Modified Time** – Keeps the conflict item/document which has the latest modified time and overwrites the older one.
 - **Append an Item/Document with a Suffix** – Keeps both of the conflict items/documents and adds a suffix (_1, _2, _3..) to the name of the conflict source item/document.

***Note:** This option is only valid for users uploaded documents.
 - **Append a New Version** – Adds the conflict source item/document to the destination as a new version of the conflict destination item/document.
- b. **Apps Conflict Resolution** – Define the conflict resolution behavior that occurs if there is a conflict with Apps in the source and destination. Choose **Skip**, **Update App Only**, or **Replace App and AppData** from the drop-down list. To successfully restore SharePoint Apps, make sure that the Agent account to perform the restore job is not a **Local system account**.
 - **Skip** – Ignores the source App that has the same name as the destination one.
 - **Update App Only** – If the source App is a more recent version than the destination one, the destination App is updated, but the original destination AppData remains.

- **Replace App and AppData** – The source App replaces the destination App and AppData, even if it is in an older version.
- c. **Consider the existing data in destination Recycle Bin** – Choose whether to compare the data in the backup with the data in the original SharePoint farm’s recycle bin. If you select **Skip** at the Container level or Content level, or you select **Append an Item/Document Name with a Suffix** or **Append a New Version** at the Content level, the **Consider the existing data in destination Recycle Bin** option is available. If you select **Yes** in this field and the selected content in the backup still exists in the original SharePoint farm’s Recycle Bin, the selected content in the backup is not restored.
- d. **Include Detailed Job Report for All Items** – Selecting **Yes** generates a detailed job report for all of the **items**. Selecting **No** still generates a job report, but only in truncated list form.
- e. **Index Policy**– Select an index policy from drop-down list. Here, you can designate one or more database servers for generating the granular level index. By default, DocAve uses the SQL Server that contains the data you are about to restore.

If you do not want to use the default mount point directory, you can use the **Assign Mount Point** option to specify the mount point directory.

- f. **Workflow** – Decide how the backed-up workflows are **restored**.
 - **Include workflow definition** – Only restores the definition of the backed-up workflows.
 - **Include workflow instance** – Restore the state, history, and tasks for each item.

***Note:** All workflow instances whose status was **In Progress** when backed up will be **Cancelled** when restored to the destination.
- g. **Item Dependent Columns and Content Types** – Choose whether to restore item-dependent columns and content types.

***Note:** If you did not select **Property** beside the selected node in the **Data Selection** step and the dependent column or content type does not exist in the destination, the column or content type will not be restored. If this is the case, use this option to restore them.

- **Restore the item-dependent columns and content types to maintain item integrity** – The item is restored and the dependent column or content type is created in the corresponding list/library. The item still uses the dependent column and content type.
- **Do not restore item-dependent columns and content types** – The item dependent columns and dependent content types will not be restored. When selecting this option, make sure the dependent columns and content types exist in the destination. Otherwise, the item cannot be restored.

- h. **Exclude User/Group Without Permission** – If you select **Yes**, the users/groups that have no permissions will not be restored. By default, **No** is selected.
- i. **Version Settings** – Choose the **Version Settings** for the content being restored to SharePoint. To improve performance, limit the versions restored. **Restore all versions** restores all versions of the backup data; while **Restore the latest version(s)** only restores the latest several **Major** or **Major and Minor** versions of the backup data as designated. The other versions are not restored. Note that the current version will always be restored together with the entered number of **Major** or **Major and Minor** versions.
- j. **Notification** – Configure the e-mail **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list, or choose to create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.

When finished configuring **Restore Settings**, click **Next**. The **Snapshot Selection** page appears.

12. **Snapshot Selection** – Restore granular data from either the local or the remote database snapshot. Click **Load Remote Backups** on the ribbon to load SnapVault remote snapshots. After the remote backups are loaded in the tree, select local or remote snapshots for the selected content database. Click **View Details** next to the snapshot to view the content databases. Make sure that the content database has its corresponding local or remote snapshots selected.

***Note:** Databases, BLOB data, and granular data can be restored from the remote snapshot in SnapVault secondary storage. Web front-end data cannot be restored from the remote snapshot in SnapVault secondary storage.

13. Click **Next**. The **Schedule** page appears.
14. **Schedule** – Choose whether or not to create the restore job based on a schedule. Select **Restore immediately after wizard finishes** to run the job immediately after finishing the restore wizard. If you decide to configure the schedule yourself, select **Configure the schedule myself** and input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.

When finished, click **Next**. The **Overview** page appears.

15. Review and edit the job selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
16. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Building an Out of Place Platform Granular Restore Plan

To build and run an out of place Platform granular restore for NetApp Systems plan:

1. Follow the instructions given in [Performing a Restore](#) to begin building the plan.
2. **Data Selection** – Select the database that includes the granular content to restore. Click **View Granular Content** link on the top right corner of the **Backup Data** pane to view the detailed backup data for the selected database. For details on searching granular data using the **Advanced Search** feature, refer to [Appendix B: About Advanced Search](#).
3. You can navigate directly to the **Backup Data** tab to expand the granular data tree. The backup tree's stored index will be used to load the backup data tree. Select your desired granular level nodes to restore. If no stored index is detected, DocAve will instruct you to select the **Browse the index from backup data** option to continue loading the tree.

Alternatively, you can click the **Global Setting for Restoring Content, Property and Security** link at the top of the **Data Selection** interface and configure the **Item Level Settings**:

- **Restore Granular Content** – Select this option to restore granular content. If you are browsing the tree to load the contents under site collections, the **Restore Granular Content** option will be automatically selected to enable the restore of the granular contents under the site collection level. If you deselect the **Restore Granular Content** option, the tree is reloaded and you can only browse the tree to the site collection level. For details, refer to [Deselecting the Restore Granular Content Feature](#).

***Note:** Restoring granular content will change the GUIDs of files and items. To keep the original GUIDs of the files and items intact, run a restore job at the database level or run a site collection-level restore job with the **Restore Granular Content** option deselected.

- **Browse Method** – Choose whether or not to browse the tree from the index generated from the backup data. The current granular level of your stored index in the backup data be displayed in bold on the left side of the interface.
 - **Browse the index from backup data** – A SharePoint content database backup snapshot will be mounted as a temporary database. Users can then browse and restore specific granular content. The tree is generated in real time and can be displayed down to item version level regardless of the database's original restore granularity.

By default, the mounted temporary database is stored on the default index server. To choose another index server, select a pre-defined index policy from the drop-down list, or click the **New Index Policy** link in the drop-down list to create a new index server. For more information, refer to [About the Verification and Index Policy](#).

Additionally, you can use non-production resources for mounting the temporary database for indexing by leveraging either the SnapMirror destination or SnapVault destination storage. If the index policy is set to **Default**, the

SnapMirror/SnapVault destination storage will be used to mount the temporary database for indexing. If you selected a custom index policy, the temporary database is generated from the SnapMirror/SnapVault destination and will be mounted to the index server.

- **Container Selection** – Select the **Global setting for container configuration** checkbox to enable the container’s global settings. A container refers to site collections, sites, lists/libraries, or folders in SharePoint.
 - **Restore container** – Select this option to restore the container in the selected backup data. Select the **Security** checkbox if you want to restore the container’s security settings, and/or select the **Property** checkbox if you want to restore the container’s property settings.
 - **Only restore security** – Select this option to restore only the container’s security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security of the container in the backup to the conflict container in the destination. **Replace** will delete the security of the conflict container in the destination first, and then add the security of the container in the backup to the conflict container in the destination.

***Note:** The **Only restore security** feature takes effect only if the selected nodes do not inherit security from their parent nodes.

***Note:** Once you select **Only restore security** option, the **Container level conflict resolution** configuration field in the **Restore Settings** page will only display **Skip** and you will not be able to configure the other Container level conflict resolution through that page.

- **Content Selection** – Select the **Global setting for content configuration** checkbox to enable the content’s global settings. Content refers to the documents or files in libraries or items in lists.
 - **Restore content** – Select this option to restore the contents in the selected backup data. Select the **Security** checkbox if you want to restore the content’s security settings as well.
 - **Only restore security** – Select this option to restore only the content’s security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security settings of the content in the backup into the conflict content in the destination. **Replace** will delete the security settings of the conflict content in the destination first, and then add the security of the content in the backup to the conflict content in the destination.

***Note:** The **Only restore security** feature takes effect only if the selected nodes do not inherit security from their parent nodes.

***Note:** Once you select **Only restore security** option, the **Content level conflict resolution** configuration field in the **Restore Settings** page will display **Skip** only.

You will not be able to configure the other Content level conflict resolution through that page.

4. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the popped up **Item Browser** window. Specify the configuration of the container/content being restored.

- **Security** – Refer to [Appendix F: SharePoint Object Security and Property](#).
- **Property** – Refer to [Appendix F: SharePoint Object Security and Property](#)

***Note:** To out-of-place restore a catalog site collection to a destination Web application or site collection, you must configure the following settings:

- a. Select the catalog site collection from the **Backup Data** tree. Use the **Find Site Collection** feature as a quick method. For details, refer to [Appendix A: About Find Site Collection](#).
 - b. Click **Next**. In the **Restore Type** interface, select the **Out of place restore** option.
 - c. In the **Destination** field, select a destination Web application or site collection.
 - d. **Action** – Select how the data will be restored to the destination.
 - **Merge** – If you selected a site collection as the destination, select **Merge**. **Merge** will add the site collection to the destination site collection.
 - **Attach** – If you select a Web application as the destination, select **Attach**. **Attach** will restore the site collection as children beneath the selected Web application.
 - e. In the **Restore Settings** interface, the **Use as App Catalog Site** field is available to configure. Select **Yes** to restore the current site collection as the app catalog site for the destination Web application. Otherwise, select **No**.
 - f. For details on other settings, refer to the information in this section.
5. When finished, click **Next**. The **Stub and BLOB Configuration** page appears.

***Note:** The **Stub and BLOB Configuration** page is available when the backup data selected for a granular level restore contains stubs. Configure the **Stub Database Settings** and **BLOB Settings** to choose to restore granular data from the backed-up stub database/BLOB data or from the original Storage Manager/Connector device.
 6. **Stub Database Settings** – Choose whether or not to restore the granular data from the backed-up stub database in the **Use Backed up Stub Database** field.
 - Select **Yes** to restore the granular data from the backed up stub database. If you select **Yes**, you are required to specify which backup method you used.
 - **Default Platform Backup** – Use the stub database that has been backed up by Platform Backup for NetApp Systems job to restore.
 - **Other/Third Party Backup** – Select this option if the stub database was backed up by other/third party tools (for example, the SQL Server backup method), and

you must manually restore and stage the stub database onto the destination SQL Server.

- **Database Access Credentials** – Enter the SQL instance name where the stub database resides and the stub database name. Specify the database authentication to use to access the customer backed up stub database.
 - Select **No** to restore the granular data from the original Connector device.
7. **BLOB Settings** – Choose whether or not to restore the granular data from the backed up BLOB data.
- Select **Yes** to restore the granular data from the backed up BLOB data. If you select **Yes**, you are required to specify which backup method you used.
 - **Default Platform Backup** – Use the BLOB data that has been backed up by Platform Backup job to restore.
 - **Other/Third Party Backup** – Select this option if the BLOB data was backed up by other/third party tools (for example, the SQL Server backup method), and you must manually restore the BLOB data to a location that must be configured as a logical device.
 - **Logical Device** – Select the logical device where the BLOB data has been staged from the **Logical device** drop-down list.
 - Select **No** to restore the granular data from the original Storage Manager/Connector storage device.
8. Click **Next**. The **Restore Type** page appears.
9. **Restore Type** – Choose how the content will be restored.

***Note:** Platform Restore for NetApp Systems does not support restoring the data backed up from:

- SharePoint 2010 to SharePoint 2013 and SharePoint 2016
- SharePoint 2013 to SharePoint 2010 and SharePoint 2016
- SharePoint 2016 to SharePoint 2010 and SharePoint 2013.

Make sure that the source node and the destination node are in the same version of SharePoint. If the site within SharePoint 2013 is a SharePoint 2010 mode site, it can only be restored to the same mode site.

- a. **Restore Type** – Select the location where to restore the backup data. In this case, select **Out of place restore** to restore the content to another SharePoint farm or a different location in the original farm.
- b. **Restore From Alternate Storage Location** – Use this option to restore data from an alternate storage location by manually cloning the databases in SMSQL. For more **information**, refer to [Restoring from an Alternate Storage Location](#).

- c. **Destination** – Choose the destination for the restore job. You can either select an existing node on the tree or **select** a manually created node. To create a node in the destination SharePoint manually, perform the steps below.

- Select a node with a blank textbox.
- Enter the URL of the destination node into the textbox following the format displayed in the textbox. If you are creating a new site collection, you will be asked to select one existing managed path from the drop-down list.
- Click **Create Container** beside the textbox to create the node in the destination farm. Alternatively, click **Create Container** in the **Manage** group in the **Time-based Restore** tab to create the corresponding node.

To search your desired granular objects (from site collection level down to item level) in the destination farm tree, use the **Advanced Search** feature. You can search your desired objects from the selected destination scope (from the farm to folder level). For more details on the **Advanced Search** interface, refer to [Appendix B: About Advanced Search](#).

- d. **Agent Group** – Select the Agent group that will perform the restore job. Click **View** to view the details of the selected Agent group.

***Note:** If your environment has a DMZ, make sure all of the Agents in the Agent group are in the same LAN as DocAve 6 Manager, and can communicate with SQL Server and Media Server.

- e. **Action** – Select how the data will be restored to the destination, and preview the impact of your selection.

- **Merge** – Adds the contents to the destination node.
- **Attach** – Restores the contents as children beneath the selected nodes.

To preview what the destination node data tree will look like after the job is executed, click **Preview**. Only the unfolded tree structure in the **Data Selection** step can be previewed in the destination tree. Click **Hide Preview** to hide the **Preview** area.

- f. **Mapping Settings** (Optional) – Configure whether to specify the mapping settings to map the user, domain, **displayed** list or column label to the destination.

- **User Mapping** – If desired, configure the user mapping to map the backed up user to the destination user. For specific instructions on setting up the user mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** User Mapping will not function if you configure it with a username that in an e-mail format.

- **Domain Mapping** – If desired, configure the domain mapping to map the backed up domain to the destination domain. For specific instructions on setting up the domain mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).
***Note:** Domain Mapping will not function if you configure it with a fully qualified domain name.
- **Language Mapping** – If desired, configure the language mapping to display a destination node in a different language than the language of the backed-up data. For specific instructions on setting up the language mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

10. Click **Next** when finished. The **Restore Settings** page appears.

11. **Restore Settings** – Configure how the content will be restored.

- a. **Conflict Resolution** – Specify the action to resolve container level and content level conflicts that arise during a Platform granular restore for NetApp Systems.
 - **Container Level Conflict Resolution** – Set the conflict resolution on the site collection, site, list, and folder levels.
 - **Skip** – Ignores the source container that conflicts with the destination one.
 - **Merge** – Combines the configuration of the source and destination containers. If there is a conflict, the source configuration overwrites the destination's configuration.
 - **Replace** – Deletes the destination container and then restores the source container to the destination. If the selected container is a top-level site, Replace function empties the top-level site instead of deleting it and restores the source top-level site to the destination. This option can only be used at folder/list/library/site/site collection level.
***Note:** As the replace conflict resolution deletes the destination container before performing the restore, make sure the destination container is no longer needed before performing the restore using this conflict resolution.
 - **Content Level Conflict Resolution** – Set the conflict resolution on the item level.
 - **Skip** – Ignores the source item/document that has the same item ID/document name as the destination item/document.
 - **Overwrite** – Copies the source item/document to the destination by overwriting the destination item/document with same item ID/document name.
 - **Overwrite by Last Modified Time** – Keeps the conflict item/document that has the latest modified time and overwrites the older one.

- **Append an Item/Document with a Suffix** – Keeps both of the conflict items/documents and adds a suffix (_1, _2, _3...) to the name of the conflict source item/document.

***Note:** This option is only valid for users uploaded documents.
 - **Append a New Version** – Adds the conflict source item/document to the destination as a new version of the conflict destination item/document.
- b. **Apps Conflict Resolution** – Define the conflict resolution behavior that occurs if there is a conflict with Apps in the source and destination. You can choose “**Skip**”, “**Update App Only**”, or “**Replace App and AppData**” from the drop-down list. To successfully restore the SharePoint Apps, make sure the Agent account of the Agent account to perform the restore job is not a **Local system account**.
 - **Skip** – Ignore the source App that has the same name as the destination one.
 - **Update App Only** – If the source App is in a more recent version than the destination one, the destination App will be updated, but with the original destination AppData remained.
 - **Replace App and AppData** – The source App will replace the destination App and AppData, even if it is in a lower version.
- c. **Consider the existing data in destination Recycle Bin** – Choose whether to compare the data in the backup with the data in the destination SharePoint farm’s recycle bin. If you select **Skip** either at the Container level or Content level, or you select the **Append an Item/Document Name with a Suffix** or **Append a New Version** at the Content level, the **Consider the existing data in destination Recycle Bin** option is available to configure. If you select **Yes** in this field and the selected content in the backup still exists in the recycle bin of the destination SharePoint farm, the selected content in the backup is not restored.
- d. **Include Detailed Job Report for All Items** – Selecting **Yes** generates a detailed job report for all the items. Selecting **No** still generates a job **report**, but only in truncated list form.
- e. **Index Policy** – Select an index policy from the drop-down list. Here you can designate one or more database servers for generating the granular level index. By default, DocAve uses the SQL Server that contains the data you are about to restore.

If you do not want to use the default mount point directory, you can select the **Assign Mount Point** option to specify the mount point directory.
- f. **Workflow** – Decide how the backed-up **workflows** are restored.
 - **Include workflow definition** – Only restores the definition of the backed-up workflows.

- **Include workflow instance** – Restores the state, history, and tasks for each item.
 - *Note:** All workflow instances whose status was **In Progress** when backed up will be **Cancelled** when restored to the destination.
 - g. **Item Dependent Columns and Content Types** – Choose whether to restore item-dependent columns and content types.
 - *Note:** If you did not select **Property** beside the selected node in the **Data Selection** step and the dependent column or content type does not exist in the destination, the column or content type will not be restored. If this is the case, use this option to restore them.
 - **Restore the item-dependent columns and content types to maintain item integrity** – The item is restored and the dependent column or content type is created in the corresponding list/library. The item still uses the dependent column and content type.
 - **Do not restore item-dependent columns and content types** – The item-dependent columns and dependent content types will not be restored. When selecting this option, make sure the dependent columns and content types exist in the destination. Otherwise, the item cannot be restored.
 - h. **Exclude User/Group Without Permission** – If you select **Yes**, the users/groups that have no permissions will not be restored. By default, **No** is selected.
 - i. **Version Settings** – Choose the **Version Settings** for the content being restored to SharePoint. To improve performance, limit the versions restored. **Restore all versions** restores all the versions of the backup data; while **Restore the latest version(s)** only restores the latest several **Major** or **Major and Minor** versions of the backup data as designated. The other versions are not restored. Note that the current version will always be restored together with the entered number of **Major** or **Major and Minor** versions.
 - j. **Notification** – Configure the e-mail **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list. You can also choose to create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.
12. When finished configuring **Restore Settings**, click **Next** to enter the **Snapshot Selection** page.
13. **Snapshot Selection** – Restore the granular data from either the local or the remote database snapshot. Click **Load Remote Backups** on the ribbon to load the SnapVault remote snapshots. After the remote backups are loaded in the tree, select local or remote snapshots for the selected content database. Click **View Details** next to the snapshot to view the content databases. Make sure that the selected content database has its corresponding local or remote snapshots selected.

***Note:** Databases, BLOB data, and granular data can be restored from the remote snapshot in SnapVault secondary storage. Web front-end data cannot be restored from the remote snapshot in SnapVault secondary storage.

14. Click **Next**. The **Schedule** page appears.
15. **Schedule** – Choose whether or not to create the restore job based on a schedule. Select **Restore immediately after wizard finishes** to run the job immediately after finishing the restore wizard. To configure the schedule yourself, select **Configure the schedule myself** and input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.
16. When finished, click **Next**. The **Overview** page appears.
17. Review and edit the job selections. To make changes, click **Edit** in the middle of the row on the **Settings** tab to go to the corresponding settings page. This links to the corresponding setting page, allowing you to edit the configuration. In the **Preview** tab, you can view the restore action and the expected farm tree after the restoration, or click **Edit** to go to the **Restore Type** interface to change the restore action.
18. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Restoring a Database to a Point in Time

In a point-in-time restore, databases are restored to a point in time selected from the timeline browser.

A point-in-time restore occurs in two restore scenarios:

- The database is restored to a given time from a backed up transaction log.
- The database is restored but only a subset of backed up transaction logs are applied to it.

***Note:** Performing a point-in-time database recovery results in a new recovery path.

The following image illustrates the potential problems when a point-in-time restore is performed.

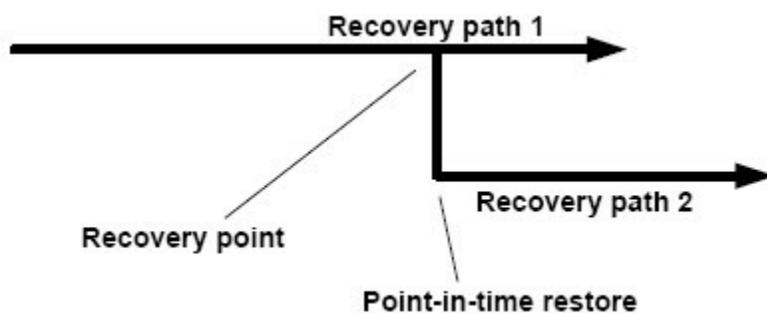


Figure 26: Recovery Paths.

In this image, Recovery path 1 consists of a Full backup followed by a number of transaction log backups (a point-in-time backup). New transaction log backups are created after the point-in-time restore takes place, which results in Recovery path 2. It is not possible to tie the transaction logs created in Recovery path 2 to the Full backup belonging to Recovery path 1. Therefore, to preserve database integrity, the only way to restore the database to its most current state after a point-in-time restore is to complete a new Full backup that has only one recovery path.

***Note:** To avoid the problems listed previously, ensure that you always create a Full backup after restoring a database to a point-in-time.

Restoring from an Alternate Storage Location

This option restores data from an alternate storage location other than your primary storage (for example, data stored on a SnapMirror copy or as a SnapVault backup). The data will be restored manually using other tools (like SnapManager for Microsoft SQL Server); you will need to locate the database backup snapshot using the prompt and restore the data in SnapManager for Microsoft SQL Server.

For database level restore:

1. If you selected **Restore from Alternate Storage Location**, DocAve begins preparing for the restore after clicking **Next** in **Notification** step. During this preparation process, the selected databases will be detached from the SharePoint environment.
2. After the restore preparation successfully completes, detailed information regarding all related components for manual restore is listed in the **Related Component** page. Perform a manual restore of the necessary components. For example, if restoring a content database, you must perform a database restore to the selected content database.
3. For instructions regarding a restore from an alternate source, see the *SnapManager for SQL Server Administrator's Guide*.
4. After the manual restore completes, click the **Verify** button to continue the restore process. DocAve attempts to verify the manually restored components and completes the restore. If the verification or the restore fails, a list of errors detected is displayed.

For item level restore:

1. If you selected **Restore from Alternate Storage Location**, the content database where the selected items reside will be displayed in the **Related Component** page after you configured the restore settings and clicked **Next**. Perform a clone restore to the content database where the selected items reside.
2. For instructions regarding a restore from an alternate source, see the *SnapManager for SQL Server Administrator's Guide*.
3. Once the original content database is restored to a temporary database, click the **Verify** button to continue the restore process. DocAve uses the manually cloned temporary database to complete the restore process. After the restore is completed, the detailed information about the restore is displayed.

Cloning Web Applications for Restore

This option, which is essentially an out-of-place restore at the database level, restores selected SharePoint Web applications by cloning backup data to the destination farm. The **Clone to another farm** feature restores backed-up Web applications and content databases only. If BLOB data or a stub database is being backed up with the selected Web application, you can clone the BLOB data and the stub database to the destination farm as well. Refer to the instructions below for more information about cloning SharePoint components for restore:

1. After you selected the Web applications from the backup data tree in the **Data Selection** step, click **Next** to go to the **Restore Type** step.
2. **Restore Type** – Configure the following settings in this step.
 - **Restore Type** – Select the **Clone to another farm** option.
 - **Restore BLOB Data and Stub Database** – With this option selected, the Storage Manager BLOB data and stub database associated with the selected Web application will be cloned to the destination.

- **Destination Farm** – Select a destination farm from the drop-down list.
 - **Agent Group** – Select an Agent group from the drop-down list to execute this Web application clone job.
3. Click **Next** to enter the **Snapshot Selection** step. Click **Load Remote Backups** on the ribbon to load the remote snapshots in the SnapVault. After the remote backups are loaded in the tree, select local or remote snapshots for the selected content database. Click **View Details** next to the snapshot to view the content databases. Make sure that all of the selected content databases have the corresponding local or remote snapshots selected.

***Note:** Databases, BLOB data, and granular data can be restored from the remote snapshot in SnapVault secondary storage. Web front-end data cannot be restored from the remote snapshot in SnapVault secondary storage.
 4. Click **Next** to go to the **Destination Component Options** page, where you will configure the clone type and the cloned components' settings in the destination.
 5. **Clone Type** – Choose one of the following clone types.
 - **Copy Clone** – Creates temporary databases in the SQL Instance via SMSQL and then copies the temporary database files to the destination. Copy Clone will use existing storage resources of the destination server.
 - **Split Clone** – Creates temporary databases in the SQL Instance via SMSQL and then executes the split-clone method of SMSQL to split the cloned database backup data from the parent volume into a separate volume. Split Clone takes less job time than a Copy Clone and Split Clone will create new volumes for the storage of the cloned farm.

***Note:** To use Split Clone, you must be on SMSQL 7.2 or later and SnapDrive 7.1 or later.
 - **Only Clone** – Creates temporary databases in the SQL Instance via SMSQL, but does not execute the split-clone method to restore real backup data to the destination. To verify that cloned Web applications restore properly to the destination, select **Only Clone**.
 6. Click **Configure** under the **Destination Configuration** column to configure the destination settings of each clone component, such as Web application, content database, or stub database (if you have the stub database backed up with the selected content database or Web application). The configuration options are the same as creating a new Web application, or configuring the content database settings during new Web application creation. Also, the stub database configuration is similar to the content database configurations that are made during new Web application creation.
 7. Click **Next**. The **Physical Device Mapping** page appears. Note that if no BLOB data is backed up, this step will be skipped.
 8. Physical device mapping clones BLOBs in the source physical device to the designated destination physical device. Select the physical device from the **Clone to Physical Device** column. Note that only physical devices used by Storage Manager display and map to the destination physical device.

***Note:** A source physical device can only be mapped to one destination physical device. In addition, if you edit the restored items/documents from the SharePoint site collection, the BLOB

data in the destination physical device will be orphaned and the stub will be converted to real content. The content will be stored in the content database where the items/documents reside.

***Note:** If your backed-up content database contains file stream data, you must install the RBS provider in the destination SharePoint farm.

You can map all of the selected source physical devices to the same destination physical device in batch. To do this, complete the steps below:

- a. Select one or more checkboxes beside the physical device mapping items, and then click **Destination Physical Device** on the ribbon. The **BLOB Batch Settings Page** appears.

***Note:** Source physical devices that are different storage types cannot be selected together. Only physical devices that are the same storage type as the selected source physical devices can be displayed and selected as the **Clone to Physical Device**.

- b. Choose a destination physical device from the drop-down list. Click **Show** to view the path and usage information of the selected physical device.
- c. Click **OK** to save the batch settings and return to the **Physical Device Mapping** interface.

***Note:** If the source physical devices are included in a BLOB storage logical device, the clone physical devices function in the destination does not automatically recognize the relationship as a BLOB storage logical device.

9. Click **Next**. The **Restore Settings** page appears.

10. **Restore Settings** – Choose detailed settings for the restore job.

- **Mapping Settings** – Select a user mapping profile or a domain mapping profile from the drop-down list to update the permissions and metadata.
 - **User mapping** – Select a user mapping profile from the drop-down list or select **New User Mapping** from the drop-down list to create a new one. After you selected a user mapping profile, click **View** to view the details of the user mapping profile settings. For specific instructions on setting up the user mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** User Mapping will not function if you configure it with a username that in an e-mail format.

***Note:** The User Mapping at database level does not support using default user or placeholder in the mapping settings.
 - **Domain mapping** – Select a domain mapping profile from the drop-down list or select **New Domain Mapping** from the drop-down list to create a new one. After you selected a domain mapping profile, click **View** to view the details of the domain profile settings. For specific instructions on setting up the domain mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** Domain Mapping will not function if you configure it with a fully qualified domain name.

***Note:** The job details about the user mappings and domain mappings can be viewed in the **Security Details** tab of the job report.

- **Notification** – Configure the e-mail notification settings. Select a previously configured notification profile from the **Select a profile** drop-down list, or create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.
11. Click **Next**. The **Schedule** page appears.
 12. **Schedule** – Choose whether or not to create the restore job based on a schedule. Select **Restore immediately after wizard finishes** to run the job immediately after finishing the restore wizard. To configure the schedule yourself, select **Configure the schedule myself** and input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.
 13. When finished, click **Next**. The **Overview** page appears.
 14. Review and edit the job selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
 15. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it immediately.

Restoring Backed-Up Web Front-End Files

To restore backed-up Web front-end files, complete the steps below:

1. Follow the instructions given in [Building a Restore Plan](#) to begin building the plan.
2. **Data Selection** – Expand the backup data tree, and select the files from **SharePoint Hive** or **Extra File System Folders** node to restore. To select individual or multiple files to restore, complete the steps below:
 - a. Click the **Files** node. The **Item Browser for Files** window appears.
 - b. All of the files in the selected folder are displayed. Search and select the desired files, and then click **OK**.
3. Configure the settings provided for restoring the backed up Web front-end files. For details, refer to [Options for Restoring Backed-up Web Front-end Files](#).

Options for Restoring Backed-up Web Front-end Files

In the **Settings** group on the **Time-based Restore** tab, there are two options that can be used to restore Web front-end files.

- **Installed Programs** – This function checks the status of installed applications on the Web front-end server and the program installation status at the time of backup.
- **Download Backup List** – This function checks data status on the selected Web front-end server and the data status **when backing up** the specified Web front-end server components. Click the **Download Backup List** button on the ribbon, select the **Web front-end server information list before backup** or **Current Web front-end server information list** checkboxes, and click **OK**. A .zip file that contains a .csv of detailed lists is downloaded to the specified local path.

There are also two restore settings for restoring specific Web front-end files.

- **Restore Front-end File Security** – This option only applies to front-end files backed up, including IIS site files (except the web.config file), SharePoint hive files, and extra file system files. When this option is selected, both file content and security permissions are restored. If this option is not selected, only file content is restored.
- **Restore Front-end File to Alternate Location** – Select this option to restore front-end files and templates files to an alternate location.

For more information on restoring backed-up Web front-end files, refer to the [Platform Restore for NetApp Systems Support Table](#).

Restoring Backed-up BLOB Data

If you selected to back up Storage Manager BLOB data or Connector BLOB data, a corresponding **Storage Manager** or **Connector** node is generated in the backup data tree under the corresponding database.

After selecting the **Storage Manager** or **Connector** node, click the **View Details** next to the node to view detailed BLOB backup data for the selected node. After selecting the data to restore and configuring the desired settings, the backed-up BLOB data will be restored back to the corresponding **Storage Path**.

***Note:** If you want to perform a platform restore job for NetApp Systems at a granular level, only one BLOB node (one Storage Manager or Connector node) can be configured through the **View Details** link.

Restoring Backed-up Stub Database

Select one stub database to restore the backed up stubs. For details on how to separately restore the stub database, refer to the section below.

***Note:** You can only select one stub database to restore at a time. You cannot select multiple stub databases at the same time or select a content database at the same time for restore.

***Note:** To restore the stub database, related BLOB data, and content databases to another SharePoint farm, it is recommended that you perform a restore using the **Clone to another farm** restore type. For details, refer to [Cloning Web Applications for Restore](#).

1. Select a stub database node from the backup data tree. Click the **View Details** link beside the node to view the detailed information about this stub database, such as the **Content Database Name, SQL Server, and Farm**.
2. Click the **Next** button at the bottom-right corner to go to the **Restore Type** page. Select **Restore to original Farm** as the restore type and select an Agent group to execute the restore job.
3. Click the **Next** button at the bottom-right corner to go to the **Restore Settings** page.
4. In the **Restore Settings** page, configure the options according to your requirements. For the detailed explanation of each option, refer to the [Building a Restore Plan at Database Level](#).

In this case, select **Overwrite** as the **Conflict Resolution** and click the **Next** button at the bottom-right corner to go to the **Schedule** page.

5. In the **Schedule** page, configure the schedule settings according to your requirements. When you select **Configure the schedule myself**, the restore job will be started at the designated **Start time** that you configure. For the detailed explanation of each option, refer to [Building a Restore Plan at Database Level](#).

In this case, use the default settings and click the **Next** button at the bottom right corner to go to the **Overview** page.

6. In the **Overview** page, you can view all the previously configured settings. Once you are satisfied with all the configurations, click **Finish** to start the out of place Platform Restore for NetApp Systems job.

Restoring Backed-Up Catalog Site Collection

To perform an out of place restore of a catalog site collection to a destination Web application or site collection, complete the steps below:

1. Follow the instructions given in [Performing a Restore](#) to begin building the plan.
2. **Data Selection** – Select the content database where the catalog site collection resides. You can use the **Find Site Collection** feature as a quick method to locate the content database and Web

application where your desired catalog site collection resides. For details, refer to [Appendix A: About Find Site Collection](#).

3. After you find the corresponding content database, click **View Granular Contents** link beside the selected content database to expand the granular data tree. You can use the **Advanced Search** feature as a quick method to help you find the desired site collection, especially when your farm contains massive contents and nodes. For details, refer to [Appendix B: About Advanced Search](#). Select the catalog site collection from the **Backup Data** tree.

For details on the **Global Setting for Restoring Content, Property and Security** settings, refer to [Building an Out of Place Platform Granular Restore Plan](#).

4. Click **Next**. In the **Restore Type** interface, select the **Out of place restore** option.
5. In the **Destination** field, select a destination Web application or site collection. The destination farm tree also supports the use of **Advanced Search** feature. For details, refer to [Appendix B: About Advanced Search](#).
6. **Action** – Select how the data will be restored to the destination.
 - **Merge** – If you selected a site collection as the destination, select **Merge**. **Merge** will add the site collection to the destination site collection.
 - **Attach** – If you select a Web application as the destination, select **Attach**. **Attach** will restore the site collection as children beneath the selected Web application.
7. In the **Restore Settings** interface, the **Use as App Catalog Site** field is available to configure. Select **Yes** to restore the current site collection as the app catalog site for the destination Web application. Otherwise, select **No**.
8. For details on other settings, refer to [Building an Out of Place Platform Granular Restore Plan](#).

Restoring Backed-up Database Master Key

If you restore the backed-up database, the backed-up database master key will be restored together. While if you want to only restore the backed-up database master key, complete the following steps:

1. Navigate to*AvePoint\DocAve 6\Agent\data\SP2010\Platform* on the Agent server included in the Agent group. Open the **SP2010PlatformConfiguration.xml** file.
2. Find the **RestoreMasterKey** from the <FarmLevel> attributes. To only restore the database master key, set the value of **RestoreMasterKey** to **true**.
3. Select the database from the backup data tree, whose database master key that you want to restore.
4. Select **Skip** as the **Restore Option**.
5. Run the Platform Restore for NetApp Systems job to restore the backed-up database master key.

***Note:** By default, the password of the database master key will be restored to **1qaz2wsxE**. Change it to your desired password after the restoration. For details, refer to Microsoft's TechNet article [ALTER MASTER KEY \(Transact-SQL\)](#).

Deselecting the Restore Granular Content Feature

Deselecting the **Restore Granular Content** checkbox disables granular content selection. This restore method can only be used for a Platform granular restore that is performed at the site collection level, either in place or out of place. If the whole site collection needs to be restored, it is recommended to perform the restore at site collection level and deselect the **Restore Granular Content** checkbox. In this case, the restore is similar to STSADM site collection level restore. It is faster and can keep internal document IDs.

***Note:** If you select a SharePoint 2013 or SharePoint 2016 site collection to restore with the **Restore Granular Content** option deselected, the apps in the site collection will not be restored.

Restore Details for Specific Farm Components

The following lists some of the details and conditions pertaining to restoring the farm components.

- **Configuration database** – This is the core component of the SharePoint farm. It can only be restored using **Restore Database Only**. The SharePoint Central Administration database will be automatically backed up or restored if the backup/restore includes the SharePoint Configuration database. It is also recommended that you restore the SharePoint Central Administration database together with the SharePoint Configuration database to avoid breaking the relationship between these two databases.
- **Web applications** – Web applications can be selected from the farm tree and restored; this includes Web application properties. Content databases under Web applications are also restored, if selected. However, if there are any changes to the IIS sites (resulting from manual changes or third-party software), the IIS site backup on the front-end Member Agent will also need to be restored.
- **Content databases** – Content databases include SharePoint data such as site collections, sites, lists, libraries, files, and all items. When a content database is restored, DocAve 6 automatically attaches them to the original Web application.
- **SharePoint solutions** – When a SharePoint solution is restored in-place, the solution will be restored with its deployment status in the backup data.
- **Front-end resources** – If only out-of-the-box SharePoint features are used, there is no need to restore the front-end resources, as everything is covered by the other farm components. If there are manual customizations applied to the IIS site (including Web.config), the IIS site should be restored. If customizations are self-contained within the SharePoint 14/15 hive folder, they can be restored as well.
 - ***Note:** Certificates used by the IIS sites will not be backed up when backing up the front-end resources. You must manually back them up and restore them.
 - ***Note:** Front-end resources cannot be restored together with other farm components. They need to be restored separately after any other farm components are restored.

Backup and Restore FAST Search Server for SharePoint 2010 Farms

Microsoft FAST Search Server 2010 for SharePoint is a new search solution that delivers the power of FAST with the simplicity and TCO of Microsoft. It provides the best general productivity search on the market and makes it easy and economical to build high-value search applications. FAST Search Server 2010 for SharePoint provides high-end search features and can search huge corpus of data extremely fast.

FAST Search Server 2010 for SharePoint solution consists of three main parts:

1. **FAST Search Server 2010 for SharePoint** – The server infrastructure that provides processing, indexing, and query capabilities, and the administration of these features.
2. **FAST Query Search Service Application (SSA)** – The Query SSA provides the query Web front-end capabilities. You install and deploy this SSA on a SharePoint Web server, and it hosts query Web parts and SDK query integration capabilities for your search solution.
3. **FAST Search Connector (Content SSA)** – The FAST Search Connector is a Search Service Application (SSA) that retrieves content for indexing from SharePoint farms and other content repositories. You install and deploy this SSA on a SharePoint application server.

Backing Up the FAST Search Server

Follow the steps below to back up the FAST Search Server:

***Note:** If the FAST Search Server is installed on a NetApp FAS LUN or an N series, DocAve 6 will perform the snapshot backup. If the FAST Search Server is installed on the local disk, DocAve 6 will send the backup data to the configured storage policy.

1. Login to DocAve 6 and navigate to **Data Protection > Platform Backup and Restore for NetApp Systems > Platform Backup**.
2. On the **Backup** tab, click **Plan Builder** on the ribbon and choose **Wizard Mode** or **Form Mode** to create the plan.
3. Load the SharePoint farm tree in the **Scope** area to display the **FAST Search Server for SharePoint 2010 Farms** node. Then expand the node.
4. Select the **FAST Search Server Name (Admin)** checkbox; a pop-up window appears, prompting you to select the **FAST Search Connector Service Application** along with it. Click **OK** to select the SSA or click **Cancel** to not select the SSA. Note that **FAST Search Query Application** is not included in the backup tree.

5. On the lower-right section of the screen or on the ribbon, perform the following actions:
 - Click **Finish** to save the configuration of the plan without running it. The Backup plan will be now listed in **Plan Manager**.
 - Click **Finish and Test Run** to save the configuration and then perform a test run job, based on the plan, immediately. The backup job is now listed in **Plan Manager**.
 - Click **Finish and Run Now** to save the configuration and then run the saved plan immediately. The backup plan is now listed in **Plan Manager**.

You can view the job status in Job Monitor by clicking the corresponding button on the ribbon.

***Note:** In step 4, selecting the **FAST Search Server for SharePoint 2010 Farms** node directly displays a warning message reading **The selected FAST Search Server nodes contain a large amount of content**. This indicates that when performing the backup, the FAST Search Admin Database nodes and FAST Search Server nodes are included; the FAST Content SSA nodes are excluded.

Restoring the FAST Search Server

Follow the steps below to restore the FAST Search Server:

1. Login to DocAve 6 and navigate to **Data Protection > Platform Backup and Restore for NetApp Systems > Platform Restore**.
2. Configure the necessary settings and go to the **Data Selection** page.
3. In this page, select the **FAST Search Server Name (Admin)** checkbox; a pop-up window appears, prompting you to select the FAST Search Connector Service Application along with it. Click **OK** to select the SSA or click **Cancel** to not select the SSA.

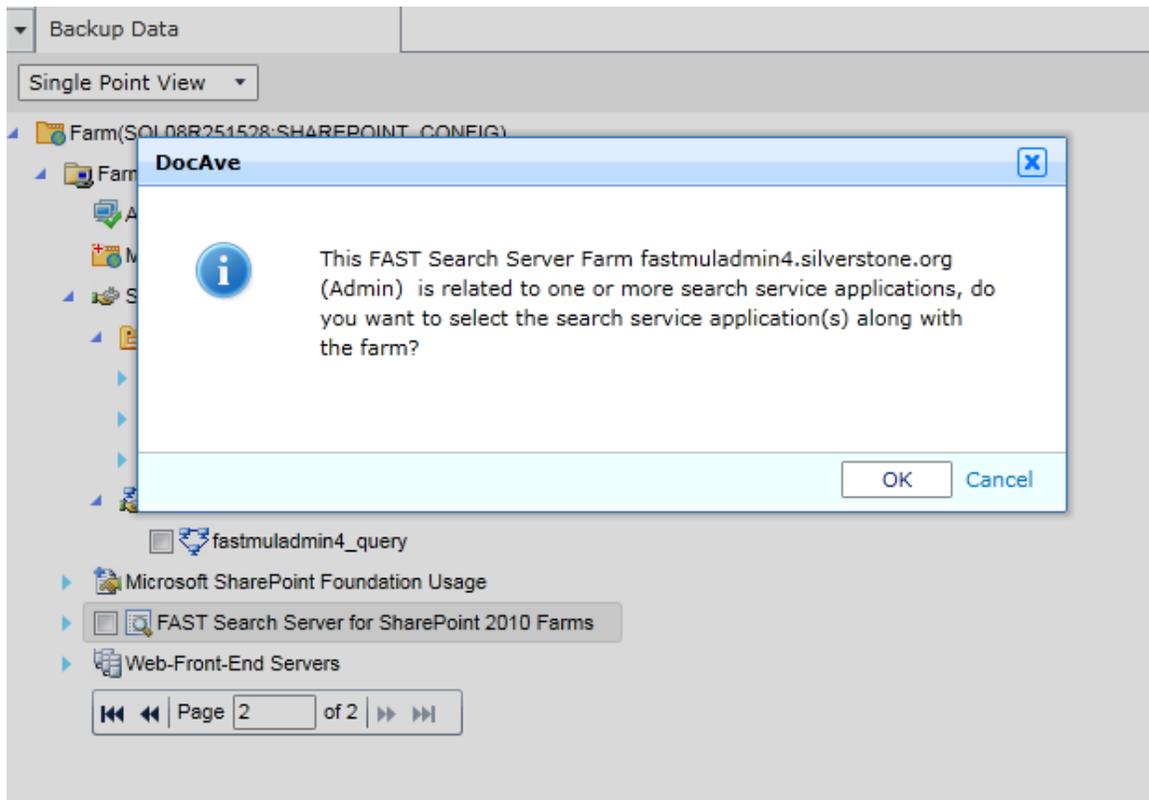


Figure 27: Restoring the FAST Search Server.

4. Only **In Place** restore type and **Overwrite/Skip** restore options are supported.
5. In the **Advanced** field:

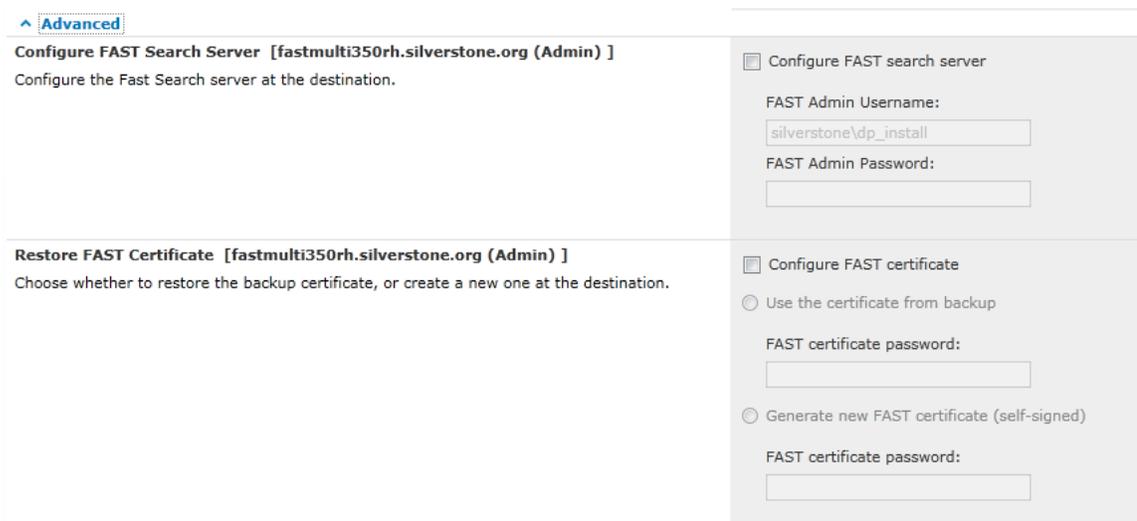


Figure 28: The Advanced field.

- a. If you do not select any checkbox, it will only restore the backed up files on the backed-up FAST Search Server.
- b. When selecting the **Configure FAST Certificate** checkbox:
 - If you select the **Use the certificate from backup** option, enter the correct certificate password to restore the certificate.
 - If you select the **Generate new FAST certificate(self-signed)** option, enter a valid certificate password to create a new certificate.

***Note:** If you select the **Configure FAST Search Server** checkbox, the **Configure FAST Certificate** checkbox is selected automatically. Then, enter the correct FAST admin password to configure the FAST Search Server.

6. Configure the other settings and click **Finish** on the **Overview** page to start the restore job. You can view the job status in Job Monitor by clicking the corresponding button on the ribbon.

Supported and Unsupported List

Refer to the information below for the supported and unsupported components for the FAST Search Server.

Component	Location	Support Status
FAST Search Center Site		Supported
FASTSearchCert	On SharePoint server	Supported
	On Stand-alone FAST server	Supported
	On FAST admin server	Supported
	On FAST non-admin server	Supported
FAST Search Index(data_fixml)	On Stand-alone FAST server	Supported
	On FAST primary non-admin server	Supported

Component	Location	Support Status
	On FAST secondary non-admin server	Supported
FAST Search Connector		Supported
	Content Source	Supported
	Crawl rule	Supported
FAST Search Connector proxy (NO proxy when created)		Unsupported
FAST Search Query		Supported
FAST Search Query proxy		Supported

About Platform Backup and Restore for NetApp Systems for SQL Mirroring Database

If there are principal databases and mirroring databases in SQL Server, you can use a Platform Backup for NetApp Systems to back up your principal databases.

Note that if you choose SQL authentication as a content database's database authentication in SharePoint, make sure that the Agent account has sufficient permissions to log into the destination SQL Server. Otherwise, the mirroring databases cannot be backed up when being used as failover databases.

***Note:** Before performing an In Place Restore at the database level, you must manually terminate the mirroring relationship because a database cannot be deleted or overwritten when it is mirrored. After completing the In Place Restore at database level, you can manually re-create the mirroring relationship.

About Platform Backup and Restore for NetApp Systems for Failover Database

Refer to the section below for the information of the SharePoint 2010 failover databases supported for Platform Backup and Restore for NetApp Systems.

- Content Database
- Admin Content Database
- State Service Database
- Business Data Connectivity Service Database
- PerformancePoint Service Application Database
- Managed Metadata Service Database
- Web Analytics Service Databases
- Word Automation Service Database
- Secure Store Service Application Database
- Search Service Application Databases
- Usage and Health Service Database
- User Profile Service Databases
- Help Search Database
- Subscription Service Database
- Session State Service Database
- Application Registry Service Database

Refer to the section below for the information on the SharePoint 2013 and SharePoint 2016 failover databases supported for Platform Backup and Restore for NetApp Systems.

- Content Database
- Admin Content Database
- State Service Database
- Business Data Connectivity Service Database
- PerformancePoint Service Application Database
- Managed Metadata Service Database
- Word Automation Service Database
- Secure Store Service Application Database

- Search Service Application Databases
- Usage and Health Service Database
- User Profile Service Databases
- App Management Service Database
- Subscription Service Database
- Session State Service Database
- Application Registry Service Database
- Machine Translation Service Database

Checking a Job Status

Platform Backup and Restore for NetApp Systems contains a Job Monitor button where users can view the status of jobs. This is useful for monitoring jobs or troubleshooting for errors.

If you want to view the backup job details on the snapshots information and the results of executing the SMSQL command `export-config`, select the backup job and select the **Download Job Details** option from the **Download** drop-down menu to download the backup job report zipped folder. Extract the folder to find the **Backupjob_ControlAgentName_SnapshotsInfo.xml** and the **SQLAgentName_SQLInstanceName_export-config.xml** files.

***Note:** The **ControlAgentName**, **SQLAgentName**, and **SQLInstanceName** in the file names will be replaced by specific values in a backup job.

For Platform granular restore job, users can check the **Object Details**, **Configuration Details**, and **Security Details** in Job Monitor for more detailed information.

If a Platform Backup for NetApp Systems job status is stuck at **Stopping**, click **Force Stop** in Job Monitor to terminate this job immediately. The job status will be set to **Force Stopped**.

For **Stopped** Platform Backup for NetApp Systems jobs and Platform Restore for NetApp Systems jobs, you can also view job settings in Job Monitor.

Refer to the [DocAve 6 Job Monitor Reference Guide](#) for more information.

Performing Disaster Recovery

The following sections contain information on four types of disaster recovery: farm repair without disconnecting the farm servers, farm clone, full farm recovery in a primary site, and full farm recovery in a secondary site (SnapMirror destination). Note that this document covers disaster recovery of medium-sized farms.

About Farm Repair

Farm Repair for NetApp Systems jobs may resolve minor issues with your SharePoint farm; these jobs are typically performed when the SharePoint farm is connected but experiencing minor issues such as unavailable services, deficiency of permissions in the SharePoint Registry, and so on. As opposed to a Farm Rebuild for NetApp Systems, which requires you to disconnect and then reconnect all servers in the farm, a Farm Repair for NetApp Systems job is much quicker as it does not require you to disconnect any servers in the farm.

To repair a farm without disconnecting the servers from the farm, complete the following steps:

1. Select the **Restore** tab and click **Farm Repair** in the **Manage** group.
2. In the **Farm Repair** interface, select the SharePoint farm from the **Farm** drop-down list.
3. In the table, view and select the following as needed:
 - Select the SharePoint farm servers you wish to repair
 - View the services that are running on the corresponding server.

The selection information is displayed at the bottom of the table. You can deselect the checkboxes by clicking **Clear Selection**.

4. Optionally, select a notification profile from the **Send Notification** drop-down list.
5. Click the **Repair** button on the ribbon to run the Farm Repair for NetApp Systems job.
6. After the job is finished, the repair status for each server in the farm will be displayed under the **Repair Status** column. You can also access Job Monitor to view this information.

About Farm Clone

The Farm Clone feature duplicates your SharePoint farm, providing you with two fully functional farms. The Farm Clone wizard will leverage the whole farm backup data to create a point-in-time sibling farm that is derived from the original farm for the purpose of creating a test, development, or disaster recovery environment. When you are about to perform a Farm Clone, note the following:

- Farm Clone supports cloning your SharePoint farm whose SharePoint servers and SQL servers are on Azure VMs.

- Farm Clone supports SharePoint 2016 farm except SharePoint 2016 [Single-Server Farm](#), and supports the SharePoint 2016 farm whose Central Administration website is secured with HTTPS using SSL.
- Farm Clone requires that the destination farm must be the same version of SharePoint cumulative, update packages, and hotfixes as the source farm.

The Farm Clone for NetApp Systems job supports cloning the farm to a different domain with user mapping and domain mapping configured, but the source domain and the destination domain must be trusted by each other.

By default, the Farm Clone for NetApp Systems job will make the source farm and the destination farm use the same farm ID. If you want to make the destination farm use a different farm ID, go to the ... \AvePoint\DocAve 6\Agent\data\SP2010\Platform directory on the destination SharePoint Central Administration server, find the **SP2010PlatformConfiguration.xml** file, and set the value of the **IsFarmCloneChangeFarmId** attribute to **true**.

Performing a Farm Clone

To perform a Farm Clone for NetApp Systems, complete the steps below:

1. Select the **Clone** tab and click **Farm Clone** in the **Manage** group. From the **Farm Clone** tab, configure the following options in the **Filter By** area.

***Note:** In the **Farm Clone** tab, only the backup jobs that backed up the whole farm can be displayed and filtered in the calendar view, and Farm Clone for NetApp Systems does not support cloning the Web front-end backup data. For details on restoring the Web front end data, refer to [Restoring Backed-Up Web Front-End Files](#).

Filter By – Limit the scope of backup data restored by filtering out specified full farm backup jobs.

- a. **Filter by Plan** – Filter the full farm backup data by plan information using this drop-down list.
 - **Farm** – Select a farm from the drop-down list to display the plans for that particular farm. Select **All Farms** to display all plans of all farms.
 - **Plan Name** – Select the plan that you want to display from the drop-down list. Select **All Plans** to display the jobs of all the plans.
 - **Restore granularity level** – Select the restore granularity level from the drop-down list; only the backup jobs of the specified restore granularity levels are displayed. Select **All Levels** to list the backup jobs of all levels.
- b. **Filter by Time Range** – Filter the full farm backup data by completion time range using this drop-down list.
 - **All Jobs** – Select this option to display all **Finished** and **Finished with Exception** Platform Backup for NetApp Systems jobs.

- **Backup jobs start within ...** – Select this option to specify a time period. All of the **Finished** and **Finished with Exception** Platform Backup for NetApp Systems jobs that have a start time within the specified time period will be displayed.
2. After configuring the filters above, click the **Filter** button in the **Filter By** area or on the ribbon to filter the backup jobs. All of the full farm backup jobs that meet all the filter rules are listed in the calendar. You can click **Reset** in the **Filter By** area or click **Reset** on the ribbon to clear all the filters and display all the **Finished** and **Finished with Exception** Platform Backup for NetApp Systems jobs.
 3. Select the backup job that you want to restore by clicking the job. Additional actions that can be performed:
 - Place the mouse cursor over the full farm backup job to display job information such as the **Plan Name**, **Job ID**, **Backup Option**, **Restore Granularity Level**, **Backup Method**, **Create Persistent Snapshot**, **Index Status**, **Copy Data**, **Job Status**, and **Data Import**. Click on **Day**, **Week**, or **Month** to change the view to see all the available full farm backup jobs during that time period.
 - Click the page turning buttons ( ) at the top-left corner to turn the page.
 4. Click **Next** to enter the **View** step.
 5. **View** – View all the backed up SharePoint components, farm topology, and server roles of the farm in the whole farm backup job. Refer to the following three view tabs:
 - **Farm Backup Data** – Displays all of the farm components backed up in the selected job.
***Note:** To ensure consistency between the source farm and the cloned sibling farm, the selections on the tree cannot be edited. The **Web Front-End Servers** node and **Custom Database** node are deselected.
 - **Topology By Role** – Displays the farm topology of the backed up farm.
 - **Topology Details** – Displays the server name and the corresponding server role in the backed up farm.
 6. Click **Next** to enter the **SQL Server Mapping** step.
 7. **Clone Type** – Choose to use one of the following clone types to clone the farm backup data to another farm.
 - **Copy Clone** – Creates temporary databases via SMSQL and then copies the temporary database files to the destination. Copy Clone will use existing storage resources of the destination server.
 - **Split Clone** – Creates temporary databases via SMSQL and then uses the split-clone method via SMSQL to split the cloned database backup data from the parent volume into a separate volume. Split Clone takes less job time than a Copy Clone, and Split Clone will create new volumes for the storage of the cloned farm.
***Note:** To use Split Clone, you must be on SMSQL 7.2 or later and SnapDrive 7.1 or later.

- **Only Clone** – Creates temporary databases in the destination SQL instance via SMSQL, but keeps the parent child relationship and does not use the split-clone method to restore the real backup data to the destination. If you only want to test your environment, select **Only Clone**.

***Note:** The destination farm must be able to map all of the backed up components of the source farm.

8. **SQL Server Mapping** – Configure the SQL Server Mapping to map the source SQL Server instance to a desired destination SQL Server instance. Select the Destination Server and Destination SQL instance for each source SQL Instance. Batch settings are also supported.

***Note:** If there are several source SQL instances containing databases that use the same database name, these source SQL instances cannot be mapped to the same destination SQL instance.

To configure the SQL Server Mapping settings in batch, complete the steps below:

- a. Select one or more source SQL Server instance from the table, and then click the Batch Settings () button. The **Destination SQL Server** window appears.
 - b. Select a destination SQL Server from the drop-down list to load all of its SQL instances.
 - c. Select a SQL instance from the **SQL Instance** drop-down list.
 - d. Click **Save**.
9. Click **Next** to enter the **Database Options** step.
 10. **Database Options** – The databases in the source farm will be cloned to the corresponding destination SQL instance selected in the **SQL Server Mapping** step. Click **Edit** under the **Details** column to view and edit the destination database settings. Only if the **Clone Type** is set to **Copy Clone**, can the destination database settings be edited. You can edit database and log file mapping in bulk by referring to the steps below:
 - a. In the **Database Information** table, select the checkboxes next to the databases that you want to edit and click the **Batch Settings** button () next to **Details**. The **Edit Database and Log File Mapping** window appears.
 - b. In the **Edit Database and Log File Mapping** window, select the databases to be edited.
 - c. Enter a destination database file path and destination log file path, and click **Apply**.

***Note:** There will be a validation test to test if the entered database file path and log file path are valid after you click **Apply**, and a prompt message will appear if they are not valid.
 - d. Click **Save** to save your edits. If you want to reset the paths, click **Reset**.

11. **Destination Server Role** – This step is only used for SharePoint 2016 farm. Configure the following settings for the SharePoint servers in the destination farm.
 - a. **Add Servers** – Click **Add Servers**; the **Add Servers** window appears. Select servers to add to the destination. You can select at most nine servers. Click **Add** to add the servers to **Destination Server** list and close the pop-up window.
 - b. **Destination Server Role** – After you add a destination server, click the blank choice box next to the server, and select a server role from the listed source server roles and Custom role. **Batch settings** () is supported.

Click **Next** to enter the **SharePoint Server Mapping** step.

12. **SharePoint Server Mapping** – Select the destination servers for the mapping of each source SharePoint server. The server role of each source SharePoint server is displayed under the **Server Role** column. Select a destination server from the **Destination Server** drop-down list for the mapping of the corresponding source server. Repeat this operation for each source SharePoint server. Batch settings for configuring the mapping are also supported. Complete the steps below:
 - a. Select one or more source servers from the table.
 - b. Click the Batch Settings () button on the **Destination Server** column header. The **Destination SharePoint Server** window appears.
 - c. Select a SharePoint server from the **Destination SharePoint Server** drop-down list as the mapping destination for all of the selected source SharePoint servers.

***Note:** The selected destination SharePoint server must be in the same SharePoint product version as the source server.
 - d. Click **Save**.

***Note:** If the selected destination SharePoint server is already connected to a SharePoint farm, the SharePoint server will be disconnected from the original farm in the **Disconnect Connection** step. If the server you select as the destination server for this Farm Clone for NetApp Systems job is included in a farm that has been backed up or configured in this platform, the backup data or configurations of the original farm may be unavailable after running this Farm Clone for NetApp Systems job.

13. After configuring the mappings for the SharePoint servers, click **Validation Test** to verify the mapping settings. In the verification process, the SharePoint configuration database will be restored to the mapped destination SQL Server for verifying the production versions and passphrase in the later steps. It may take a while.
14. After the validation is finished, click **Next**. The **Disconnect Connection** page appears.

***Note:** If all of the destination SharePoint servers are not connected to any farm, the **Disconnect Connection** step will be skipped.

15. **Disconnect Connection** – Disconnect all the SharePoint servers in this farm. All the SharePoint servers which have connected to the current farm will be displayed here.
- **Manage columns (+)** – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button (+), and then check the checkbox next to the column name to have that column shown in the list.
 - **Hide the column (-)** – Hover over a column heading and then select the hide the column button (-) to hide the column.
16. Click **Disconnect** to disconnect the connections of all the displayed SharePoint servers from this farm. If some of the SharePoint servers are not disconnected successfully, click the **Disconnect** button to disconnect those servers again. For the second **Disconnect** operation, only the SharePoint servers that have not been successfully disconnected in the first time will be disconnected from the farm.

If all of the displayed SharePoint servers have already been disconnected from this farm, go to the next step.

17. **Index Options** – Choose whether to clone the index components of Search Service Application to the destination index server. To clone the index components, select **Yes** in the **Clone Index** field. Otherwise, select **No**. If you select to clone the index components, configure the index location in the **Index Information** table. If the location is not configured, the default location for storing the index components in the SharePoint server, configured in the **SharePoint Server Mapping**, will be used.

Follow the two methods below to configure the location to store the backup data of the index components:

- **Separate configuration** – Enter a local directory of the destination index server into the **Location** column to store the cloned index component, and then repeat this operation for each index component.
- **Batch setting** – Select one or more index components from the table, and then select the Batch Settings (⊕) button on the **Location** column header. The **Index Location** window appears. Enter a local directory in the format of `C:\data` to store the cloned index components that you selected in the table. Click **Save**.

***Note:** Help Search Index components are not supported for Farm Clone for NetApp Systems.

18. Click **Next** to go to the **SharePoint Configuration** step.
19. **SharePoint Configuration** – Configure the settings required for reconfiguring the restored SharePoint farm.
- **Passphrase** – Enter the passphrase for this farm before reconnecting all the servers back.
 - **Port Number** – Displays the port used by the SharePoint 2010/2013/2016 Central Administration.

- **Authentication Provider** – Display the security authentication type for this newly cloned farm. Platform Backup and Restore for NetApp Systems supports the two following security authentication types: **NTLM** and **Negotiate (Kerberos)**. The authentication provider of the cloned farm will be the same as the backed up farm and cannot be changed in this step.

Click **Validation Test** to verify the information you entered. When the test is successful, click **Next**.

20. **Clone Options** – Configure the **Clone BLOB**, **Conflict Resolution**, **Mapping Settings**, and **Notification** for the Farm Clone for NetApp Systems job. .

- **Clone BLOB** – This field only appears when the backed up farm has Storage Manager BLOB backup data. Choose whether or not to clone the Storage Manager BLOB data in the farm. If you select the **Clone Storage Manager BLOB data** option, you are required to configure the physical device mapping to map the source physical device to a destination physical device. Click the box under the **Destination Physical Device** column to load all of the available destination physical devices that are using the same storage type, and then select a destination physical device for the source one.

The physical device mapping supports batch settings to map all of the selected source physical devices to the same destination physical device. Complete the steps below:

- Select the checkbox beside a physical device mapping item, and then click **Destination Physical Device** on the ribbon. The **BLOB Batch Settings Page** appears.
- Choose a destination physical device from the drop-down list. Click **Show** to view the path and usage information of the selected physical device.
- Click **OK** to save the batch settings and return to the **Physical Device Mapping** interface.

***Note:** Farm Clone for NetApp Systems does not support cloning Connector BLOB data.

- **Conflict Resolution** – Choose a resolution in the event that a conflict occurs during this restore. To skip cloning the backed up database with destination database kept intact, select **Skip**; to remove the conflicting database in the destination, and clone the backup data to the destination, select **Overwrite**.

***Note:** The Farm Clone for NetApp Systems job will always overwrite the SharePoint Configuration database regardless of the selected conflict resolution. The Farm Clone for NetApp Systems job will change the SharePoint Configuration database ID in order to let DocAve 6 process the two farms at the same time. The following information in the SharePoint Configuration database will be updated:

- The SQL Server information and the associated databases recorded in the Configuration database.
- The information recorded in the Object table of the Configuration database.

- If you configured the destination farm to use a different farm ID than the source one, the Farm ID for all of the objects recorded in the Configuration database will also be updated.
- **Mapping Settings** – Select a user mapping profile or a domain mapping profile from the corresponding drop-down list to update the permissions and metadata when restoring database to an alternate destination.
 - **User mapping** – Select a user mapping profile from the drop-down list or select **New User Mapping** from the drop-down list to create a new one. After you have selected a user mapping profile, click **View** to view the details of the user mapping profile settings. For specific instructions on setting up the user mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** The User Mapping at database level does not support using default user or placeholder in the mapping settings. User Mapping cannot map user groups in SharePoint 2013 farm to the destination during a Farm Clone for NetApp Systems.
 - **Domain mapping** – Select a domain mapping profile from the drop-down list or select **New Domain Mapping** from the drop-down list to create a new one. After you have selected a domain mapping profile, click **View** to view the details of the domain profile settings. For specific instructions on setting up the domain mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** The job details about the user mappings and domain mappings can be viewed in the **Security Details** tab of the job report.

***Note:** If configuring the user mapping by entering username in the e-mail format, or configuring the domain mapping by entering the domain with full qualified domain name, the User Mapping or Domain Mapping will not function.
- **Notification** – Configure the email **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list. You can also choose to create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile. Click **Next**.

21. **Overview** – View the current farm settings you have configured. You can click **Edit** to go back to each step to change the settings.

22. Click **Start** to run the Farm Clone for NetApp Systems job.

***Note:** Farm Clone for NetApp Systems job does not support cloning some specific SharePoint components to the destination. For details on restoring those components, refer to [Configuring Specific Components after Farm Clone](#).

Supported and Unsupported List of Farm Clone for SharePoint 2016 Farm

Components	Supported or Not
Web Application	Supported
Alternate Access Mapping	Supported
FBA Database	Supported
Global Site Template	Supported
Access Services	Supported
Application Discovery and Load Balancer Service Application	Supported
APP Management Service	Supported
Business Data Connectivity Service	Supported
Managed Metadata Service	Supported
Machine Translation Service	Supported
PerformancePoint Service Application	Supported
Subscription Service	Supported
Solution	Supported
Search Service Application	Supported
Secure Store Service	Supported
Security Token Service Application	Supported
Session State Service	Supported
State Service	Supported
Usage and Health Data collection	Supported
User Profile Service Application	Supported
Visio Graphics Service	Supported
Workflow Service Application	Supported
Word Automation Services	Supported
InfoPath Forms Services	Supported
Service Cross Farm	Supported
Project Server Service Application	Supported
BLOB	Only Storage Manager BLOB data supports Farm Clone.

Configuring Specific Components after Farm Clone

Some of the farm components may not work well after the Farm Clone for NetApp Systems job. Refer to the section below to do some configurations on the specific components to make them functional after the Farm Clone for NetApp Systems job is finished.

Configuring Custom Web Parts and Custom Solutions

If the Custom Web Parts and Custom Solutions exist in your source farm, you must manually install and deploy them in the cloned farm in order to make them functional in the cloned Web applications.

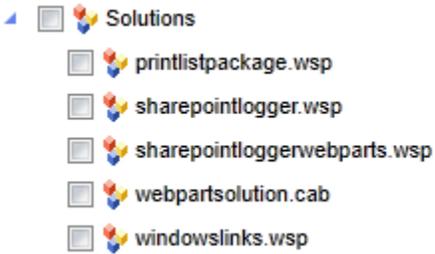


Figure 29: Selecting the custom solutions to restore.

After you have manually installed and deployed the Custom Web Parts and Custom Solutions, navigate to **SharePoint Central Administration > System Settings > Manage farm solutions** to check whether the solutions have been successfully deployed.

Name	Status	Deployed To
printlistpackage.wsp	Deployed	http://sp10ca04624/,...
sharepointlogger.wsp	Deployed	Globally deployed.
sharepointloggerwebparts.wsp	Deployed	http://sp10ca04624/,...
webpartsolution.cab	Deployed	http://sp10ca04624/,...
windowslinks.wsp	Deployed	Globally deployed.

Figure 30: Deploying the custom solutions.

Configuring NewsGator after Farm Clone

Immediately after cloning your farm, NewsGator will not be functional in the destination farm. To enable it, perform the following instructions:

1. Make sure the User Profile Service is **Started**.
2. Retract the NewsGator solutions that are globally deployed, and then redeploy the solutions. Note that the NewsGator solutions that are globally deployed all start with **NewsGator**.
3. After successfully deploying the NewsGator solutions, deactivate the features even though they may already be active after Farm Clone for NetApp Systems. Then, activate the NewsGator features again.
4. After successfully activating the NewsGator features, make sure the service instances are created and **Started**.

***Note:** For NewsGator VideoStream Service, edit the properties of the NewsGator VideoStream, and reconfigure the folders in the **VideoStream Configuration** field.

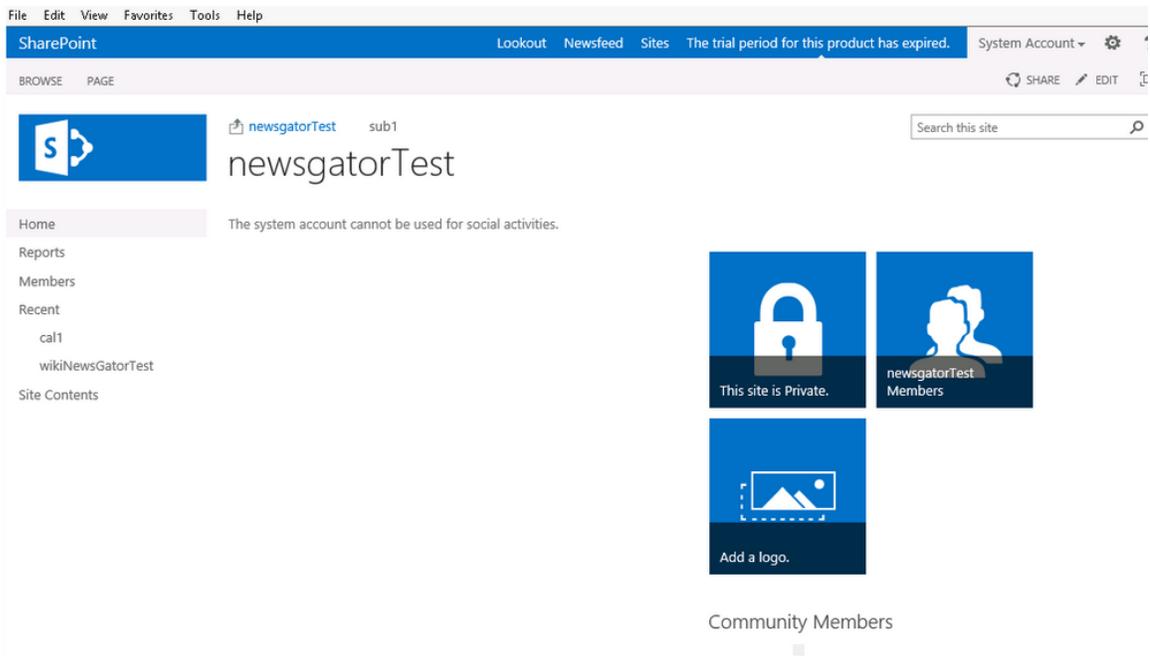


Figure 31: Accessing NewsGator site collection.

Configuring Nintex Workflow after Farm Clone

Immediately after cloning your farm, Nintex Workflow is not functional in the destination farm. To enable it, perform the following:

1. Navigate to **Central Administration > Nintex Workflow Management > Nintex Workflow Database Setup.**

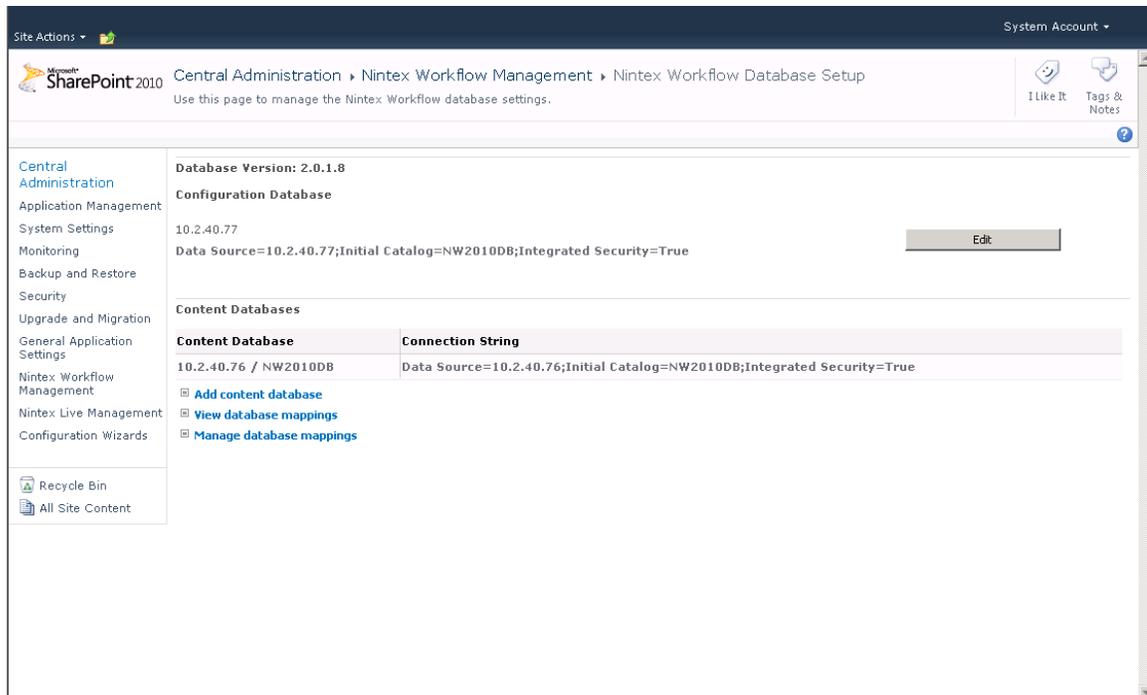


Figure 32: Accessing the Nintex Workflow Database Setup interface.

2. Click **Edit** to change the Nintex configuration database server to the destination server. Save the configurations.
3. Log into the destination SQL Server where the Nintex configuration database resides. Locate the Nintex configuration database and change the value under the **ServerName** column in the **dbo.Database** table to the destination SQL Server.

Helpful Notes about Farm Clone

Be sure to review the following helpful notes before and after a Farm Clone for NetApp Systems:

- **Project Server**—Project Server must be installed on each SharePoint server in the destination SharePoint farm before performing Farm Clone for NetApp Systems. If they are not installed, verification of the SharePoint Server Mapping will fail.
- **OWA for SharePoint 2010** – The OWA Server for SharePoint 2010 must be installed on each destination SharePoint server before performing Farm Clone for NetApp Systems. If this is not done, verification of SharePoint Server Mapping will fail.
- **OWA for SharePoint 2013** – The OWA Server for SharePoint 2013 is a separate application server from the SharePoint farm, thus the same OWA farm can be used by both production and disaster recovery environment. After the Farm Clone for NetApp Systems, the SharePoint configuration database will automatically continue pointing to the same OWA Server as the source farm, and then no further configurations are required.

- **FAST Search Server** –After a Farm Clone for NetApp Systems, configure the properties of the FAST Search Connector and Query in the destination farm, associate them with the newly configured FAST Search Server, and then crawl.
- **Windows Azure workflow** – Windows Azure Workflow Server is independent of the SharePoint farm. After a Farm Clone for NetApp Systems, configure the destination farm to use the same Windows Azure Workflow Server as the source farm. Install Workflow Manager Client on each of the SharePoint Web front-end servers in the destination farm, use a new **ScopeName**, and register the service again using **Register-SPWorkflowService** with the **-Force** parameter. Publish the workflow to the SharePoint Designer 2013, if you want to use the SharePoint 2013 Designer Workflow.
- **SQL Server PowerPivot for SQL Server 2012 and SharePoint 2013** – SQL Server PowerPivot feature cannot be installed without an existing farm. After a Farm Clone for NetApp Systems, you must reinstall the SQL Server PowerPivot Feature and the related Data Providers, retract the solution in SharePoint Central Administration, and then configure SQL Server PowerPivot using the **PowerPivot Configuration Tool**.
- **SQL Server PowerPivot for SQL Server 2008 and SharePoint 2010** is not supported in Farm Clone for NetApp Systems. The destination servers cannot be connected to the farm since there are no PowerPivot-related bins in the Global Assembly Cache.
- **SQL Server Reporting Services for SQL Server 2012 and SharePoint 2013** – Before performing a Farm Clone for NetApp Systems, install the SQL Server Reporting Services feature and add-ins. After the Farm Clone for NetApp Systems completes, run PowerShell commands to install the Reporting Services, Proxy, and Service Instance, and then start the Service Instance.
- **SQL Server Reporting Services for SQL Server 2008 R2 and SharePoint 2010** – Install the SQL Server Reporting Services feature with SharePoint integrated mode in the destination SharePoint farm after the Farm Clone for NetApp Systems job, manually configure the settings of the destination Reporting Server and configure the Reporting URL of the destination server.
- DocAve 6 does not support **SharePoint Foundation Help Search** being cloned to another farm.
- DocAve 6 does not support **Web front-end server data** being cloned to another farm.
- DocAve 6 does not support **KnowledgeLake Imaging** being cloned to another farm.
- This version of the software will assume that the SharePoint servers have already been deployed and installed and will not support clone of service applications or web-front-ends. Since both farms are intended to be active, it is assumed that the server names will be different from the source to the destination. DocAve 6 Agents must be deployed on the servers in the cloned sibling farm, to ensure that this farm will be added to the original DocAve 6 Manager.
- SharePoint version and patches must match, a validation test in the wizard will check the SharePoint version and CU history for missing patches.
- The snapshot to create the new environment must have been taken after the upgrade to DocAve 6.8.

- Backup plans must be created for the newly cloned farm, and it will appear as a new farm with a different name in the backup wizard interface. This will create a new backup data set for this farm.

Full Farm Rebuild in Primary Site

After you have backed up the entire farm using Platform Backup for NetApp Systems, you can use the **Farm Rebuild** function to perform a rebuilding of your farm should the need arise.

***Note:** The **Web-Front-End Servers** data that you have backed up (including the IIS Settings, SharePoint Hive, Global Assembly Cache, Custom Features, SharePoint Site Definitions, and file system folders) will not be restored during the Farm Rebuild for NetApp Systems. If necessary, select the desired **Web-Front-End Servers** nodes to restore the corresponding backup data after the Farm Rebuild for NetApp Systems.

***Note:** Farm Rebuild supports SharePoint 2016 farm except SharePoint 2016 [Single-Server Farm](#).

Supported and Unsupported List of Farm Rebuild for SharePoint 2010 Farm

Supported and Unsupported Farm Features for Farm Rebuild

Features	Supported or Not
Configuration Database	Supported
SharePoint Web Service	Supported
Central Administration Web Application	Supported
Central Administration Content Database	Supported
Web Application	Supported
Content Database	Supported
Global Search Settings	Supported
SharePoint Help Search	Supported
InfoPath Forms Services	Not Supported
FBA Databases	Supported
Solutions	Supported
FAST Search Server	Not Supported
Web Front-End Server	Not Supported
Global Site Template	Not Supported
Custom Database	Not Supported

Supported and Unsupported Service Applications for Farm Rebuild

Service Application	Supported or Not
Access Services	Supported
Application Registry Service	Supported
Business Data Connectivity Service	Supported
Excel Services	Supported
Managed Metadata Service	Supported
PerformancePoint Service	Supported
Search Service Application	Supported

Service Application	Supported or Not
Secure Store Service	Supported
Security Token Service Application	Supported
State Service	Supported
User Profile Service Application	Supported
Visio Graphics Service	Supported
Web Analytics Service	Supported
Word Automation Service	Supported
Usage and Health Data Collection Service Application	Supported
Session State Service	Supported
Subscription Service Application	Supported
Word Viewing Service	Supported
PowerPoint Service Application	Supported
Project Service Application	Supported
SQL Server Power Pivot Service Application	Supported
Lotus Notes Connector	Not Supported

Supported and Unsupported List of Farm Rebuild for SharePoint 2013 Farm

Supported and Unsupported Farm Features for Farm Rebuild

Features	Supported or Not
Configuration Database	Supported
SharePoint Web Service	Supported
Central Admin Web Application	Supported
Admin Content Database	Supported
Web Application	Supported
Content Database	Supported
Global Search Settings	Supported
InfoPath Forms Services	Not Supported
FBA Databases	Supported
Solutions	Supported
Web Front-End Server	Not Supported
Global Site Template	Not Supported
Custom Database	Not Supported

Supported and Unsupported Service Applications for Farm Rebuild

Service Application	Supported or Not
Access Services	Supported
Access Services 2010	Supported
App Management Service	Supported
Business Data Connectivity Service	Supported
Excel Services	Supported
Managed Metadata Service	Supported
Machine Translation Service	Supported
PerformancePoint Service	Supported
PowerPoint Conversion Service Application	Supported

Service Application	Supported or Not
Search Service Application	Supported
Secure Store Service	Supported
Security Token Service Application	Supported
State Service	Supported
User Profile Service Application	Supported
Visio Graphics Service	Supported
Word Automation Service	Supported
Work Management Service Application	Supported
Usage and Health Data Collection Service Application	Supported
Session State Service	Supported
Subscription Service Application	Supported
Project Service Application	Supported
SQL Server Power Pivot Service Application	Supported
Lotus Notes Connector	Not Supported

Supported and Unsupported List of Farm Rebuild for SharePoint 2016 Farm

Components	Supported or Not
Access Service	Supported
Access Service 2010	Supported
APP Management Service	Supported
Business Data Connectivity Service	Supported
Machine Translation Service	Supported
Managed Metadata Service	Supported
PerformancePoint Service	Supported
PowerPoint Conversion Service	Supported
Secure Store Service	Supported
State Service	Supported
Usage and Health Service	Supported
User Profile Service	Supported
Visio Graphics Service	Supported
Subscription Service	Supported
Word Automation	Supported
Workflow Service	Supported
Solutions	Supported
InfoPath Forms Services	Not Supported
FBA Database	Supported
Global Site Template	Not Supported
Web Front-End Server	Supported
Configuration Database	Supported
Admin Content Database	Supported
Web Application	Supported
License to Feature Mappings	Supported

Components	Supported or Not
Global Search Settings	Supported
Session State Service	Supported
Custom Database	Not Supported
BLOB	Supported
Project Server Service Application	Supported
Search Service Application	Supported

Mandatory Prerequisites for Disaster Recovery

To perform the Farm Rebuild for NetApp Systems, the following requirements must be met prior to a restore. **Be sure that these prerequisites are complete before proceeding!**

- A Platform Backup for NetApp Systems backup of the data for the entire farm (including the SharePoint configuration database and the Central Administration database) must be available.
- The SharePoint farm server topology should be identical to the topology at the time of backup. The system architecture must also match the platform at the time of backup. For example, an x64-bit architecture should be used if x64 architecture was used at the time of the backup.
- All related software installed on the rebuilt destination should be the identical version and the patch level as before. Examples of related software are: SharePoint, SQL Server, SnapManager for Microsoft SQL Server, DocAve 6, as well as the .NET Framework.
- User permissions on both the local server and SQL Server should be set to the same as before.
- Configure the same NetApp FAS LUN storage layout as before.

Warnings and Assumptions

- **NTLM** and **Negotiate (Kerberos)** are the supported security authentication types.
- During the Farm Rebuild for NetApp Systems process, the farm will be unavailable for use.
- The time for a Farm Rebuild for NetApp Systems to complete is associated with data size and the number of servers in the SharePoint farm. The more the data and the servers in the farm, the longer the job will take.
- Do not close your IE browser when executing a Farm Rebuild for NetApp Systems. If the Farm Rebuild for NetApp Systems process is interrupted before it completes, you will have to restart the Farm Rebuild for NetApp Systems wizard from the beginning.
- The IIS service will restart during the Farm Rebuild for NetApp Systems process. You will be notified through a pop-up message before the restart occurs.

Rebuilding the Farm

Generally speaking, the Farm Rebuild for NetApp Systems has five main procedures:

1. Disconnecting the Farm – Disconnect the servers from the original farm.
2. Restore BLOB – Restore the backed-up BLOB data. (This step is required if any BLOB data is backed up.)
3. Restoring Databases – Restore the following databases:
 - SharePoint Configuration database
 - SharePoint Central Administration database
 - Service application databases
 - Content database
 - Stub database
4. Connecting the Farm – Connect the servers to the target farm using two procedures:
 - Connect the servers to the SharePoint Configuration database, and configure the farm topology.
 - Provision the services on the SharePoint servers, and make sure the components in the farm are functional.
5. Restore Index – Restore the index components of the Search Service Applications. (This step is required if any index components are backed up.)

Detailed full Farm Rebuild for NetApp Systems steps are as follows:

1. Select the **Restore** tab and click **Farm Rebuild** in the **Manage** group.
2. From the **Farm Rebuild** tab, configure the options in the **Filter By** area, which limits the scope of backup data to be restored by filtering out specified Full Platform Backup for NetApp Systems jobs.

***Note:** The **Farm Rebuild** calendar displays only those jobs that have backed-up the SharePoint Configuration database.

- **Plan Filter** – Filter the full backup data by plan information using this drop-down list.
 - **Farm** – Select a farm from the drop-down list to display the plans for that particular farm. Select **All Farms** to display all plans for all farms.
 - **Plan Name** – Select the plan that you want to display from the drop-down list. Select **All Plans** to display the jobs of all the plans.
 - **Restore granularity level** – Select the restore granularity level from the drop-down list; only backup jobs of the specified restore granularity levels are displayed. Select **All Levels** to list the backup jobs of all levels.
- **Time Range** – Filter the Full farm backup data by completion time range using this drop-down list.

- **All Jobs** – Select this option to display all **Finished/Finished with Exception** Platform backup jobs.
 - **Backup jobs start within ...** – Select this option to specify a time period. All of the **Finished/Finished with Exception** Platform backup jobs whose start time is in the specified time period are displayed.
3. After configuring the three filters above, click the **Filter** button in the **Filter By** area or on the ribbon to filter the backup jobs. All of the Full farm backup jobs that meet all of the filter rules are listed in the calendar. You can click **Reset** in the **Filter By** area or click **Reset** on the ribbon to clear all the filters and display all the **Finished/Finished with Exception** Platform Backup for NetApp Systems jobs.
 4. Place the mouse cursor over the Full farm backup job to display job information such as the **Plan Name, Job ID, Restore Granularity Level, Index Status, Job Status** and **Data Import**. Click on **Day, Week, or Month** to change the view to see all the available full farm backup jobs during that time period. Click the page turning button   at the top-left corner to turn the page.
 5. Select the Full farm backup job that you want to restore. Click **Next**.
 6. **View** – View all of the backed-up SharePoint components in the Full farm backup job.

***Note:** The selection on the tree is disabled and cannot be changed. The **Web Front-End Servers** node and **Custom Database** node are deselected.
 7. **Restore Type** – Choose how the content will be restored.
 - **Restore Type** – To restore the backup data to the original farm with custom configurations, select **Restore to original farm**; to restore the farm by manually performing the restore via SMSQL, select **Restore from alternate storage location**.
 - **Restore to original farm** – Use this option to restore the databases normally by configuring the corresponding configurations.
 - **Restore from Alternate Storage Location** – Use this option to restore the databases from an alternate storage location by manually restoring the databases in SMSQL. For more information, refer to [Restoring from an Alternate Storage Location](#).
 - **Restore from SnapMirror Destination** – Choose whether or not restore the backup data from the SnapMirror destination. You can select this option to restore the backup data from SnapMirror destination if your environment has SnapMirror configured but the backup data in the SnapMirror source location is corrupted. With this option selected, you must make sure the backups in the SnapMirror destination are available for restore.

***Note:** If you are restoring from a SnapMirror destination, the **Snapshot Selection** step that configures the restore with SnapVault will be hidden from the wizard.
 - **Restore Purpose** – To build a production farm using the original farm’s backup data, select **Build a production farm**; to build a temporary farm using the backup data, select **Build a temporary farm**. A temporary farm will allow you to test your backup data and environment after the Farm Rebuild for NetApp Systems. This allows you to make

changes to your environment if you encounter any problems. The same backup job can be used over and over again until the Farm Rebuild for NetApp Systems works properly.

8. **Snapshot Selection** – Click **Load Remote Backups** on the ribbon to load the remote snapshots in SnapVault. After the remote backups are loaded in the tree, select local or remote snapshots for the selected databases. Click **View Details** next to the snapshot to view the databases. Make sure that all of the selected databases have the corresponding local or remote snapshots selected.
9. **Options** – Select whether or not to restore BLOB data, whether or not to restore all of the replicas of the AlwaysOn Availability Group, whether or not to use mapping settings or how to use mapping settings, and select a notification to receive the job report.

- **Restore BLOB** – Select whether or not to restore the BLOB data.
- **Replica Restore Options** – Choose to restore only one of the backed-up replicas at random, or to restore all of the replicas of the AlwaysOn Availability Group.
 - **Only restore one replica** – One of the backed-up replicas will be selected at random for the restore. This replica will be connected while accessing the database from SharePoint.
 - **Restore all of the replicas** – All of the backed-up replicas will be restored and the databases will be synchronized across the replicas in the AlwaysOn Availability Group.

***Note:** If the Primary replica of the AlwaysOn Availability Group is not backed up, the AlwaysOn Availability Group will fail over during the restore. At random, one of the Secondary replicas will be set to Primary, and this replica will be connected while accessing the database from SharePoint.

- **Mapping Settings** – Select a user mapping profile or a domain mapping profile from the corresponding drop-down list to update the permissions and metadata when restoring database to an alternate destination.
 - **User mapping** – Select a user mapping profile from the drop-down list or select **New User Mapping** from the drop-down list to create a new one. After you have selected a user mapping profile, click **View** to view the details of the user mapping profile settings. For specific instructions on setting up user mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** User Mapping at the database level does not support using default users or placeholders in mapping settings.

- **Domain mapping** – Select a domain mapping profile from the drop-down list or select **New Domain Mapping** from the drop-down list to create a new one. After you have selected a domain mapping profile, click **View** to view the details of the domain profile. For specific instructions on setting up domain mapping, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** Do not configure user mapping by entering a username in e-mail format, or configure domain mapping by entering a fully qualified domain name.

- **Notification** – Configure the e-mail **Notification** settings. Select a previously configured notification profile from the **Select a profile** drop-down list, or create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.
10. **Disconnect Connection** – Disconnect all of the SharePoint servers in this farm. All SharePoint servers that are connected to the current farm will be displayed here. Hovering the mouse over one column displays a . Click  to hide this column from the current view. You can also select which column to be displayed in the current view by clicking , selecting the checkboxes of the columns you want to be displayed in the current view, and clicking **OK**.
 11. Click **Disconnect** to disconnect all of the displayed SharePoint servers from this farm. If all the displayed SharePoint servers have already been disconnected from this farm, go to the next step directly.
 12. **Restore BLOB** – Restore the BLOB data in the farm. It is recommended that you restore all of the BLOB data listed in the table. Specify the **Conflict Resolution** to choose whether or not to overwrite the BLOB data in the event that a conflict occurs during a restore.
 13. **Restore Database** – Restore all of the backed up databases in the full farm backup job. The databases are all restored with no attempt to connect them to the SharePoint environment according to the selected conflict resolution.

***Note:** To restore the SQL Server logins when restoring a backed-up database, locate the **SP2010PlatformConfiguration.xml** file in the DocAve 6 Agent installation path: ...
`\AvePoint\DocAve6\Agent\data\SP2010\Platform`. In the **SP2010PlatformConfiguration.xml** file, enable the **RestoreLoginsConfig RestoreLogins** parameter by setting its value to **True**. The default value is **False**, so by default, the SQL Server logins will not be restored when performing a restore job. It is recommended that you have the database role of **Sysadmin** in SQL Server to restore the SQL Server logins; this ensures that high-level role logins are restored.

 - **Conflict Resolution** – Specify whether or not to overwrite the original contents if there is a conflict between the original database name and that of the backed-up database.
 - **Skip** – If a selected database in the backup has the same name as a database in the original farm, then the selected database in the backup is not restored.
 - **Overwrite** – If a selected database in the backup has the same name as a database in the original farm, then the original database is deleted first and the database in the backup is then restored.
 14. Click **Restore** to begin the restore process. After the restore of the databases is finished, the restore status will be updated in the **Status** column and the checkboxes before all the databases will become clickable. If the restore of an individual database fails, only select this database, specify the restore setting, and perform the restore job again.
 15. **SharePoint Configuration** – Configure the settings required for reconfiguring the restored SharePoint farm. You must enter the passphrase for this farm before reconnecting all of the servers. Select the **Specify Port Number** checkbox, and you are able to change the port used by the SharePoint 2010, SharePoint 2013, or SharePoint 2016 Central Administration. **NTLM** and **Negotiate (Kerberos)** are the supported security authentication types.

***Note:** If you are rebuilding your farm to a later version of SharePoint in the destination, the **Update Settings** field appears. Choose to update SharePoint automatically after connecting servers to the target farm or to update it later manually.

***Note:** If you plan to restore backed-up SharePoint 2010/SharePoint 2013/SharePoint 2016 Central Administration IIS settings after the Farm Rebuild for NetApp Systems, make sure you use the original port number for the SharePoint 2010/SharePoint 2013/SharePoint 2016 Central Administration in this step. SharePoint 2010/SharePoint 2013/SharePoint 2016 Central Administration can be accessed normally after restoring the backed-up IIS settings.

16. Click **Validation Test** to verify the settings you have entered.
17. **Connect** – Connect all of the SharePoint servers back to this farm. All SharePoint servers that have been disconnected from the current farm earlier in this procedure will be displayed here.
 - **Manage columns** (⊕) – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button (⊕), and then check the checkbox next to the column name to have that column shown in the list.
 - **Hide the column** (⊖) – Hover over a column heading and then select the hide the column button (⊖) to hide the column.
18. Click **Connect** to connect all of the displayed SharePoint servers back to this farm.
19. Click **Next**. The **Restore Index** page appears.
20. **Restore Index** – Restores all the index components of the search service applications that were backed up in a full farm backup job. Click **Restore** to restore all of the index components in the farm. The details about restoring the index components are listed in the table. Once the restore process completes, the restore status of each index component is updated in the **Status** column. You can perform the following actions on the index components table:
 - Select a desired number from the **Show rows** drop-down menu to specify the number of index components displayed per page. Select **<or >** to turn to the previous or next page.
 - If some index components fail to restore successfully, click **Restore** to attempt to restore the index components again.

***Note:** If some of the Search Service Application index components failed to be restored, perform a separate in place restore at database level with **Overwrite** selected as the **Conflict Resolution** to restore the Search Service Application again after the Farm Rebuild for NetApp Systems, so that the index components can work well in the SharePoint farm after the restoration.

21. **Overview** – View the current farm settings you have configured.
22. Click **Finish** to finish the Farm Rebuild for NetApp Systems.

***Note:** After the Farm Rebuild for NetApp Systems is finished, restart the DocAve Agent Service in order to obtain the most up-to-date information on the target farm.

Full Farm Recovery in SnapMirror Destination

This section describes how to perform a disaster recovery (DR) using SnapMirror backup data (SnapMirror license required on both source and destination storage systems) from the perspective of SharePoint and DocAve. It does not cover how to recover Active Directory (AD) or any other components not covered by DocAve.

Prerequisites

Prior to performing this restore, the following requirements must be met:

- Platform Backup for NetApp Systems backups of the DocAve Control Database, SharePoint databases, indexes, Connector BLOB data, and Storage Manager BLOB data must be available. Typically these are automatically replicated through SnapMirror.
***IMPORTANT:** To ensure that Storage Manager and Connector can be used after disaster recovery, you must use the same DocAve Control Database when re-installing the new DocAve Manager. Also, make sure that all BLOB data is ready in the DR site and the storage system profiles/physical devices/logical devices are configured using the correct configurations/paths.
- The registry backup of SnapManager for SQL Server must be available, which is **HKEY_LOCAL_MACHINE\SOFTWARE\Network Appliance\SnapManager for SQL Server**. You must manually export the registry to a location that can be accessed from the disaster recovery environment, and then import the exported registry to the disaster recovery environment.
- At the DR site, SharePoint farm topology (including DocAve topology) should be identical to the production site. The system architecture must also match the platform at the time of backup. For example, an x64-bit architecture should be used if x64 architecture was used at the time of the backup.
- All related software installed on the DR site should be the identical version and the patch level as before. Examples of related software are: SharePoint, SQL Server, SnapManager for Microsoft SQL Server, DocAve, as well as the .NET Framework.
- The hostname of the source and the destination should be the same.

For example, if you use IP in the configuration and use IP to configure SharePoint or DocAve Media service, the IP should be the same. For SQL, except port, the instance name and alias of the source and the destination should be the same. If you install DocAve in other places, you should use identical hostname or IP for DocAve Manager. The port can be different.

There are several ways to achieve this. For example, a separate AD domain for the DR site can be used to keep the same server topology, or if the DR site does not need to coexist with the production site, disk imaging or virtualization technology can be used to ensure the same topology is used.

- User permissions on both the local server and SQL Server should be set to the same as before.
- If a separate AD domain is used at DR site, that domain should have a trusted relationship with the primary site's AD so that users can still access SharePoint content. This can also be run if the DR site is in the same AD domain as the original location.

Full Farm Rebuild in Secondary Location

After all servers are rebuilt and the preceding prerequisites are met, complete the following steps for disaster recovery:

1. Install all required software components, including SnapDrive, SQL Server, and SnapManager for Microsoft SQL Server. For more information about these installations, refer to *SnapDrive for Windows Installation and Administration Guide* and *SnapManager for Microsoft SQL Server Installation and Administration Guide*. Only connect SQL Server using SnapManager for Microsoft SQL Server after you have already imported the registry backup of SnapManager for Microsoft SQL Server. Follow the steps below:
 - a. Import the SMSQL registry key from the exported file.
 - b. Add SQL Server to the SMSQL management list.
 - c. Run SMSQL Configuration Wizard.
2. Install SharePoint. If you are only restoring farm components such as Web applications, you can create a new farm in the destination that has the same name and farm topology as the source farm. Otherwise, SharePoint can be left un-configured when performing an entire farm restore.
3. Install DocAve Manager according to the steps listed in the [DocAve 6 Installation User Guide](#).
4. Connect the SnapMirror NetApp FAS LUN containing the backup job data, or manually copy this data to a location that the DR site logical device can access. Follow the steps below:
 - a. Configure iSCSI Initiator settings so that the server uses the SnapDrive NetApp FAS LUN.
 - b. Install SnapDrive and SMSQL.

***Note:** Do not connect SQL Server using SMSQL at this time.
 - c. Connect the following NetApp FAS LUNs in destination volumes with SnapDrive. Be sure to keep the drive letter the same as the NetApp FAS LUNs in source :
 - Destination SharePoint NetApp FAS LUN
 - Destination SQL NetApp FAS LUN
 - Destination DocAve NetApp FAS LUN
5. Install DocAve Agents according to the steps listed in the [DocAve 6 Installation User Guide](#).

Perform the full farm restore referring to [Restoring from an Alternate Storage Location](#).

Troubleshooting for Platform Backup and Restore for NetApp Systems

Refer to the section below for DocAve 6 Platform Backup and Restore for NetApp Systems troubleshooting.

Cannot See the Farm in Migrate Index Wizard

When using the Migrate Index tool, you may find that the farm you want to select does not appear in the **Farm Selection** drop-down list.

Try the following to solve this issue:

- Go to **Control Panel > Agent Monitor** to verify that the correct Agent type is selected. If not, select it.
- Verify that the Agent is active by going to **Control Panel > Agent Monitor**. If the Agent is not active, go to the Agent machine to check whether the Agent service is down, or ping the server where Control service resides to check the connection.
- Check whether the DocAve 6 login user has permission to the desired farm by going to **Control Panel > Account Manager > Permission Level**.

Cannot Load Remote Backups

In some cases, you may not be able to load remote backups from the Platform Restore wizard.

Try the following to solve this issue:

- Make sure you have properly configured the SnapVault in your environment.
- Ensure that the **Archive backup to secondary storage** option is selected in the Platform Backup wizard. In the **Run Now** interface or backup schedule settings, select the **Archive backup to secondary storage** option in the **SnapVault** field of the **Advanced** tab.
- Download the backup job report. It may be that SMSQL failed to update SnapVault.
- Log into the SQL Server where the local snapshot resides, and then use SMSQL to browse the database and verify that the remote snapshot exists.
- Log into the SQL Server where the local snapshot resides, and then execute the `get-backup` cmdlet. Check the output result for **LocalBackup** and **RemoteBackup**. **True** means the local backup or the remote backup can be loaded.

Appendix A: About Find Site Collection

The **Find Site Collection** feature provides you with a quick method of finding a site collection in your backup data by entering the URL or using wildcards.

***Note:** The search scope is all of the content databases that have been backed up by the selected backup job and that have a site collection-level index or lower.

1. On the **Time-based Restore** tab within the **Data Selection** step of the **Restore Wizard**, find the **Find Site Collection** button on the ribbon.
2. Click the **Find Site Collection** button on the ribbon. The **Find Site Collection** interface appears.
3. Enter the URL into the text box ahead of the **Search** button. The search function supports wildcards "*" and "?".
4. You can configure the **Advanced** settings to specify the maximum number of search results.
 - a. Click the **Advanced** button to expand the tab.
 - b. Enter the maximum number of the search results you want to display. By default, the maximum number is **1,000**. Larger results to display, higher risks to encounter poor efficiency. You can specify an integer between **1** and **5,000,000**.
 - c. Click **Apply** to apply your advanced settings.
5. Click **Search** to search for the desired site collections.

Appendix B: About Advanced Search

Advanced Search provides a quick method for locating specific objects or data within each granular level (from site collection level down to item level). You can use Advanced Search in the Time-based Restore at the granular level to search for granular content to restore and to select a node in the destination farm for the granular content you are about to restore.

1. On the **Time-based Restore** tab within the **Data Selection** step of the **Restore Wizard**, select the database that you want to restore the granular data from.
2. Click **View Granular Content** beside the database. Click **Global Settings for Restoring Content, Property, and Security**, and then select the **Restore Granular Content** option on the **Restore Granular Content** field.
3. Specify the search scope by clicking the object name in the **Backup Data** tree.
4. In the **Search** group on the ribbon, click **Advanced Search**. The **Advanced Search** page appears.
5. The granular object levels that equals or lower than the ones you select in the backup tree are listed in the drop-down list before the **Add Criteria** button. The value supports wildcard (*).

Using **Advanced Search**, you can search:

Level	Rule	Condition	Value	Result
Site Collection	URL	Matches	sitecollection	Searches for the site collection whose URL matches sitecollection .
		Equals	http://test:20000/sites/sitecollectionA	Searches for the site collection whose URL equals http://test:20000/sites/sitecollectionA.
	Modified Time	Before	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the site collection whose last modified time is earlier than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)
After		2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the site collection whose last modified time is later than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	
Between		From 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) To 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the site collection whose last modified time is between 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) and 2013-12-27 16:41:00 (UTC+08:00) Beijing,	

Level	Rule	Condition	Value	Result	
				Chongqing, Hong Kong, Urumqi)	
Site	URL	Matches	siteA	Searches for the site whose URL matches siteA .	
		Equals	http://test:20000/sites/sitecollectionA/siteA	Searches for the site whose URL equals http://test:20000/sites/sitecollectionA/siteA.	
	Site Title	Matches	A	Searches for the site whose title matches A .	
		Equals	siteA	Searches for the site whose title equals siteA .	
	Modified Time	Before	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the site whose last modified time is earlier than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	
		After	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the site whose last modified time is later than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	
		Between	From 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) To 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the site whose last modified time is between 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) and 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	
	List	Name	Matches	A	Searches for the list whose name matches A .
			Equals	listA	Searches for the list whose name equals listA .
Modified Time		Before	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the list whose last modified time is earlier than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	
		After	2013-12-27 16:41:00 (UTC+08:00) Beijing,	Searches for the list whose last modified time is later than 2013-12-27 16:41:00	

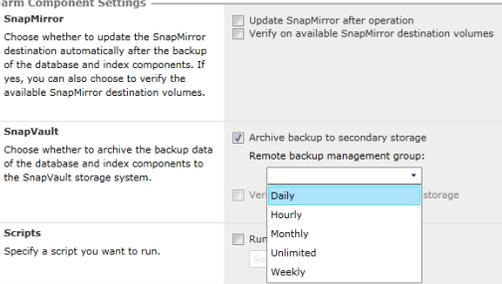
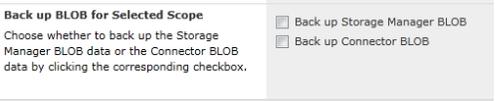
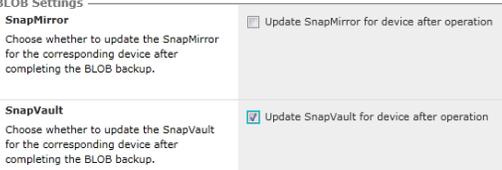
Level	Rule	Condition	Value	Result
			Chongqing, Hong Kong, Urumqi)	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)
		Between	From 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) To 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the list whose last modified time is between 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) and 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)
App	Title	Matches	A	Searches for the App whose title matches A .
		Equals	AppA	Searches for the App whose title equals AppA .
Folder	Name	Matches	A	Searches for the folder whose name matches A .
		Equals	folderA	Searches for the folder whose name equals folderA .
	Modified Time	Before	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the folder whose last modified time is earlier than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)
		After	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the folder whose last modified time is later than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)
	Between	From 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) To 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the folder whose last modified time is between 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) and 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	
Item/Document	Title	Matches	A	Searches for the item whose title matches A .
		Equals	itemA	Searches for the item whose title equals itemA .

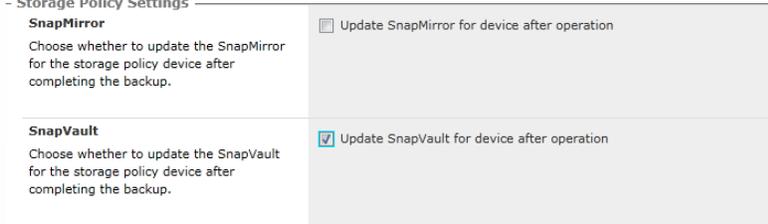
Level	Rule	Condition	Value	Result
	Attribute	Matches	A	Searches for the item whose attribute matches A .
		Equals	userA	Searches for userA as one of the attributes of the item.
	Modified Time	Before	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the item/document whose last modified time is earlier than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)
		After	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the item/document whose last modified time is later than 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)
		Between	From 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) To 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the item/document whose last modified time is between 2013-12-12 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi) and 2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)

6. Click **Add Criteria** to add a new filter condition. Change the logical relationship between the filter rules by clicking the logic icon after the rule. There are two logics now: **And** and **Or**. The default logic is **And**.
 - **And** – The content that meets all of the rules is searched out.
 - **Or** – The content that meets one of the rules is searched out.
7. Under the **Basic Filter Conditions** tab, view the search rules logical relationship.
8. Click **Search** to execute the search operation. The search results display under the **Search Result** tab. View the search results in **Tree View** or **List View** by clicking the corresponding buttons under the **Search Result** tab.

Appendix C: About Local and Remote Backup Snapshot Retention

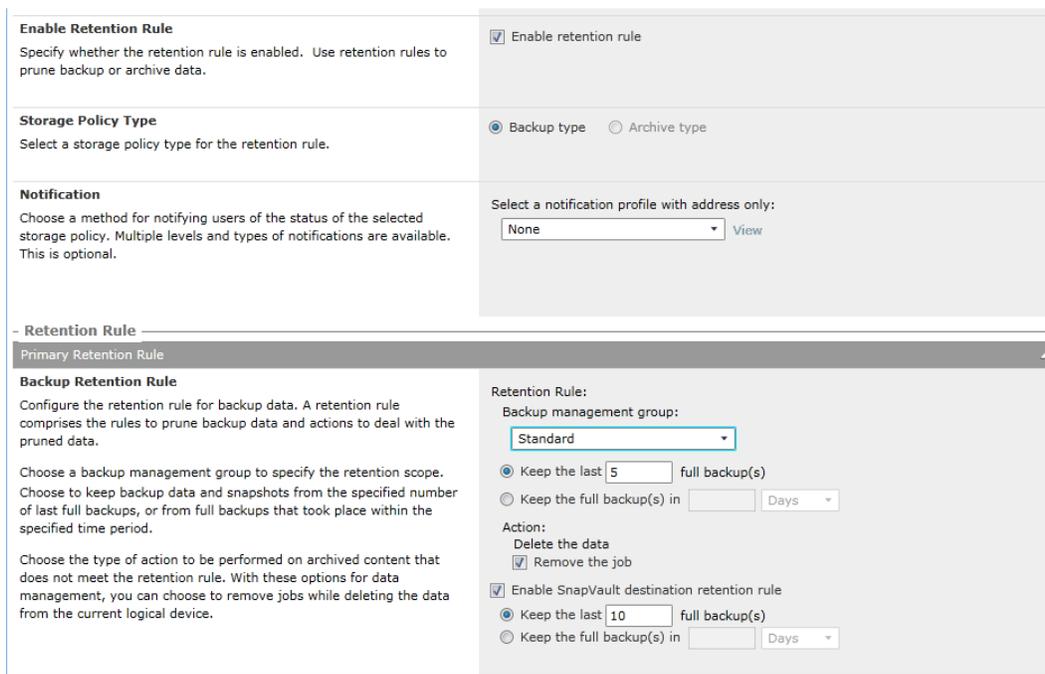
The information in the table below describes the generation of local and remote backup snapshots for the listed components in the SharePoint farm.

Component s	Generating Local Snapshots	Generating Remote Snapshots in SnapVault Destination
Database	<p>Select databases to back up in the backup plan. The Platform Backup for NetApp Systems job backs up the databases and generates the database snapshots by leveraging the SMSQL new-backup cmdlet.</p>	<p>The backed up databases are in the device with SnapVault relationship configured, and the Archive backup to secondary storage option for SnapVault in the Farm Component Settings is selected in the backup schedule settings or Run Now interface.</p> 
Search Index	<p>Select SharePoint Search Index to back up.</p>	<p>The backed up Search Index components are in the device with SnapVault relationship configured, and the Archive backup to secondary storage option for SnapVault in the Farm Component Settings is selected in the backup schedule settings or Run Now interface.</p>
BLOB	<p>Select the Back up Storage Manager BLOB option or Back up Connector BLOB option in the schedule settings or Run Now interface.</p> 	<p>The backed up BLOB data is in the device with SnapVault relationship configured, and the Update SnapVault for device after operation option for SnapVault in the BLOB Settings is selected in the backup schedule settings or Run Now interface.</p> 

Components	Generating Local Snapshots	Generating Remote Snapshots in SnapVault Destination
Snapshots generated in the storage policy device via update-SnapVault	<p>If the Update SnapVault for device after operation option under the Storage Policy Settings field is selected when configuring the settings of backup job schedule or on the Run Now interface, the local snapshot will be created on the storage system where the storage device resides; if the storage device has SnapVault relationship configured, the local snapshot will be updated to the SnapVault destination as the remote snapshot.</p> 	
Backup job metadata in storage policy device	Data (backup catalog, farm component properties, etc.) generated by Platform Backup for NetApp Systems jobs and the job record.	

There are two ways of deleting the backup snapshots in DocAve:

- Configure retention rule of storage policy used in backup to delete the backup data from the local or SnapVault destination. For details on configuring the storage policy retention rule, refer to [DocAve 6 Control Panel Reference Guide](#).



Enable Retention Rule
Specify whether the retention rule is enabled. Use retention rules to prune backup or archive data.
 Enable retention rule

Storage Policy Type
Select a storage policy type for the retention rule.
 Backup type Archive type

Notification
Choose a method for notifying users of the status of the selected storage policy. Multiple levels and types of notifications are available. This is optional.
Select a notification profile with address only:
None

- Retention Rule

Primary Retention Rule

Backup Retention Rule
Configure the retention rule for backup data. A retention rule comprises the rules to prune backup data and actions to deal with the pruned data.
Choose a backup management group to specify the retention scope. Choose to keep backup data and snapshots from the specified number of last full backups, or from full backups that took place within the specified time period.
Choose the type of action to be performed on archived content that does not meet the retention rule. With these options for data management, you can choose to remove jobs while deleting the data from the current logical device.

Retention Rule:
Backup management group:
Standard
 Keep the last 5 full backup(s)
 Keep the full backup(s) in Days
Action:
Delete the data
 Remove the job
 Enable SnapVault destination retention rule
 Keep the last 10 full backup(s)
 Keep the full backup(s) in Days

Figure 33: Storage Policy retention rule.

- Use **Delete Job and Backup Data** feature in Job Monitor to delete the backups from local or SnapVault destination. For details, refer to [DocAve 6 Job Monitor Reference Guide](#).

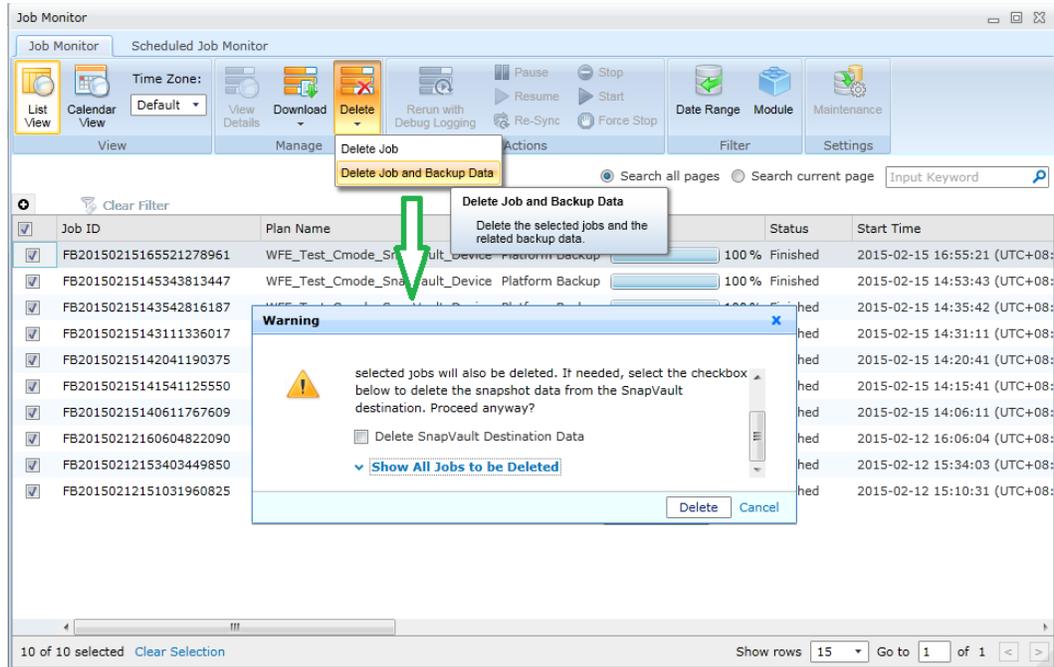


Figure 34: Delete Job and Backup Data in Job Monitor.

DocAve supports deleting remote snapshots from the SnapVault destination. In order to delete the snapshots from the SnapVault destination, you must make sure the following prerequisite is met:

- DocAve can connect to the destination storage system, that is, you must create Storage System Profiles for the destination storage systems where the remote snapshots of SnapVault destination reside. For details on creating storage system profile, refer to the [DocAve 6 Control Panel Reference Guide](#).

***Note:** The storage system profile must be created for each storage system that stores the SnapVault destination remote snapshots of the following components: SharePoint Search Index, BLOB data, and all of the data in the Media device generated by Update SnapVault.

Scenario 1: Deleting Backup Snapshots via Storage Policy Retention Rule

DocAve retention job can delete the following backup data:

- Database backup data maintained by SMSQL (local and SnapVault destination)
- SharePoint Search Index backup data (local and SnapVault destination)

- BLOB backup data (local and SnapVault destination)
- Snapshots in the Media devices generated via Update SnapVault (local and SnapVault destination)
- Backup job data (backup catalog, farm components' properties, etc.) and job record in Media devices

Only Deleting Local Snapshots

With the **Enable SnapVault destination retention rule** option deselected, DocAve will filter out the backup jobs according to the defined retention rule and delete the local backup data of these backup jobs.

As for a backup job to delete, DocAve will at first check if all of the database snapshots of this backup job exist. If all of the database snapshots do not exist, DocAve will delete the other backup data of this backup job; otherwise, any of the backup data of this backup job will not be deleted.

By default, DocAve will identify that the database snapshots do not exist when both of the local database snapshot and the remote snapshot in SnapVault secondary storage are detected not existing.

You can customize the configuration file to define the condition where the database snapshots do not exist:

1. Navigate to the ...*AvePoint\DocAve 6\Agent\data\SP2010\Platform* directory on the database server where the DocAve Agent resides. Find the **SP2010PlatformConfiguration.xml** file.
2. Locate the **JobRetentionDeletedSnapshotRuleConfig** node. By default, the value of **JobRetentionDeletedSnapshotRule** is **default**. Refer to the valid values as following:
 - **Default** – Indicates that the database snapshots do not exist when both of the local database snapshots and the remote snapshots in SnapVault secondary storage do not exist.
 - **Local** – Indicates that the database snapshots do not exist when the local database snapshots do not exist.
 - **Remote** – Indicates that the database snapshots do not exist when the remote database snapshots do not exist.

The deletion of the database snapshot is performed in Platform Backup for NetApp Systems job instead of the Retention job. In the Platform Backup for NetApp Systems job, DocAve adds attributes and values according to the defined retention rule to the SMSQL new-backup cmdlet in order to delete the snapshots met the DocAve retention rule. In the Retention job, DocAve invokes the SMSQL get-backup cmdlet to obtain the snapshot status and check if the database snapshots exist.

Refer to the instructions below about the workflow to delete local snapshots:

- If any of the database snapshot exist, the backup snapshots of the database related components, such as SharePoint Search Index and BLOB data, will not be deleted. In

addition, if any snapshot of the backup job is not successfully deleted, the backup data of this backup job in Media device and the backup job record will not be deleted.

- If all of the database snapshots of the backup job have been successfully deleted (do not exist), the backup snapshots of the SharePoint Search Index and BLOB data will be deleted.
- If all of the snapshots of database, SharePoint Search Index, and BLOB data are successfully deleted (do not exist), the snapshots in the Media device generated by Update-SnapVault will be deleted.
- If all of the snapshots of this backup job above are successfully deleted (do not exist), the backup job data in the Media device and the job record will be deleted.

Deleting Both Local and Remote Snapshots

Once the **Enable SnapVault destination retention rule** option is selected, DocAve will consider that the remote snapshots of this backup job exist in the SnapVault secondary storage. The remote snapshots in SnapVault secondary storage will be checked and deleted.

Refer to the instructions below for details on how DocAve works with the **Enable SnapVault destination retention rule** option selected.

- DocAve will filter out the backup jobs according to the defined retention rule and delete the local backup data of these backup jobs. If the local database snapshot does not exist, DocAve will identify that the local database snapshot has been successfully deleted. For details on deleting local snapshot, see [above](#).
- DocAve will filter out the backup jobs according to the SnapVault destination retention rule and delete the remote snapshots in the SnapVault destination. For details, see below:
 - DocAve will delete the remote database snapshots of this backup job from the SnapVault destination which are not returned by the SMSQL get-database cmdlet. The deletion is performed by the SMSQL delete-backup cmdlet and DocAve 6 checks if the remote database snapshots are successfully deleted from the SnapVault destination according to the returned value of this action. If all of the database snapshots are deleted, DocAve 6 will delete the remote snapshots of the other components in this backup job; otherwise, any of the remote snapshots of this backup job will not be deleted.
 - If any of the remote database snapshot exist, the remote backup snapshots of the database related components, such as SharePoint Search Index or BLOB data, will not be deleted. In addition, if any remote snapshot of the backup job is not successfully deleted, the backup data of this backup job in Media device and the backup job record will not be deleted.
 - If all the remote database snapshots of the backup job have been successfully deleted (do not exist), the remote snapshots of the SharePoint Search Index or BLOB data will be deleted.

- If all of the snapshots of the database, SharePoint Search Index or BLOB data are successfully deleted (do not exist), the snapshots in the Media device generated by Update-SnapVault will be deleted.
- Check the deletion status of the local and remote snapshots of each backup job. The deletion of the local snapshots and remote snapshots are mutual non-interference:
 - If all of the local and remote snapshots of a backup job are successfully deleted, delete the backup job data in the Media device and the job record.
 - If any of the local or remote snapshots of a backup job failed to be deleted, keep the backup job data in the Media device and do not delete the job record, thus this backup job can be used for restore.

Checking Old Backups to Be Deleted

If the storage policy you used in the backup plan has the retention rule configured, you can select the **Check Old Backups to Be Deleted** option in the backup job schedule settings or the **Run Now** interface to check the snapshot status of the previous backup jobs.

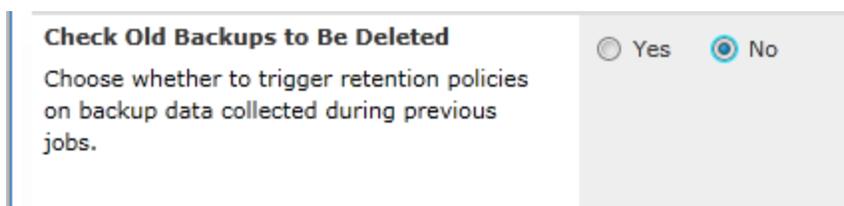


Figure 35: The Check Old Backups to Be Deleted option.

With **Yes** selected, DocAve 6 retention job will check the snapshot status of the previously performed backup jobs in addition to those backup jobs whose snapshots are going to be deleted. The snapshots of the old backups will be verified to see if they can be used for restore. If the snapshots of some components backed up in the old backup jobs cannot be used, those components cannot be selected from the **Backup Data** tree of the **Data Selection** step when performing the restore. Note that the retention job report does not report the verification.

If the **Enable SnapVault destination retention rule** option is deselected when configuring the Backup Retention rule, DocAve 6 will only check the local snapshots' status of the old backup jobs. If the SnapVault destination retention rule is configured, the remote snapshots' status will be checked additionally.

Scenario 2: Deleting Job and Backup Snapshot via Job Monitor

In Job Monitor, select one or more Platform Backup for NetApp Systems jobs that you want to delete and then click **Delete** on the ribbon. Select **Delete Job and Backup Data** from the drop-down list. A confirmation window appears. Click **OK** to delete the backup data in the local and delete the backup job

record. In addition, you can select the **Delete SnapVault Destination Data** option in the window to delete the snapshots from the SnapVault destination.

Only Deleting Local Snapshots

If the **Delete SnapVault Destination Data** option is deselected, DocAve 6 will only delete the backup data from the local.

Refer to the instructions below for details on how DocAve 6 works with the **Delete SnapVault Destination Data** option deselected:

- DocAve 6 will delete all of the local snapshots of databases, SharePoint Search Index, and BLOB.
- If the local snapshots of the databases are successfully deleted, DocAve 6 will delete the local snapshot in the Media device generated by Update SnapVault and the backup job data in the Media device and the job record.

Deleting Both Local and Remote Snapshots

If the **Delete SnapVault Destination Data** option is selected, DocAve 6 will delete both of the local and remote snapshots of the selected backup jobs from the SnapVault source and destination.

Refer to the instructions below for details on how DocAve 6 works with the **Delete SnapVault Destination Data** option selected:

- DocAve 6 deletes all of the local snapshots of the selected backup jobs including the local snapshots of the databases, SharePoint Search Index, and BLOB. If all of the database snapshots in the local are successfully deleted, DocAve 6 will delete the local snapshots in the Media device generated by Update SnapVault.
***Note:** DocAve 6 will identify that all of the local snapshots of the backup job are successfully deleted, if the database snapshots of the backup job are successfully deleted from local.
- DocAve 6 deletes all of the remote snapshots of the selected backup jobs from the SnapVault destination including the remote snapshots of database, SharePoint Search Index, and BLOB. If all of the remote database snapshots in the SnapVault destination are successfully deleted, the SnapVault destination remote snapshots generated via updating SnapVault will be deleted from the Media device.
***Note:** DocAve 6 will identify that a backup job's backup data is successfully deleted from the SnapVault destination if all of the database snapshots of the backup job are successfully deleted from the SnapVault destination.
- Check the deletion status of the local and remote snapshots of each backup job. The deletion of the local snapshots and remote snapshots are mutual non-interfering:

- If all of the local and remote database snapshots of a backup job are successfully deleted, delete the backup job data in the Media device and the job record.
- If any of the local or remote database snapshots of a backup job failed to be deleted, keep the backup job data in the Media device and do not delete the job record, thus this backup job can be used for restore.

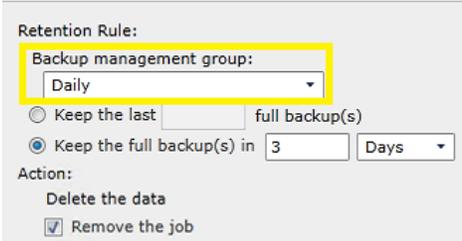
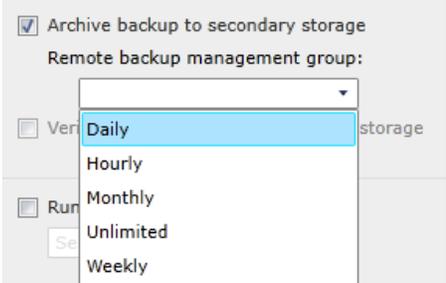
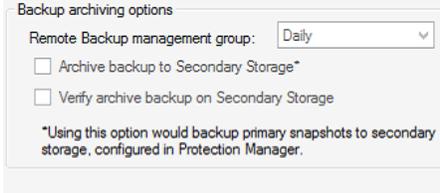
Scenario 3: Deleting Remote Snapshots from SnapVault

Destination with clustered environments

In the clustered environment, if you do not want to use DocAve 6 to delete the remote snapshots via storage policy SnapVault destination retention rule or Job Monitor, you can configure a Vault Policy to delete the SnapVault destination remote snapshots.

The following section describes how to configure DocAve 6 and SnapVault retention with a Cluster-Mode storage system. The 7 mode SnapVault retention relies on NetApp DFM protection policy and is not described in this section.

Database Backup Data Retention Configuration Between DocAve 6 and SMSQL

Backup Data	DocAve 6		SMSQL	
	7 Mode	Cluster Mode		
Local backup	Retention rule in storage policy: 		Backup management group for local snapshots: Select the backup management group for this backup operation: 	
Remote backup (archived backup on SnapVault)	The SnapVault option in the backup job schedule or Run Now interface: 		NetApp DFM controls the retention policy 	

The following is an example of configuring the remote database backup data retention on the clustered NetApp Data ONTAP 8.2 SnapVault environment:

1. Create a XDP SnapVault policy using NetApp OnCommand System Manager. On the environment, SnapVault policy can only control number of SnapVault snapshots to keep.

***Note:** The SnapMirror-Label must be one of the SMSQL remote backup management group types. You can add multiple rules to the SnapVault policy, and each rule with one SnapMirror label mapping to one of the SMSQL remote backup management group types. By assigning different retention counts, you can assign retention to different SMSQL remote backup management groups in the Vault Policy.

In this case, select **Hourly** as SnapMirror-label.

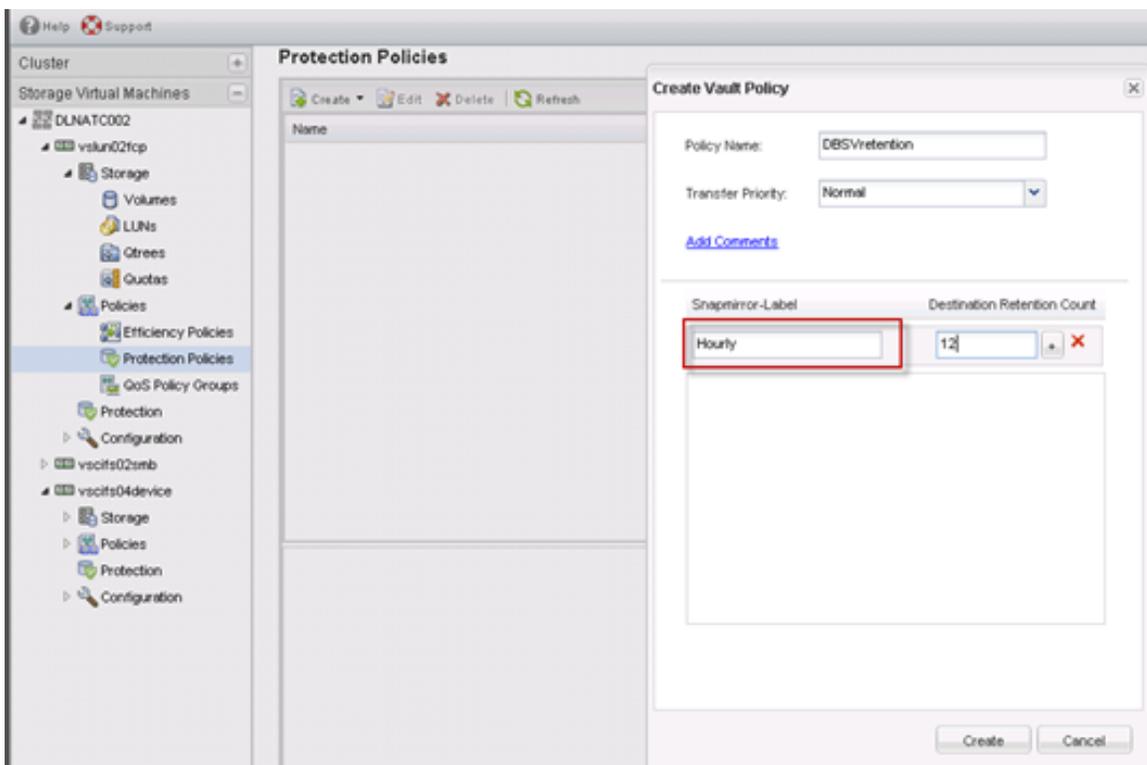


Figure 36: Selecting Hourly as the Snapmirror-Label.

2. Update the SnapVault relationship for the SMSQL database volume and the SnapVault destination volume with the newly created Vault Policy:

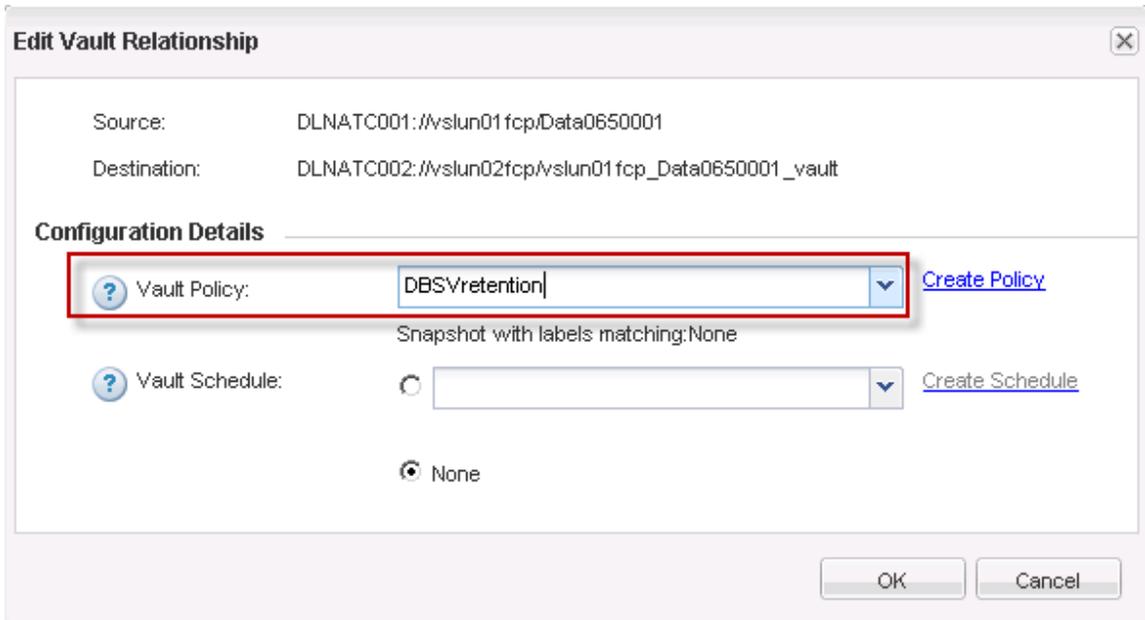


Figure 37: Configuring Vault Policy.

3. SMSQL local snapshot retention is based on DocAve 6 storage policy retention rule. DocAve 6 will send the local snapshot backup management group and backups/days to keep as parameters to SMSQL new-backup cmdlet. The local backup management group need not be exactly the same as the remote backup management group used in Vault SnapMirror-label.

In this example, we can set backup retention in **Daily** group and keep the local backup snapshots in **3** days.

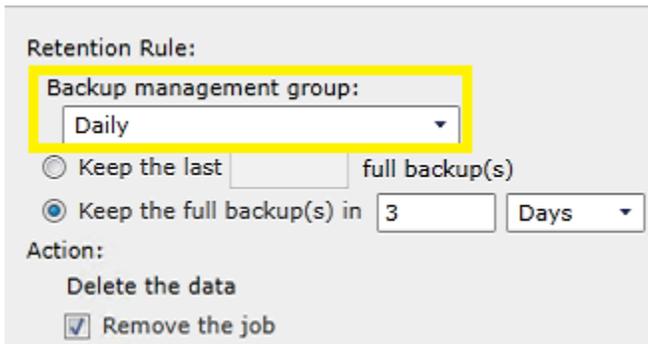


Figure 38: Configuring retention rule.

4. When configuring the schedule settings or the settings on the **Run Now** interface in DocAve 6, select the same remote backup management group as the SnapMirror of the previously created Vault Policy. The group type will be sent to SMSQL new-backup cmdlet and SMSQL will establish retention control for the archived backup on the SnapVault destination. You must choose the remote backup management group type that has a rule defined in the Vault Policy (configured in step 1) whose SnapMirror-label is the same as the remote backup group.

In this case, select **Hourly** from the **Remote backup management group** drop-down list as configured in Vault Policy:

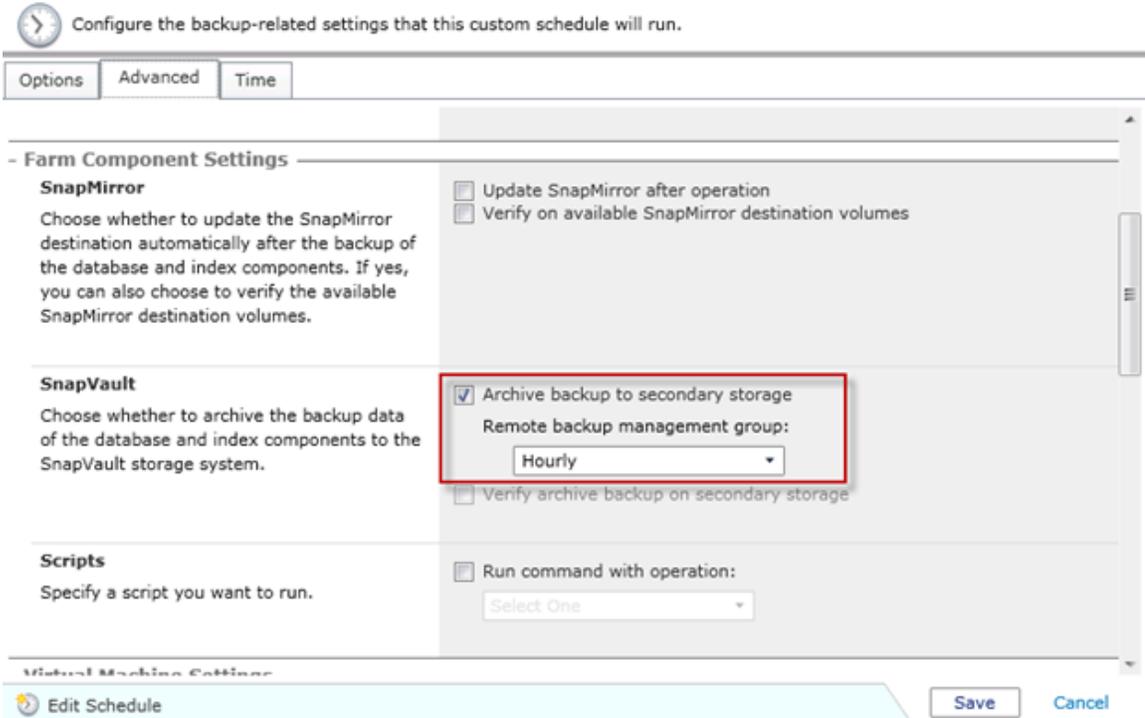


Figure 39: Configuring the SnapVault settings in the Farm Component Settings field.

- After running DocAve 6 Platform Backup for NetApp Systems job with SnapVault enabled, check the SMSQL console. The SMSQL console shows:
 - The local backup in SMSQL:

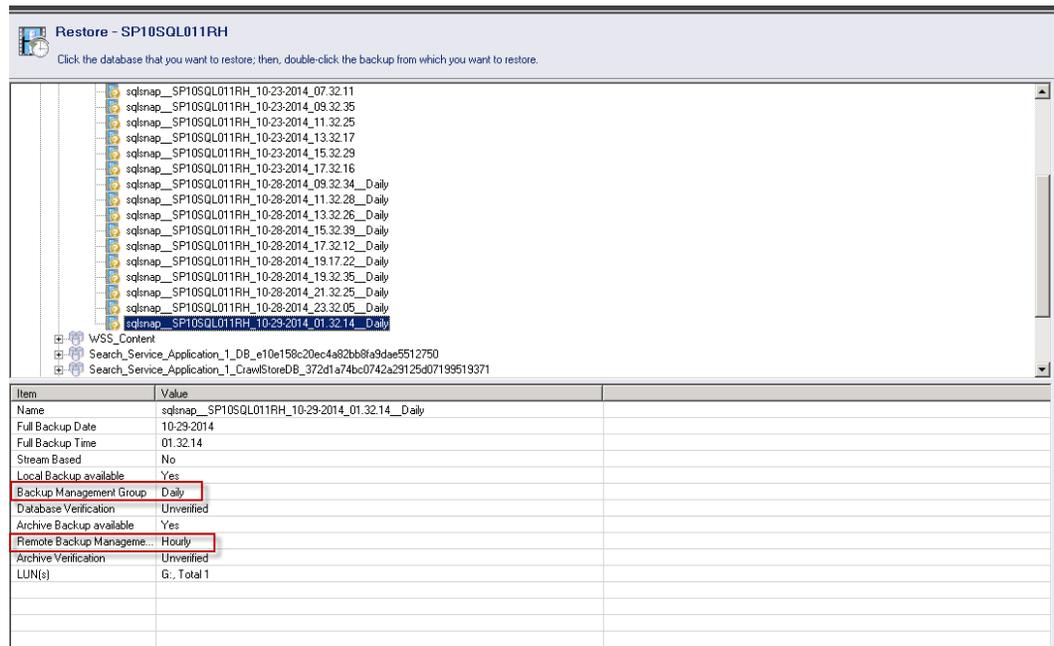


Figure 40: Local snapshots.

- The remote backup (archived backup on SnapVault) on SMSQL is managed by **Hourly** remote backup management group:

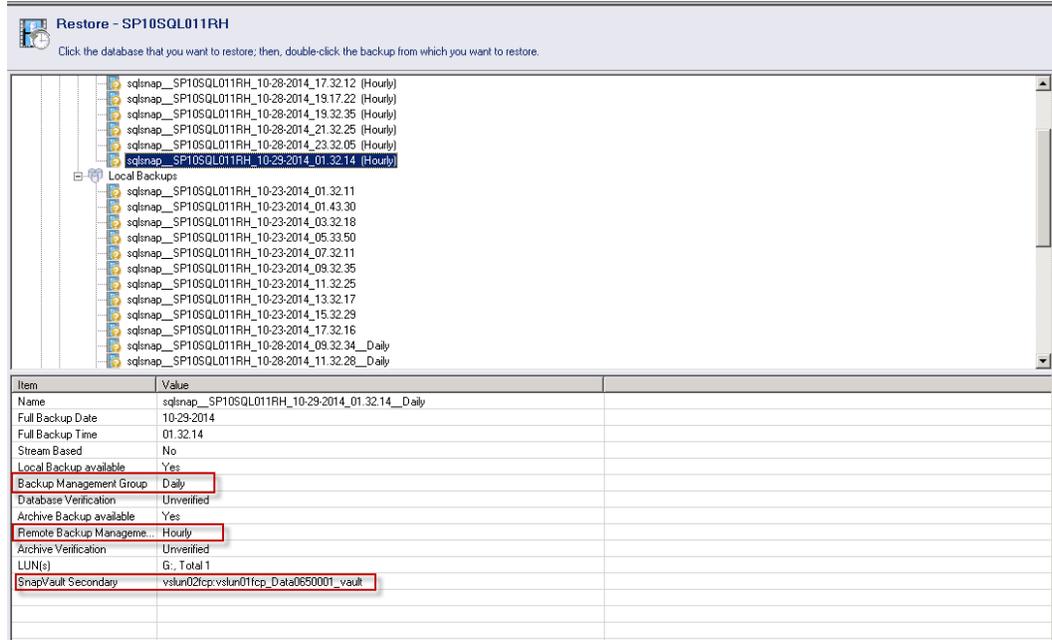


Figure 41: Remote snapshots.

6. Check for all of the snapshots in the Cluster mode SnapVault destination. You can view the SMSQL-created archived backup on SnapVault destination storage and the snapshot is with the defined SnapMirror label, the **Remote backup management group type**, which means the snapshot on SnapVault destination server will be managed by the Vault Policy created in step 1.

```

DLNATC002::volume snapshot> show -volume vslun01fcp_Data0650001_vault -vserver vslun02fcp -fields snapmirror-label
vserver      volume      snapshot      snapmirror-label
-----
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-14-2014_22.14.11  Daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-14-2014_22.14.11  Daily
vslun02fcp  vslun01fcp_Data0650001_vault  @snapmir@{0E12E196-D26A-4C98-B669-793AD42A5E47}
-
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-15-2014_19.16.29  Daily
vslun02fcp  vslun01fcp_Data0650001_vault  @snapmir@{02E3CB6B-4583-4D5D-8A4C-51F96F4F8EBD}
-
vslun02fcp  vslun01fcp_Data0650001_vault  @snapmir@{A52F02AA-F302-47BB-9917-5CE53AC6AC2A}
-
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-17-2014_00.21.12  Daily
vslun02fcp  vslun01fcp_Data0650001_vault  2014_10_17_01.55.01.536 E 1
-
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-17-2014_01.55.44  Daily
vslun02fcp  vslun01fcp_Data0650001_vault  @snapmir@{97EB6124-2232-4F66-B77D-46B61C761469}
-
vslun02fcp  vslun01fcp_Data0650001_vault  SMSF_FB20141021140318966754_Device_96c55b81e7dabafc
-
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-23-2014_01.14.24  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-23-2014_01.14.24  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-28-2014_17.32.12  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-28-2014_17.32.12  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-28-2014_19.17.22  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-28-2014_19.17.22  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-28-2014_19.32.35  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-28-2014_19.32.35  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-28-2014_21.32.25  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-28-2014_21.32.25  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-28-2014_23.32.05  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-28-2014_23.32.05  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlsnap_sp10sql011rh_10-29-2014_01.32.14  daily
vslun02fcp  vslun01fcp_Data0650001_vault  sqlinfo_sp10sql011rh_10-29-2014_01.32.14  daily
25 entries were displayed.

```

Figure 42: Viewing the snapshots.

BLOB Backup Data Retention Configuration

The following is an example of retention configurations for the remote BLOB backup data in NetApp FAS CIFS share of clustered NetApp Data ONTAP 8.2 SnapVault environment:

1. Create a XDP SnapVault policy using NetApp OnCommand System Manager. The SnapMirror-Label must be in the format of **DocAve 6_SnapmirrorLabel_RetentionGroup**, and the retention group must be one of the backup management group types.

In this case, enter the **DocAve 6_SnapmirrorLabel_Standard** as SnapMirror-label and keep **3** snapshots.

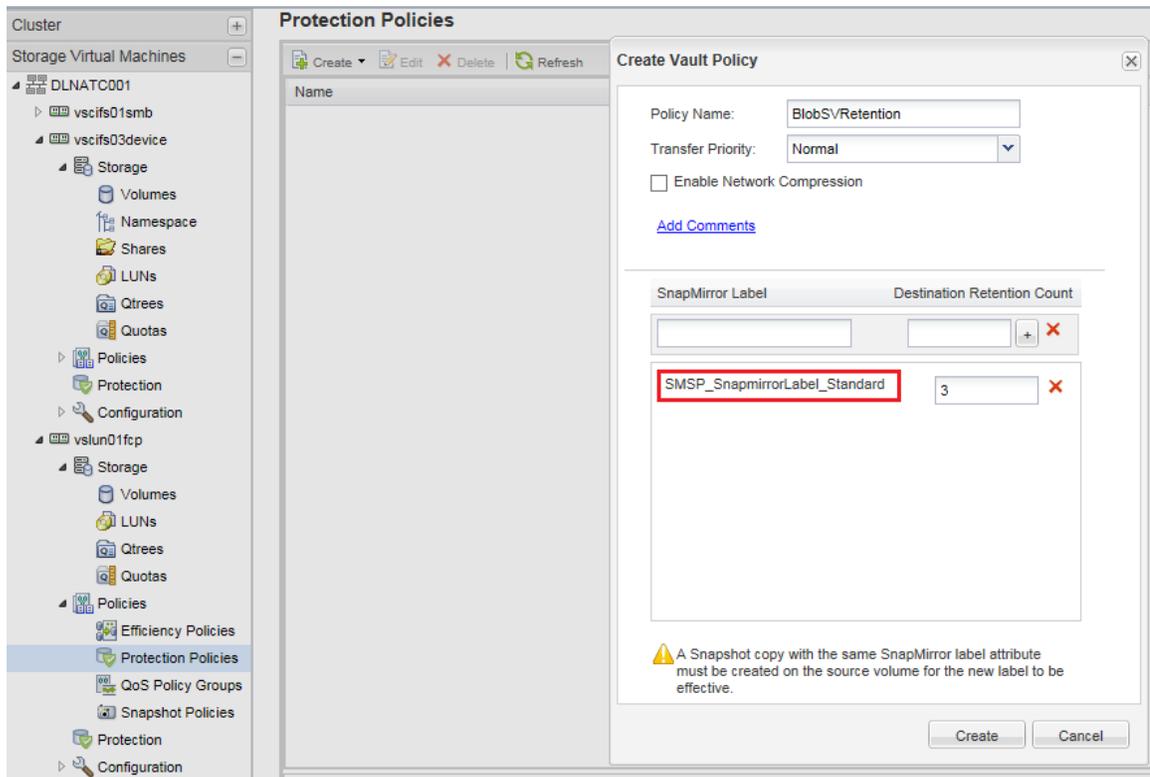


Figure 43: Configuring the Snapmirror-Label.

2. Update the SnapVault relationship for the SMSQL destination volume and the SnapVault destination volume with the newly created Vault Policy:

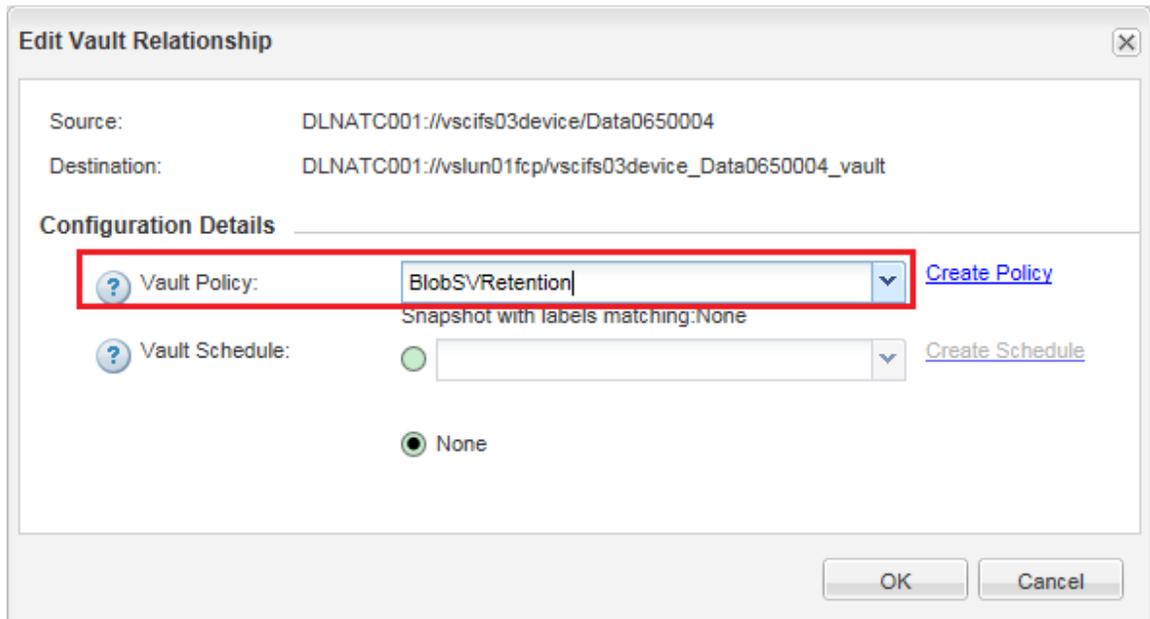
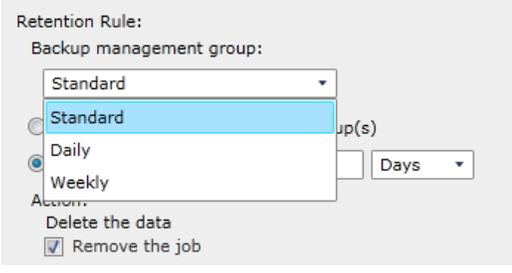


Figure 44: Configuring Vault Policy.

- The SnapMirror-label of local and remote backup snapshots for BLOB data are defined by DocAve 6 storage policy retention rule. Refer to the naming convention as follows:

DocAve 6 Storage Policy Retention Rule	Backup Management Group	BLOB Snapshot SnapMirror-Label
With Enable retention rule deselected 	Standard	DocAve 6_SnapmirrorLabel_ Standard
With Enable retention rule selected: 	Standard	DocAve 6_SnapmirrorLabel_ Standard
	Daily	DocAve 6_SnapmirrorLabel_ Daily
	Weekly	DocAve 6_SnapmirrorLabel_ Weekly

- The selected backup management group of the DocAve 6 storage policy retention rule must be the same as the **RetentionGroup** configured in the Vault Policy.

In this example, select **Standard** as the backup management group and keep the snapshots for the last four backup jobs.

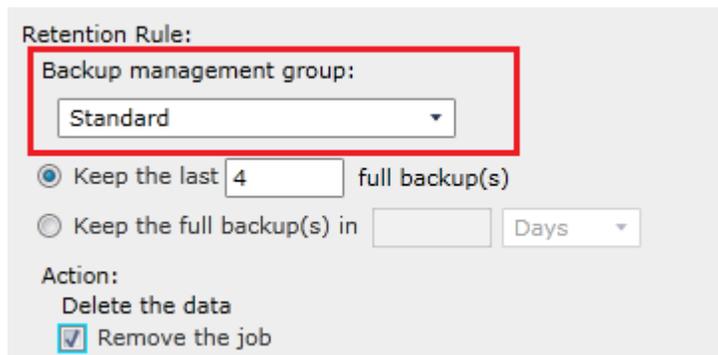


Figure 45: Configuring DocAve 6 storage policy retention rule.

- In DocAve 6, select the **Update SnapVault for device after operation** option in the **BLOB Settings** field, when configuring the schedule settings or the settings on **Run Now** interface. The remote snapshots of BLOB backup data will be generated in SnapVault destination storage during the backup job and the SnapMirror-label of the remote snapshots will be the same as the local snapshots.

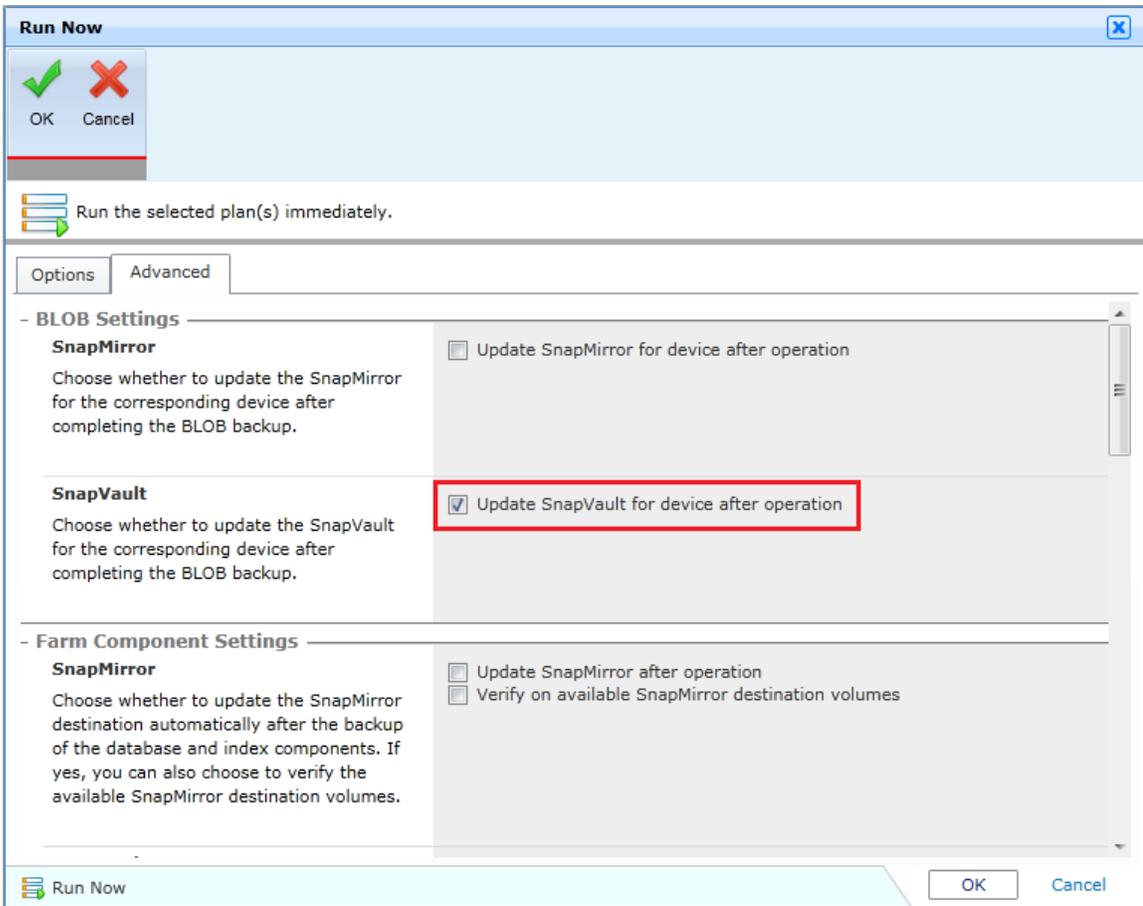


Figure 46: Configuring SnapVault settings in BLOB Settings field.

- After running the DocAve 6 Platform Backup for NetApp Systems job, check the local and remote snapshots in the clustered NetApp Data ONTAP storage server. It shows that the SnapMirror-Label of the remote snapshots on the SnapVault destination storage is the same as the SnapMirror-Label defined in the Vault Policy, that is, the retention of the remote snapshots of BLOB data generated by DocAve 6 can be controlled by SnapVault server.

```

DENATC001::volume snapshot> show -volume Data0650004 -vserver vscifs03device -fields snapmirror-label
vserver      volume      snapshot
-----
vscifs03device Data0650004 SMSP_FB20150215145343813447_Device_6f13a3765ef4bef8 SMSP_SnapmirrorLabel_Device2
vscifs03device Data0650004 SMSP_FB20150215165521278961_Device_6d52f2b7a718ae8c SMSP_SnapmirrorLabel_Device2
vscifs03device Data0650004 SMSP_FB20150216144043398521_6293a5684f18e73f SMSP_SnapmirrorLabel_Standard
vscifs03device Data0650004 SMSP_FB20150216145155837291_9f718e6a38d302c7 SMSP_SnapmirrorLabel_Standard
vscifs03device Data0650004 SMSP_FB20150216145921837018_89264f719ac063e6 SMSP_SnapmirrorLabel_Standard
vscifs03device Data0650004 SMSP_FB20150216160926849301_938e910fd810ff28 SMSP_SnapmirrorLabel_Standard
6 entries were displayed.

DENATC001::volume snapshot> show -volume vscifs03device_Data0650004_vault -vserver vslun01fcp -fields snapmirror-label
vserver      volume      snapshot
-----
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150215143542816187_Device_9d3235522b1fc284 SMSP_SnapmirrorLabel_Device2
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150215145343813447_Device_6f13a3765ef4bef8 SMSP_SnapmirrorLabel_Device2
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150215165521278961_Device_6d52f2b7a718ae8c SMSP_SnapmirrorLabel_Device2
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150216145155837291_9f718e6a38d302c7 SMSP_SnapmirrorLabel_Standard
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150216145921837018_89264f719ac063e6 SMSP_SnapmirrorLabel_Standard
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150216160926849301_938e910fd810ff28 SMSP_SnapmirrorLabel_Standard
6 entries were displayed.

DENATC001::volume snapshot>

```

Figure 47: Viewing the snapshots.

Storage Policy Device Retention Configuration

The following is an example of the retention configuration for the storage policy device of NetApp FAS CIFS share in the clustered NetApp Data ONTAP 8.2 SnapVault environment:

1. Create a XDP SnapVault policy using NetApp OnCommand System Manager. The SnapMirror-label must be in the format of **DocAve 6_SnapmirrorLabel_Device2**.

In this case, enter the **DocAve 6_SnapmirrorLabel_Device2** as SnapMirror-label and keep **3** snapshots.

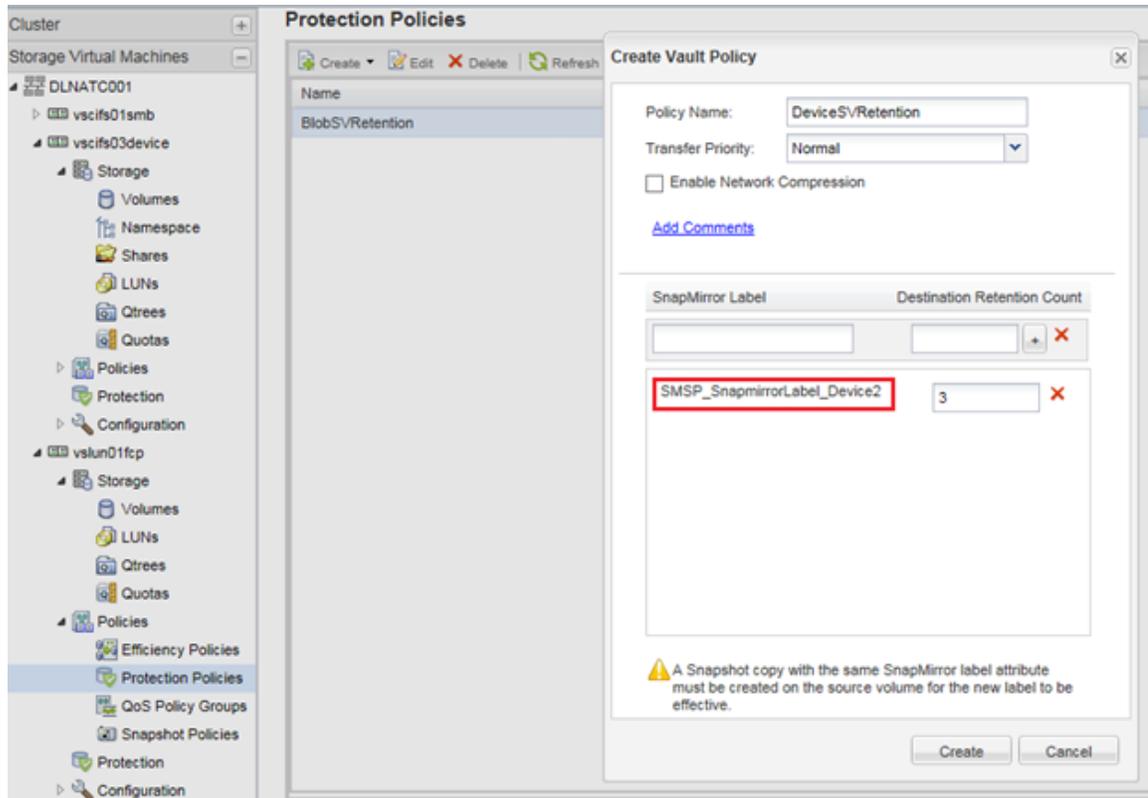


Figure 48: Configuring the Snapmirror Label.

2. Update the SnapVault relationship for the destination volume and the SnapVault destination volume with the newly created Vault Policy:

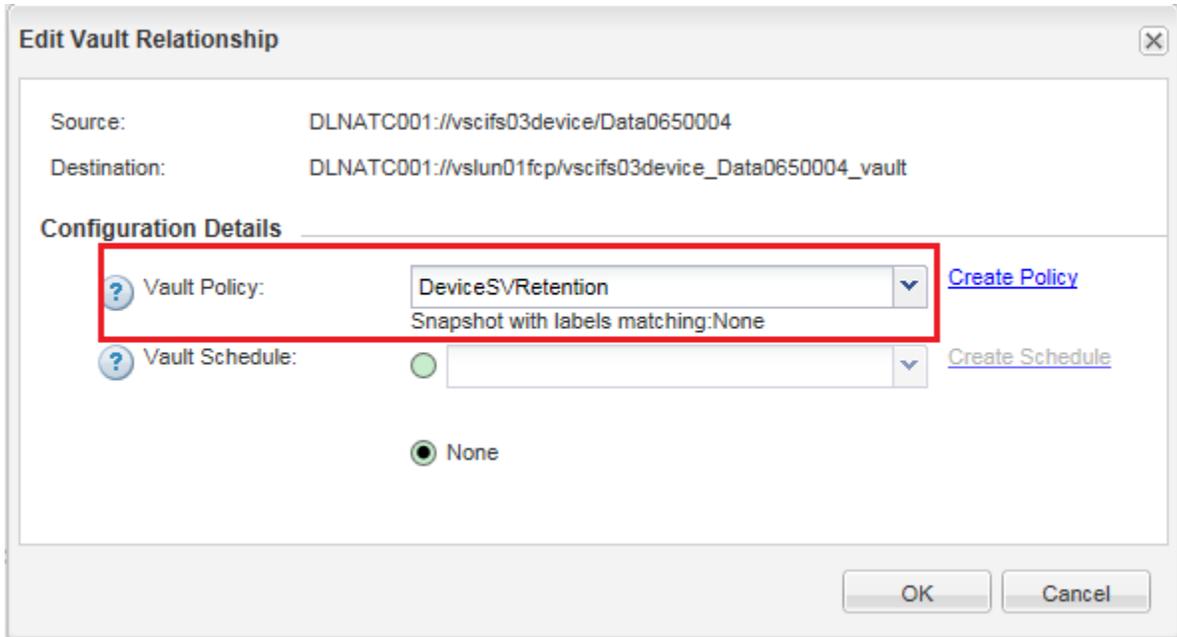


Figure 49: Configuring Vault Policy.

3. The SnapMirror-label of local and remote backup snapshots for storage policy device are “DocAve 6_SnapmirrorLabel_Device2”. In DocAve 6, select the **Update SnapVault for device after operation** option in the **Storage Policy Settings** field, when configuring the schedule settings or the settings on **Run Now** interface. The SnapMirror-label of the local snapshots for the storage policy devices will be **DocAve 6_SnapmirrorLabel_Device2**, and then update the local snapshots to the SnapVault destination storage. The remote snapshots of storage policy devices will be generated in SnapVault destination storage during the backup job and the SnapMirror-label of the remote snapshots will be the same as the local snapshots.

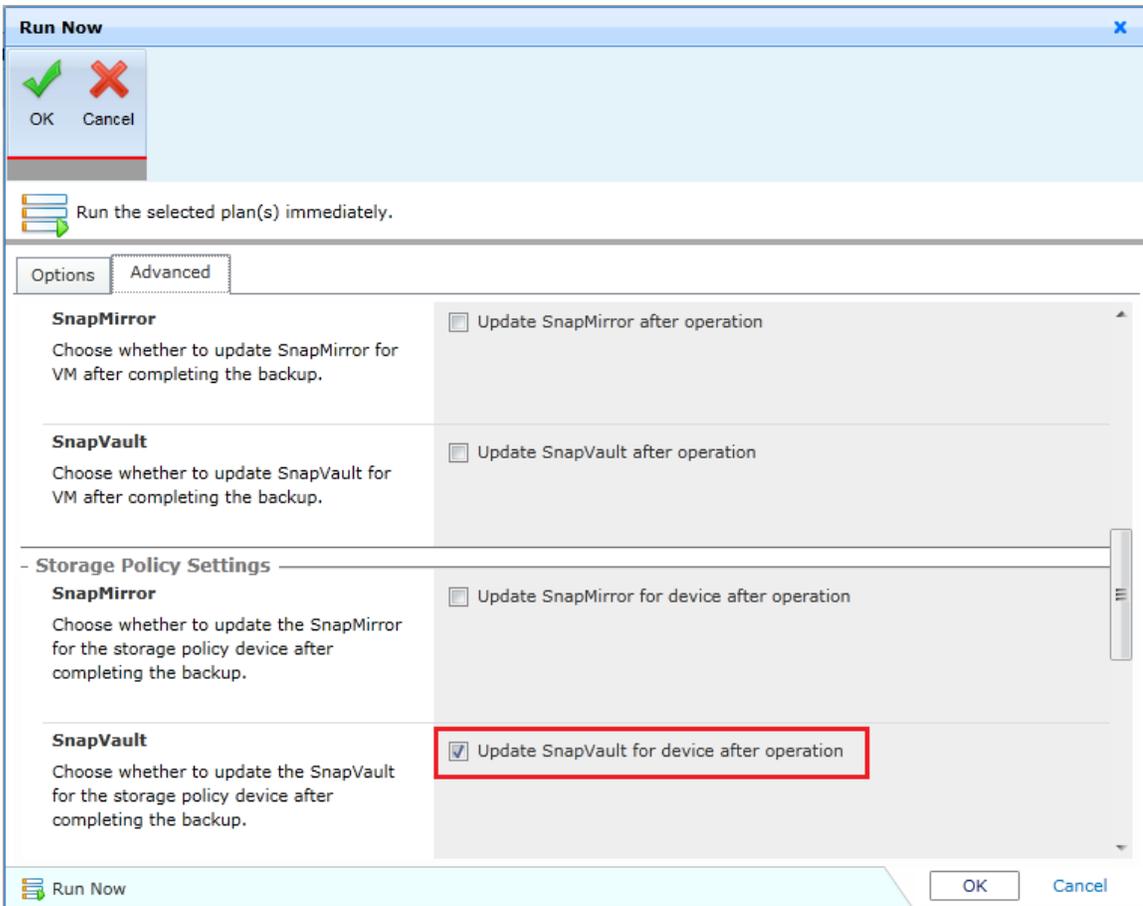


Figure 50: Configuring SnapVault settings in the Storage Policy Settings field.

4. After running the DocAve 6 Platform Backup job, check the local and remote snapshots in the Cluster Mode server. It shows that the SnapMirror-Label of the remote snapshots on the SnapVault destination storage are the same as the SnapMirror-Label defined in the Vault Policy, that is, the retention of the remote snapshots of storage policy device generated by DocAve 6 can be controlled by SnapVault server.

```

DENATC001::volume snapshot> show -volume Data0650004 -vserver vscifs03device -fields snapmirror-label
vserver      volume      snapshot
-----
vscifs03device Data0650004 SMSP_FB20150215145343813447_Device_6f13a3765ef4bef8 SMSP_SnapmirrorLabel_Device2
vscifs03device Data0650004 SMSP_FB20150215165521278961_Device_6d52f2b7a718ae8c SMSP_SnapmirrorLabel_Device2
vscifs03device Data0650004 SMSP_FB20150216144043398521_6293a5684f18e73f SMSP_SnapmirrorLabel_Standard
vscifs03device Data0650004 SMSP_FB20150216145155837291_9f718e6a38d302c7 SMSP_SnapmirrorLabel_Standard
vscifs03device Data0650004 SMSP_FB20150216145921837018_89264f719ac063e6 SMSP_SnapmirrorLabel_Standard
vscifs03device Data0650004 SMSP_FB20150216160926849301_938e910fd810ff28 SMSP_SnapmirrorLabel_Standard
6 entries were displayed.

DENATC001::volume snapshot> show -volume vscifs03device_Data0650004_vault -vserver vslun01fcp -fields snapmirror-label
vserver      volume      snapshot
-----
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150215143542816187_Device_9d3235522b1fc284 SMSP_SnapmirrorLabel_Device2
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150215145343813447_Device_6f13a3765ef4bef8 SMSP_SnapmirrorLabel_Device2
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150215165521278961_Device_6d52f2b7a718ae8c SMSP_SnapmirrorLabel_Device2
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150216145155837291_9f718e6a38d302c7 SMSP_SnapmirrorLabel_Standard
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150216145921837018_89264f719ac063e6 SMSP_SnapmirrorLabel_Standard
vslun01fcp vscifs03device_Data0650004_vault SMSP_FB20150216160926849301_938e910fd810ff28 SMSP_SnapmirrorLabel_Standard
6 entries were displayed.

DENATC001::volume snapshot>

```

Figure 51: Viewing the snapshots.

Appendix D: Supported SharePoint Components

Refer to the sections below for information on what components in SharePoint 2010, SharePoint 2013, and SharePoint 2016 are supported in DocAve 6.

SharePoint 2010 Components Supported in Platform Backup and Restore for NetApp Systems

If you are backing up the whole content database and then restoring it using the database level restore, all of the Web parts are supported in Platform Backup and Restore for NetApp Systems.

If you are using the Platform granular restore, refer to the table below for the supported and unsupported Web parts in DocAve 6 Platform granular restore.

SharePoint 2010 Supported Web Parts

Web Part		Supported	Unsupported
Business Data	Business Data Actions	√	
	Business Data Connectivity Filter	√	
	Business Data Item	√	
	Business Data List	√	
	Business Data Related List	√	
	Chart Web Part		√
	Excel Web Access	√	
	Indicator Details	√	
	Status List	√	
	Visio Web Access	√	
Content Rollup	Categories	√	
	Content Query	√	
	Relevant Documents	√	
	RSS Viewer	√	
	Site Aggregator	√	
	Sites in Category	√	
	Summary Links	√	
	Table Of Contents	√	
	Web Analytics Web Part	√	
	WSRP Viewer	√	
XML Viewer	√		
Filters	Apply Filters Button		√
	Choice Filter	√	
	Current User Filter	√	

Web Part		Supported	Unsupported
	Date Filter	√	
	Page Field Filter	√	
	QueryString(URL) Filter	√	
	SharePoint List Filter	√	
	Text Filter	√	
Forms	HTML Form Web Part	√	
	InfoPath Form Web Part		√
Media and Content	Content Editor	√	
	Image Viewer	√	
	Media Web Part	√	
	Page Viewer	√	
	Picture Library Slideshow Web Part	√	
Outlook Web App	My Calendar	√	
	My contacts	√	
	My Inbox	√	
	My Mail Folder	√	
	My Tasks	√	
Search	Advanced Search Box	√	
	Dual Chinese Search	√	
	Federated Results	√	
	People Refinement Panel	√	
	People Search Box	√	
	People Search Core Results	√	
	Refinement Panel	√	
	Related Queries	√	
	Search Action Links	√	
	Search Box	√	
	Search Core Results	√	
	Search Paging	√	
	Search Statistics	√	
	Search Summary	√	
	Top Federated Results	√	
Social Collaboration	Contact Details	√	
	Note Board	√	
	Organization Browser	√	
	Site Users	√	
	Tag Cloud	√	
	User Tasks	√	

SharePoint 2010 Service Applications Supported for Restore

Refer to the table below for the supported and unsupported SharePoint 2010 service applications for DocAve 6 Platform Restore.

Service Application	Databases of the Service Application	Supported in In-place Restore
Access Services	This Service Application does not have a database	√
Application Registry Service	application registry service database	√
Business Data Connectivity Service	Bdc_Service_DB(Business Data Connectivity Database)	√
Excel Services Application	This Service Application does not have a database	√
Managed Metadata Service	Managed Metadata Service_Database(Service Application Database)	√
PerformancePoint Service Application	PerformancePoint Service Application_Database(Microsoft.PerformancePoint.Scorecards.BIMonitoringServiceDatabase)	√
Search Service Application	Search_Service_Application_DB(Administration Database) Search_Service_Application_CrawlStoreDB(Crawl Database) Search_Service_Application_PropertyStoreDB(Property Database)	√
Secure Store Service	Secure_Store_Service_DB(Secure Store Service Database)	√
SecurityToken Service Application	This Service Application does not have a database	√
State Service	StateService_Database(State Service Database Settings)	√

Service Application	Databases of the Service Application	Supported in In-place Restore
Session State Service	SessionStateService_Database	√
SQL Server Reporting Service	Reporting Service Database Reporting Service Alerting Database Reporting Service Temp Database	√
User Profile Service Application	User Profile Service Application_ProfileDB (Microsoft.Office.Server.Administration.ProfileDatabase) User Profile Service Application_SyncDB(Microsoft.Office.Server.Administration.SynchronizationDatabase) User Profile Service Application_SocialDB (Microsoft.Office.Server.Administration.SocialDatabase)	√
Visio Graphics Service	This Service Application does not have a database	√
Web Analytics Service Application	WebAnalyticsServiceApplication_StagingDB(Web Analytics Staging Database) WebAnalyticsServiceApplication_ReportingDB(Web Analytics Warehouse Database)	√
Word Automation Services (Word Conversion Service)	WordAutomationServices_Database(Microsoft.Office.Word.Server.Service.QueueDatabase)	√
Lotus Notes Connector	N/A	×
Usage and Health data collection	WSS_Logging	√
Word Viewing Service	N/A	√
PowerPoint Service Application	N/A	√

Service Application	Databases of the Service Application	Supported in In-place Restore
Project Service Application	This Service Application does not have a database. Platform Backup and Restore for NetApp Systems backs up and restores the databases of the Project 2010 PWA site: ProjectServer_Published ProjectServer_Draft ProjectServer_Archive ProjectServer_Reporting	√
SQL Server PowerPivot Service Application	PowerpivotServiceApplication	√
Subscription Settings Service Application	Subscription Settings Database	√

SharePoint 2010 Components Supported for Restore

Refer to the table below for the supported and unsupported SharePoint 2010 components for DocAve 6 Platform Restore.

Features	Supported in In-place Restore	Notes
Configuration Database	√	
Central Admin Web Application	√	
Admin Content Database	√	
Web Application	√	
Content Database	√	
Global Search Settings	√	Farm-level search settings and Crawler impact rules are supported.
SharePoint Help Search	√	

Features	Supported in In-place Restore	Notes
InfoPath Form Services	√	InfoPath Forms Services Settings and InfoPath Forms Services Form templates are supported.
FBA Databases	√	The FBA Database and some configurations in the Web.config under WebApp IIS Setting (such as MemberShipProvider) are supported.
Solutions	√	For in place restore, restoring the uploaded solution and its status in the Solution Management is supported.
FAST Search Server 2010 for SharePoint	√	DocAve 6 Platform Backup and Restore for NetApp Systems backs up FAST components, configuration files, index data and so on. You can also refer to the link below for the manual full backup and restore of FAST Search Server: http://technet.microsoft.com/en-us/library/ff460221.aspx
Knowledge Lake Imaging	√	
BLOB	√	
NewsGator	√	Social Sites (NewsGator) 1.2 and 2.5 are supported from DocAve 6.
Nintex Workflow	√	Nintex workflows can be restored to their original location where they were backed up.

Features	Supported in In-place Restore	Notes
Farm Level Backup and Item Level Restore	√	If you want to do Platform granular Restore, the Platform granular Restore index must be generated.
Web Front-End Server	√	<ul style="list-style-type: none"> IIS Settings (such as Form Authentication, SSL certification and so on) can be configured individually on the Web front-end server; they are not saved in SharePoint. SharePoint Template directory is the most important directory to record the IIS extensions. Files such as feature files and site definition files in the Web front-end server are saved in this directory. DocAve 6 Platform Backup and Restore for NetApp Systems can also backup and restore the files in the file system of the Web front-end server.

SharePoint 2013 Components Supported in Platform Backup and Restore for NetApp Systems

SharePoint 2013 Service Application Supported for Restore

Refer to the table below for the supported and unsupported SharePoint 2013 service applications for DocAve 6 Platform Restore.

Service Application	Databases of the Service Application	Supported in In-place Restore
Access Services	This Service Application does not have a database	√
Access Services 2010	This Service Application does not have a database	√

Service Application	Databases of the Service Application	Supported in In-place Restore
App Management Service	AppMng_Service_DB (App Management Database)	√
Business Data Connectivity Service	Bdc_Service_DB(Business Data Connectivity Database)	√
Excel Services Application	This Service Application does not have a database	√
Lotus Notes Connector	N/A	×
Machine Translation Service	Machine Translation_Database	√
Managed Metadata Service	Managed Metadata Service_Database(Service Application Database)	√
PerformancePoint Service Application	PerformancePoint Service Application_Database(Microsoft.PerformancePoint.Scorecards.BIMonitoringServiceDatabase)	√
PowerPoint Conversion Service Application	This Service Application does not have a database	√
Project Service Application	This Service Application does not have a database . Platform Backup and Restore for NetApp Systems backs up and restores the databases of Project 2013 PWA site: ProjectWebApp	√
Search Service Application	Search_Service_Application_DB(Administration Database) Search_Service_Application_AnalyticsReportingStoreDB(Analytics Reporting Database) Search_Service_Application_CrawlStoreDB(Crawl Database) Search_Service_Application_LinksStoreDB(Link Database)	√
Secure Store Service	Secure_Store_Service_DB(Secure Store Service Database)	√
Security Token Service Application	This Service Application does not have a database	√
Session State Service	SessionStateService_Database	√
State Service	StateService_Database(State Service Database Settings)	√
Subscription Settings Service Application	Subscription Settings Database	√
SQL Server Reporting Service	Reporting Service Database Reporting Service Alerting Database Reporting Service Temp Database	√
SQL Server Powerpivot Service Application	PowerpivotServiceApplication	√

Service Application	Databases of the Service Application	Supported in In-place Restore
Usage and Health data collection	WSS_Logging	√
User Profile Service Application	User Profile Service Application_ProfileDB (Microsoft.Office.Server.Administration.ProfileDatabase) User Profile Service Application_SyncDB(Microsoft.Office.Server.Administration.SynchronizationDatabase) User Profile Service Application_SocialDB (Microsoft.Office.Server.Administration.SocialDatabase)	√
Visio Graphics Service	This Service Application does not have a database	√
Word Automation Services(Word Conversion Service)	WordAutomationServices_Database(Microsoft.Office.Word.Server.Service.QueueDatabase)	√
Workflow Service Application	N/A	√
Work Management Service	This Service Application does not have a database	√

SharePoint 2013 Components Supported for Restore

Refer to the table below for the supported and unsupported SharePoint 2013 components for DocAve 6 Platform Restore.

Features	Supported in In-place Restore	Notes
Web Application	√	
Content Database	√	
Configuration Database	√(Restore Database Only must be used)	
Central Admin Web Application	√	
Admin Content Database	√	
Solutions	√	For in place restore, restoring the uploaded solution and its status in the Solution Management is supported.
InfoPath Form Services	√	InfoPath Forms Services Settings and InfoPath Forms Services Form templates are supported.
Global Site Template	√	
Custom DB	√	
Web Front-End Server	√	
Item Level Restore	√	
FBA Databases	√	The FBA Database and some configurations in the Web.config under WebApp IIS Setting (such as MemberShipProvider) are supported.
BLOB	√	
NewsGator	√	Social Sites (NewsGator) 4.0/5.0 for SharePoint 2013 is supported in DocAve 6 8.2.
Nintex Workflow	√	Nintex workflows can be restored to their original location where they were backed up.

SharePoint 2016 Components Supported in Platform Backup and Restore for NetApp Systems

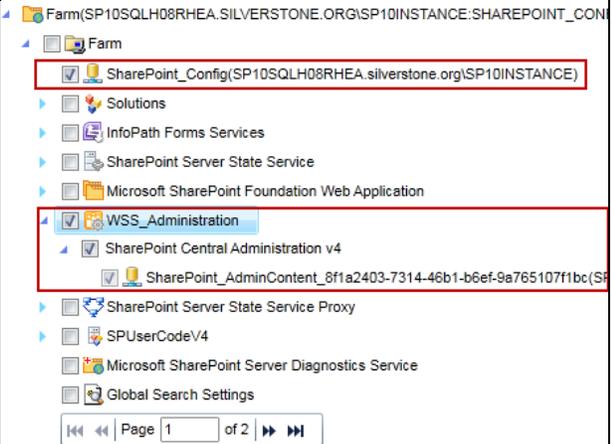
Refer to the table below for details on the SharePoint 2016 components supported in Platform Backup and Restore for NetApp Systems.

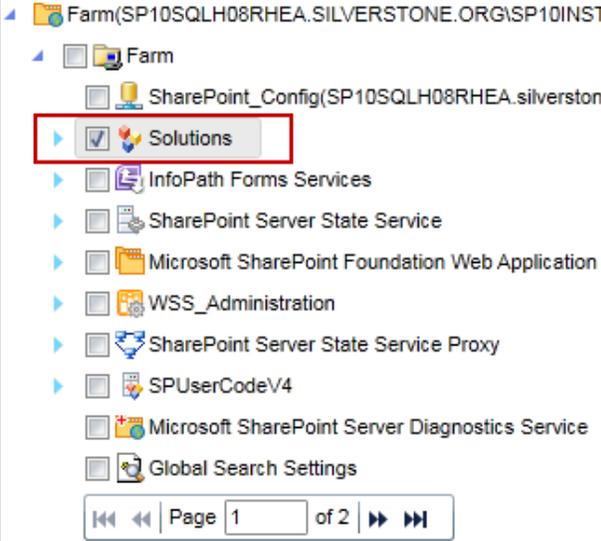
Components	Supported Status for In-place Restore
Access Service	Supported
Access Service 2010	Supported
APP Management Service	Supported
Business Data Connectivity Service	Supported
Machine Translation Service	Supported
Managed Metadata Service	Supported
PerformancePoint Service	Supported
PowerPoint Conversion Service	Supported
Secure Store Service	Supported
State Service	Supported
Usage and Health Service	Supported
User Profile Service	Supported
Visio Graphics Service	Supported
Subscription Service	Supported
Word Automation	Supported
Workflow Service	Supported
Solution	Supported
InfoPath Service	Supported
FBA	Supported
Global Site Template	Supported
Web Front-End Server	Supported
Configuration Database	Supported
Admin Content Database	Supported
Web Application	Supported
License to Feature Mappings	Supported
Global Search Settings	Supported
Session State Service	Supported
Custom Database	Supported
BLOB	Supported
Project Server Service Application	Supported
Search Service Application	Supported

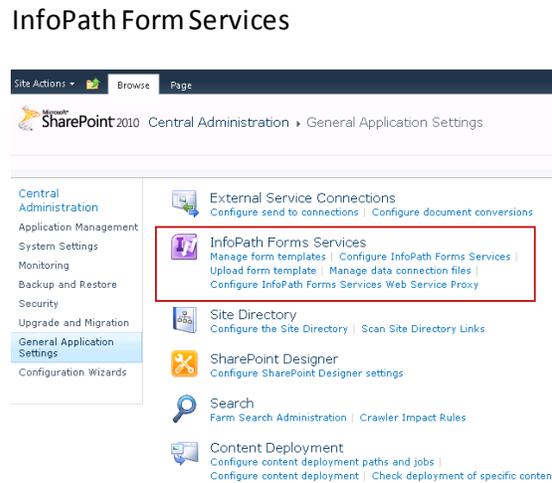
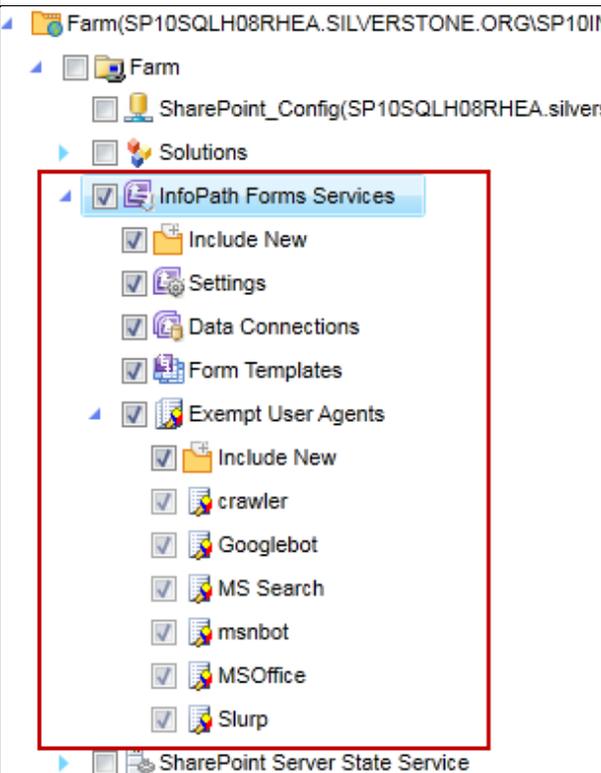
Platform Restore for NetApp Systems Support Table

***Note:** Before you restore any content at the selected restore granularity, make sure that the related higher-level SharePoint objects are restored at the farm level or database level. For example, if you want to use the customized feature correctly, you must restore the backed up features in the **Custom Features** node prior to restoring any SharePoint content that use this feature.

√ means the restore is **Supported** at this level and a blank area means the restore is **Not Supported** at this level.

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Central Administration and SharePoint Configuration Database		√	√						<p>The SharePoint configuration database and the SharePoint Central Administration database are related to each other; they can only be restored using In Place restore (with the Restore Raw Database option enabled).</p> <p>If you do not select the Restore Database Only option, these nodes will be skipped in the restore job (even if you have selected to restore them).</p>	 <p>The screenshot shows a tree view of restore options for a SharePoint farm. The 'SharePoint_Config' node is selected with a checkmark. Under 'WSS_Administration', the 'SharePoint Central Administration v4' node is also selected with a checkmark. Other nodes like 'Solutions', 'InfoPath Forms Services', and 'SharePoint Server State Service' are not selected.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Solutions		√	√						 <p>The screenshot shows a tree view of restore options for a SharePoint farm. The 'Solutions' folder is selected and highlighted with a red box. Other options include InfoPath Forms Services, SharePoint Server State Service, Microsoft SharePoint Foundation Web Application, WSS_Administration, SharePoint Server State Service Proxy, SPUserCodeV4, Microsoft SharePoint Server Diagnostics Service, and Global Search Settings. A pagination bar at the bottom indicates 'Page 1 of 2'.</p>	

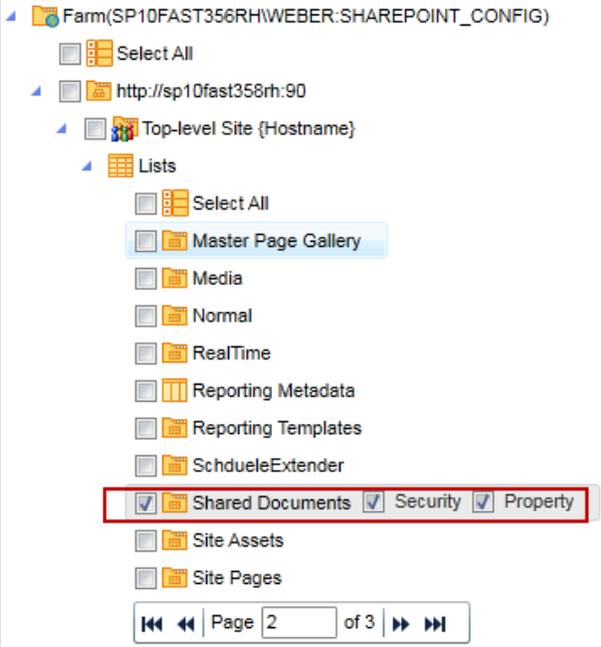
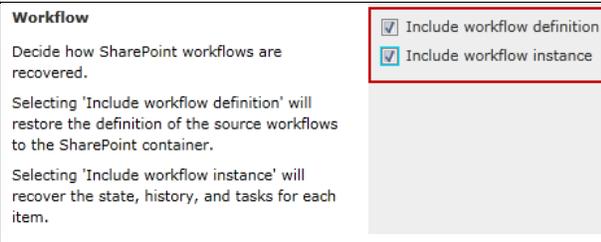
What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
		✓	✓							

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
License to Feature Mappings		√							This feature is specific to SharePoint 2013 and SharePoint 2016.	<p>The screenshot shows a tree view of restore options for a SharePoint farm. The 'License to Feature Mappings' option is selected and highlighted with a red box. Other options include SharePoint Config, Solutions, InfoPath Forms Services, SharePoint Server State Service, Microsoft SharePoint Foundation Web Application, WSS_Administration, SharePoint Server State Service Proxy, SPUserCodeV4, and Microsoft SharePoint Server Diagnostics Service. A pagination bar at the bottom indicates 'Page 1 of 2'.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Server State Service		√	√						<p>The screenshot shows a tree view of restore options for a SharePoint farm. Two items are highlighted with red boxes: 'SharePoint Server State Service' (with its sub-item 'State Service') and 'SharePoint Server State Service Proxy' (with its sub-item 'State Service'). Other visible options include 'Solutions', 'InfoPath Forms Services', 'Microsoft SharePoint Foundation Web Application', 'WSS_Administration', 'SPUserCodeV4', 'Microsoft SharePoint Server Diagnostics Service', and 'Global Search Settings'. A pagination bar at the bottom indicates 'Page 1 of 2'.</p>	

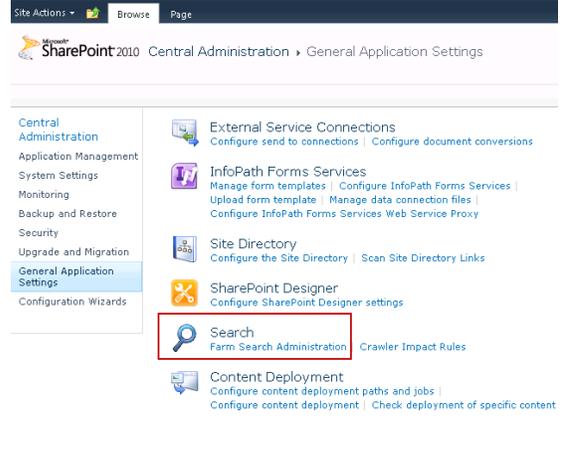
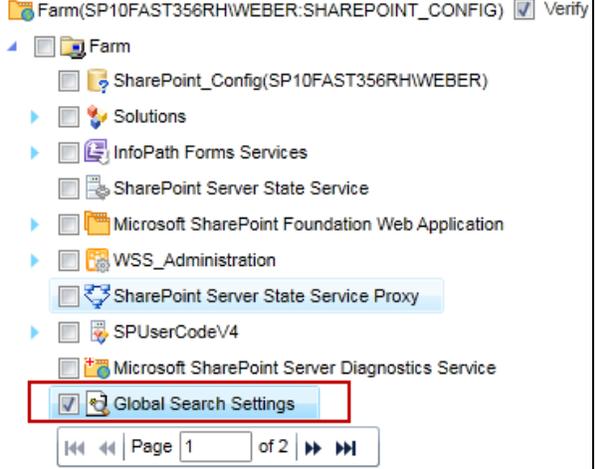
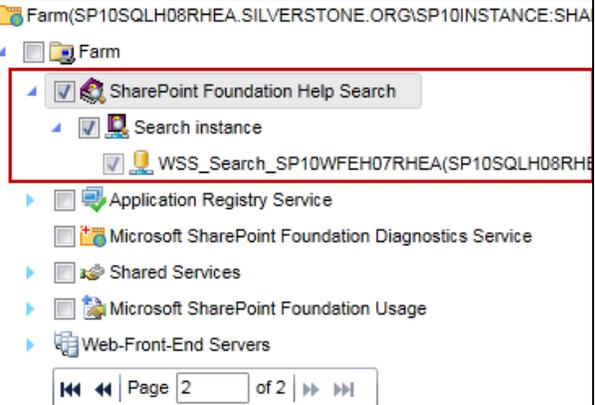
What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Web Application		√	√						<p>If you choose to overwrite an existing target Web application using a backed-up Web application with the same name in an In Place restore, the content database of the target Web application will be deleted and replaced with the one in the backup. However, the properties of the target Web application will not be deleted.</p> <p>For Web applications with extended zones, you can configure the extended zones after clicking Show Other Zone Information.</p>	

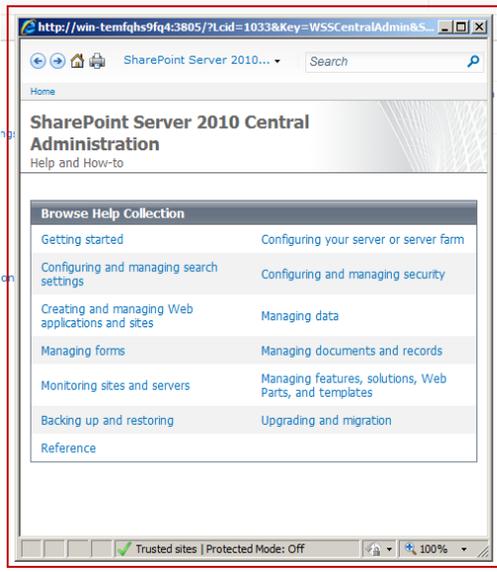
What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Content Database		√	√	√	√	√	√	√	Features can be restored at farm level, database level, site collection level, and site level. However, when restoring at site collection and site level, SnapManager only restores the existing status and using status of this feature; it does not restore the features' physical files, which are in ... \Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\FEATURES.	<p>The screenshot shows a tree view of a SharePoint farm. The 'WSS_Content_5555' folder is selected and highlighted with a red box. Other visible items include 'SharePoint_Config', 'Solutions', 'InfoPath Forms Services', 'SharePoint Server State Service', 'Microsoft SharePoint Foundation Web Application', 'Include New', 'Timer Jobs Group', 'SharePoint - header443443', 'SharePoint - header80', 'WSS_Administration', 'SharePoint Server State Service Proxy', 'SPUserCodeV4', 'Microsoft SharePoint Server Diagnostics Service', and 'Global Search Settings'.</p>
Sites with Content Types		√	√	√	√				The content types in the site/site collection will be restored together with the site/site collection.	<p>The screenshot shows a 'Backup Data' window with 'Single Point View' selected. The tree view shows a farm with a site selected. The site selection options are checked: 'http://sp13ca03268', 'Security', 'Property', and 'Top-level Site (connector)'. A 'Select All' button is also visible.</p>

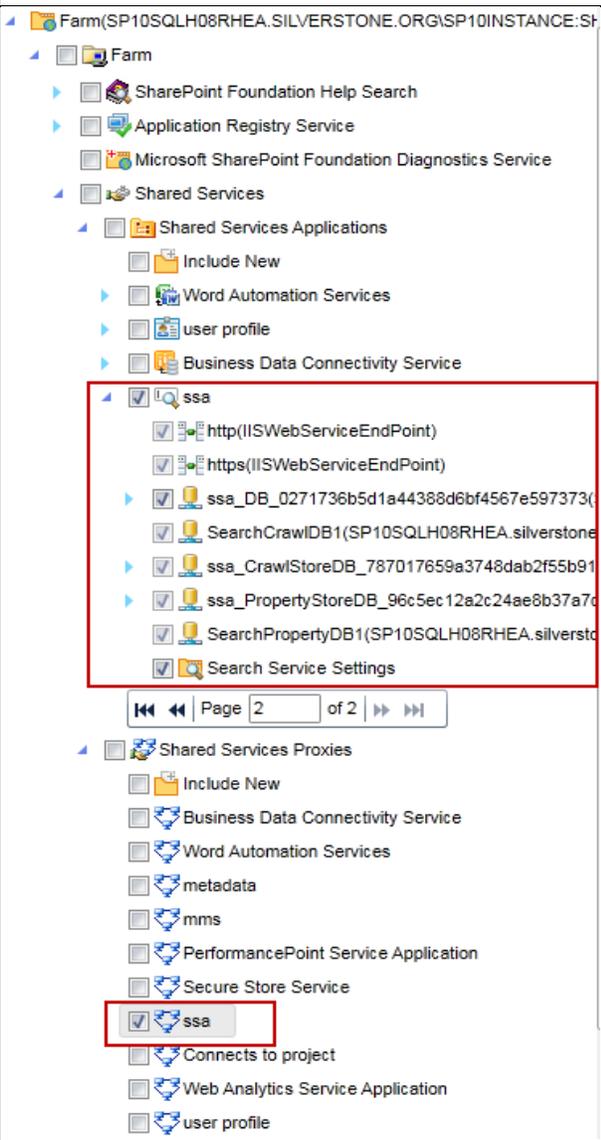
What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Lists with Content Types		√	√	√	√	√			The content types in the list will be restored together with the list.	
SharePoint Built-in Workflow		√	√	√	√	√	√	√	If you want to restore the workflow, you must select the SharePoint object that is associated with the workflow on the tree, and check the checkbox in front of Include workflow definition/Include workflow instance . If you are restoring the whole database, the workflow will be restored together with the database, so there are no such options.	

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Designer Customizations		√	√	√	√	√	√	√	The SharePoint Designer customizations can be restored together with the selected content in the content database.	N/A
Web Part		√	√	√	√	√	√	√	If you want to restore Web parts, make sure the content you selected on the backup tree contains the Web parts you want to restore. The content you selected on the tree can be navigated down to page and page version level.	N/A
Lists and items with Managed Metadata		√	√	√	√	√	√	√	If you want to restore an item that uses managed metadata term sets, make sure the related managed metadata service is successfully restored at the database level first. Otherwise, the item cannot be associated with the specified managed metadata term sets.	N/A
Sites with Custom Templates		√	√	√	√				If the custom template is generated from the SharePoint built-in site templates (typically from "Save site as template"), it will be restored together with the site.	N/A

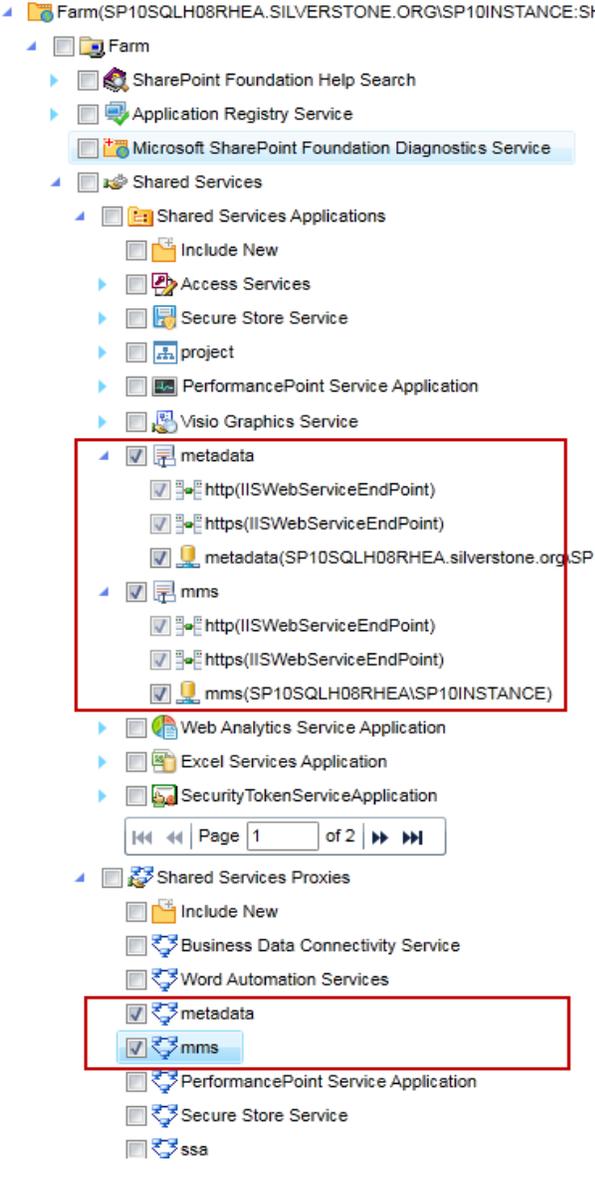
What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
									If the custom template is written by the customer, it may not be usable after a Platform restore job because of template variation.	
SPUserCode V4		√	√						Type: Microsoft SharePoint Foundation Sandboxed Code Service Description: Settings for the Sandboxed Code Service.	

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)	
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level			
Global Search Settings											
SharePoint Foundation Help Search									<p>Type: Index files and Databases</p> <p>Description: Search instances for Microsoft SharePoint Foundation</p> <p>*Note: The SharePoint Foundation Help Search is specific for SharePoint 2010.</p>		

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
 <p>The screenshot shows the 'Browse Help Collection' page in the SharePoint Server 2010 Central Administration console. The page lists various help topics such as 'Getting started', 'Configuring and managing search settings', 'Creating and managing Web applications and sites', 'Managing forms', 'Monitoring sites and servers', 'Backing up and restoring', and 'Reference'. The 'Backing up and restoring' link is highlighted.</p>										

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Search Service Application		√	√						<p>Search Service Settings: It is a virtual node that does not exist in SharePoint and it contains the following components:</p> <ul style="list-style-type: none"> • Content Source • Crawl Rules • File Types • Crawl Impact Rules • Authentication Pages • Federated Locations • Metadata Properties • Scopes <p>The Search Service Settings node backs up the properties of the search service application, so this node can only be restored to a search service application when performing an out of place restore.</p> <p>For Restore Exported Federated Location, you can select No to back up the properties and then restore them; or you can select Yes to Export the federated location and then Import it.</p> <p>Index Partition and Query Component: Under the Server drop-down list, all SharePoint servers that can run the Search Service Instance will be displayed. Regardless of whether the service is enabled or not, the service can be restored normally. After the</p>	 <p>The screenshot shows the SharePoint 2010 interface for a farm. The 'Shared Services Applications' list is expanded, and the 'ssa' (Search Service Application) node is selected and highlighted with a red box. Below it, the 'Search Service Settings' node is also highlighted with a red box. The screenshot includes a page number 'Page 2 of 2' and various service icons like 'Business Data Connectivity Service', 'Word Automation Services', and 'Secure Store Service'.</p>

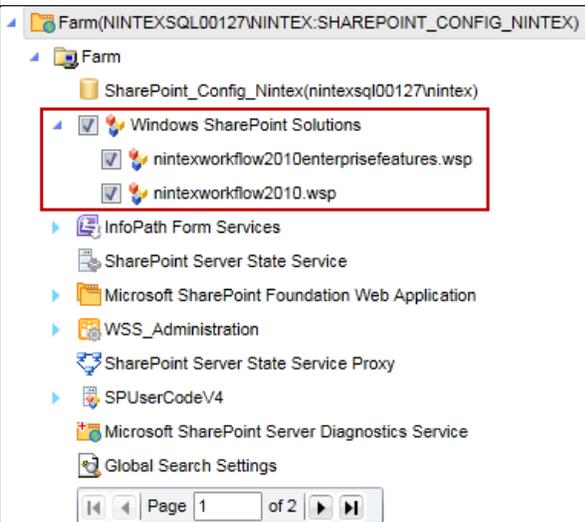
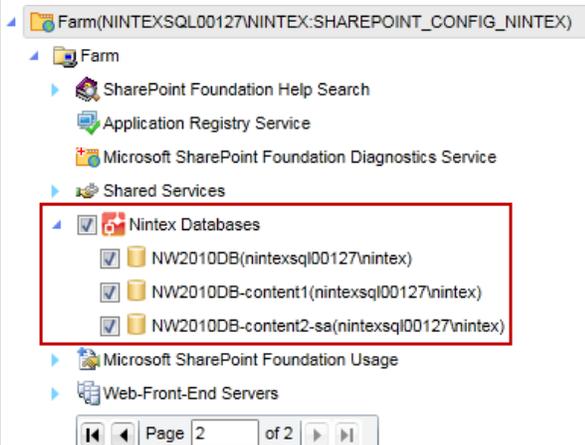
What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
									restore, the Search Service will be started on the specified SharePoint server.	

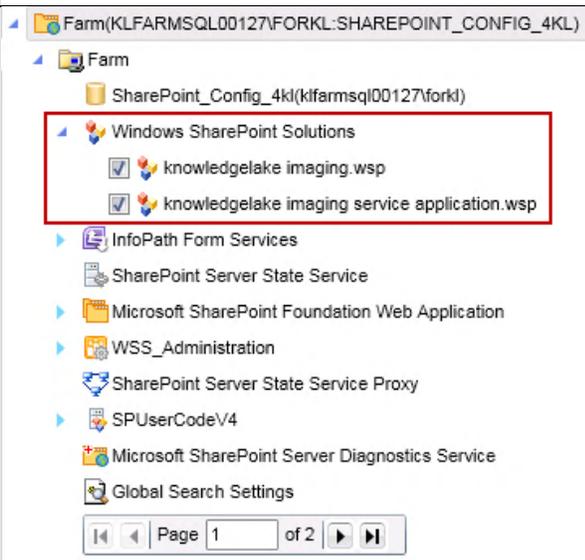
Service Application	√	√					<p>http (IISWebServiceEndPoint) and https (IISWebServiceEndPoint) are the EndPoint groups of the IIS Web Service. They are also called Service Application Endpoint Group in SharePoint.</p> <p>Service Applications that have no database or proxy: Access Services Service Application, Excel Services Application, and Visio Graphics Service Application.</p> <p>When restoring the service application proxy, a new proxy having the same name and type will be created in the target farm, and all of SharePoint will be restored and preserved.</p>	 <p>The screenshot shows the 'Farm' configuration page in SharePoint Central Administration. Under 'Shared Services Applications', the 'metadata' and 'mms' applications are expanded. For each, the 'http(IISWebServiceEndPoint)' and 'https(IISWebServiceEndPoint)' endpoints are checked. The 'mms' application also has a database endpoint checked. A red box highlights these endpoint configurations. Below, under 'Shared Services Proxies', the 'mms' proxy is also checked and highlighted with a red box.</p>
---------------------	---	---	--	--	--	--	--	--

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
FAST Search Server for SharePoint 2010 Farms		√	√						This feature is specific to SharePoint 2010.	<p>The screenshot shows the configuration console for a SharePoint farm. The tree view is expanded to 'FAST Search Server for SharePoint 2010 Farms'. Underneath, 'fast1000546.base.com (Admin)' is selected, and its sub-item 'FASTSearchAdminDatabase(10.2.38.56)' is also selected. A red box highlights this selection path. At the bottom, a pagination control shows 'Page 2 of 2'.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
NewsGator Social Site		√	√						<p>NewsGator 1.2 and 2.5 for SharePoint 2010 and NewsGator 4.0 and 5.0 for SharePoint 2013 are supported in Platform Backup and Restore for NetApp Systems.</p> <p>NewsGator Social Site must be installed in the target farm first.</p> <p>If you uninstalled the NewsGator Social Site and want to restore it, make sure all of the nodes are selected.</p> <p>Only In Place restore type is enabled when restoring NewsGator Social Site.</p> <p>If NewsGator Service exists in the farm, select Overwrite to overwrite the old files; if it has been uninstalled, either Overwrite or Skip can be used.</p>	

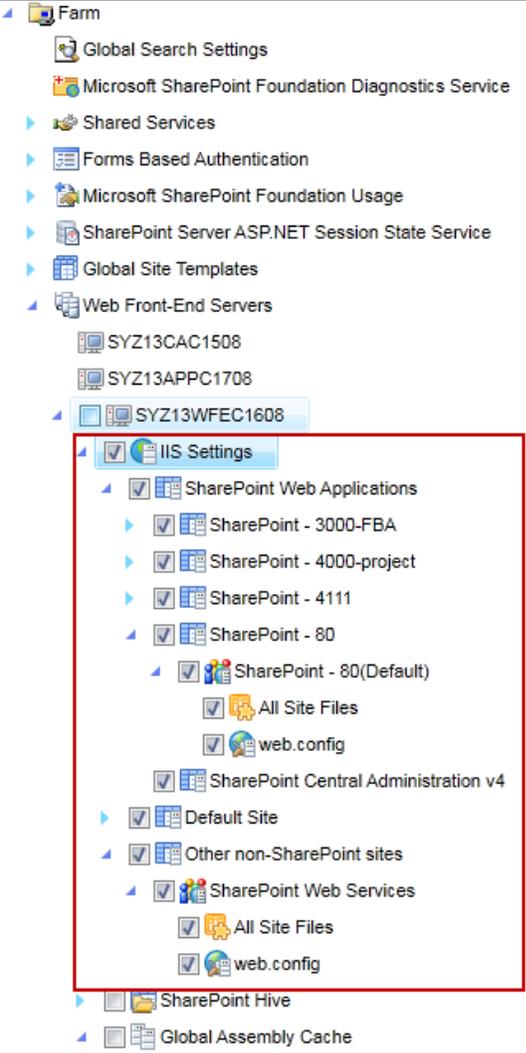
What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Nintex Workflow		√	√						<p>Nintex Workflow 2010 or Nintex Workflow 2013 must be installed in the target farm first.</p> <p>Only In Place restore type is enabled when restoring Nintex Workflow.</p> <p>If Nintex Workflow exists in the farm, select Overwrite to overwrite the old one; if it has been removed, either Overwrite or Skip can be used.</p>	 

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
KnowledgeLake Imaging 2010		√	√						<p>This feature is specific to SharePoint 2010.</p> <p>KnowledgeLake Imaging 2010 must be installed in the target farm first. To back up and restore the KnowledgeLake Imaging components, the KnowledgeLake Imaging service application solution must be deployed on each server in the SharePoint farm.</p> <p>Only In Place restore type is enabled when restoring KnowledgeLake Imaging 2010.</p> <p>If KnowledgeLake Imaging exists in the farm, select Overwrite to overwrite the old one; if it has been removed, either Overwrite or Skip can be used.</p>	 <p>The screenshot shows the 'Farm(KLFARMSQL00127\FORKL:SHAREPOINT_CONFIG_4KL)' configuration page. Under the 'Farm' section, 'SharePoint_Config_4kl(klfarmsql00127/forkl)' is expanded to show 'Windows SharePoint Solutions'. Two items are checked: 'knowledgelake imaging.wsp' and 'knowledgelake imaging service application.wsp'. Other services like 'InfoPath Form Services', 'SharePoint Server State Service', 'Microsoft SharePoint Foundation Web Application', 'WSS_Administration', 'SharePoint Server State Service Proxy', 'SPUserCodeV4', 'Microsoft SharePoint Server Diagnostics Service', and 'Global Search Settings' are also listed.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
										<p>The screenshot shows the 'Farm(KLFARMSQL00127\FORKL:SHAREPOINT_CONFIG_4KL)' tree view. The following items are selected and highlighted with red boxes:</p> <ul style="list-style-type: none"> KnowledgeLake Imaging Data <ul style="list-style-type: none"> kldata(klfarmsql00127\forkl) Shared Services Applications <ul style="list-style-type: none"> KnowledgeLake Imaging Service Application <ul style="list-style-type: none"> Default(IISWebServiceEndPoint) KnowledgeLake Imaging Service Application_e882d... Shared Services Proxies <ul style="list-style-type: none"> Search Service Application 1 <ul style="list-style-type: none"> KnowledgeLake Imaging Service Application <p>Other visible items include Application Registry Service, Microsoft SharePoint Foundation Diagnostics Service, SecurityTokenServiceApplication, Search Service Application 1, Microsoft SharePoint Foundation Usage, and Web-Front-End Servers. A pagination bar at the bottom indicates 'Page 2 of 2'.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Custom Database		√	√						You cannot select detailed content inside the database to restore. You can only restore the whole database.	<p>The screenshot shows a tree view of restore options. Under 'Customize Database', the 'WIN-TEMFQHS9FQ4' folder is expanded, and both 'WIN-TEMFQHS9FQ4' and 'ReportServer(WIN-TEMFQHS9FQ4)' are checked. A red box highlights this section.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
IIS Settings		√	√						<p>If the data you want to restore does not exist in the destination, the data will be restored to the destination regardless of whether you choose the Overwrite or Skip option.</p> <p>If the data you want to restore exists in the destination, the destination data will be overwritten by the backed up one if you select Overwrite option; if you select Skip option, the destination data will not be overwritten.</p>	

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Hive		√	√							

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Global Assembly Cache		√	√						<p>If the data you want to restore does not exist in the destination, the data will be restored to the destination regardless of whether you choose the Overwrite or Skip option.</p> <p>If the data you want to restore exists in the destination, the destination data will be overwritten by the backed up one if you select Overwrite option; if you select Skip option, the destination data will not be overwritten.</p>	

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Custom Features		✓	✓							<p>The screenshot shows a tree view of restore options for a SharePoint 2010 farm. The 'Custom Features' option is selected and highlighted with a red box. Other options include Application Registry Service, Microsoft SharePoint Foundation Diagnostics Service, Shared Services, Microsoft SharePoint Foundation Usage, FAST Search Server for SharePoint 2010 Farms, Web-Front-End Servers, SP10FAST357RH, IIS Settings, SharePoint Hive, Global Assembly Cache, SharePoint SiteDefinitions, and Extra File System Folders.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint SiteDefinitions		√	√							<p>The screenshot shows a tree view of restore options for a SharePoint farm. The 'SharePoint SiteDefinitions' option is selected and highlighted with a red box. Other options include Application Registry Service, Microsoft SharePoint Foundation Diagnostics Service, Shared Services, Microsoft SharePoint Foundation Usage, FAST Search Server for SharePoint 2010 Farms, Web-Front-End Servers, SP10FAST357RH, IIS Settings, SharePoint Hive, Global Assembly Cache, Custom Features, and Extra File System Folders.</p>

What to Restore	Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring (SharePoint 2010 Screenshots Shown Below)
				Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Extra File System Folders		√	√						<p>The screenshot shows a file explorer view of a SharePoint 2010 server. The path is C:\>SP10CA012RH>Extra File System Folders. The 'C:' drive is expanded, showing 'Files' and 'Folders'. Under 'Folders', 'Select All' is checked. Below it, several sub-folders are listed: '1', 'aa', 'bbb', 'ccc', 'Data', 'ddd', 'inetpub', 'jy', 'ODX test', and 'PerfLogs'. The 'bbb' folder is expanded, showing 'Files (All the objects are selected.)' and 'Folders'. A pagination bar at the bottom indicates 'Page 1 of 2'.</p>	

Platform Customization Table Notes

Below are the detailed notes that are referenced in the Platform Customization Table.

Workflow Definition and Instance

To restore workflow content, you must select the related checkboxes first.

- **Workflow Definition** – The user-created workflow definition in the site, list, or library. SharePoint built-in workflows, workflows defined by SharePoint Designer, and workflows defined by Nintex are supported. Workflows defined by Visio Studio are not supported.
- **Workflow Instance** – The item instance created upon the triggering of a workflow definition. This includes the workflow state, workflow history, and workflow tasks.
***Note:** The workflow instance of the SharePoint Designer workflow whose platform type is **SharePoint 2013 Workflow** is not supported being restored.

The workflow instance of the checked-out file is not supported being restored.

In order to restore the workflow definition and workflow instance correctly, the following requirements must be met:

- The workflow definition must be restored to the destination farm before restoring the workflow instance.
- The workflow feature must be enabled before you restore the workflow definition and workflow instance.

***Note:** All workflow instances whose status was **In Progress** when backed up will be **Cancelled** when restored to the destination.

Restoring Workflow Definitions

If there is an existing destination workflow definition that has the same name as one in the backup, then the backed-up workflow definition is not restored. Otherwise, the backed-up workflow definition is restored to the destination.

Restoring Workflow Instances

If the content that the workflow instance is based on is skipped during a restore, the workflow instance will not be restored. If the related content is restored to the destination but there is an existing destination workflow definition with the same name as one in the source, the backed-up workflow instance will be restored to the destination.

If there is no workflow definition for this workflow instance, it is skipped and the corresponding information is recorded in the logs.

Appendix E: SharePoint 2013 Social Features Supported in Platform Backup and Restore for NetApp Systems

Refer to the table below for the supported and unsupported SharePoint 2013 social features for DocAve 6 Platform Backup and Restore for NetApp Systems.

Social Feature		Granular Level Restore	Database Level Restore	Comment
My Site		Supported	Supported	
SkyDrive Pro (namely, OneDrive for Business)		Supported	Supported	
Blog		Supported	Supported	
Tag		Not Supported	Supported	The Tags are stored in Managed Metadata Service as System Term. It must be restored with Managed Metadata Service.
Microblog and Feed	Post	Supported	Supported	
	Reply	Supported	Supported	
	Like	Supported	Supported	
	Picture	Not Supported	Supported	
	Link	Supported	Supported	
	@	Not Supported	Supported	
	Mentions	Not Supported	Supported	
	Tag	Not Supported	Supported	The tags must be restored with Managed Metadata Service.
Follow	People	Supported	Supported	
	Site	Supported	Supported	
	Document	Supported	Supported	
	Tag	Not Supported	Supported	The tags must be restored with Managed Metadata Service.
Community Site	Categories	Supported	Supported	
	Discussion Board	Supported	Supported	
	Members	Supported	Supported	
	Budge	Supported	Supported	
	Reputation	Supported	Supported	
	Best Reply	Supported	Supported	
	Question	Supported	Supported	
	Community Settings	Supported	Supported	

Social Feature	Granular Level Restore	Database Level Restore	Comment
Community Portal	Supported	Supported	

Appendix F: SharePoint Object Security and Property

Refer to the table below for detailed information on the security and property of each SharePoint object.

Type	SharePoint Object	Attributes of the SharePoint Object which belongs to the specified Type
Security	Site Collection	Users and groups of the Site Collection
	Site	Mappings of the users and their permissions, Permission Levels, Groups, Users
	List	Mappings of the users and their permissions, Users, Groups
	Folder/Item/File	Mappings of the users and their permissions, Users, Groups
Property	Site Collection	Basic information used to create the Site Collection, Other information of the Site Collection, Site Features
	Site	Basic information used to create the Site, Other information of the Site, Site Columns, Site Content Types, Navigation, Site Features, Triggers for the users' actions in the Site
	List	Basic information used to create the List, Other information of the List, List Columns, List Content Types, Triggers for the users' actions in the List, Alert
	Folder/Item/File	Properties of the Folder/Item/File, Alert

Appendix G: Using Hot Key Mode in Platform Backup and Restore for NetApp Systems

DocAve 6 supports Hot Key mode, which allows you to perform actions quickly by using only the keyboard.

To access Hot Key mode, press **Ctrl+Alt+Z** simultaneously on the keyboard while in the Platform Backup and Restore for NetApp Systems interface.

The following is a list of hot keys for the Home page of the Platform Backup and Restore for NetApp Systems interface. To go back to the Home page of the Platform Backup and Restore for NetApp Systems interface, press **Ctrl+Alt+Z** on the keyboard.

For example, continue pressing **B** to go back to the **Backup** tab of Platform Backup and Restore for NetApp Systems.

Operation Interface	Hot Key
Backup	B
Restore	R
Clone	C
Plan Manager	P
DocAve Home Page	1
DocAve Online Community	2
Control Panel	3
Job Monitor	4
Plan Group	5
Health Analyzer	6
Logon Account	9
Help and About information	0

Backup Tab

The following is a list of hot keys for the **Backup** tab functions.

Functionality Name and Hot Key					
Plan Builder	P	Wizard Mode	W	Storage Policy	S
				Staging Policy	A
				Custom Database	U

Functionality Name and Hot Key												
				Command With Operation		ZO						
				Back		B						
				Next		N						
				Finish		F	Finish		F			
							Finish and Run Now		R			
							Finished and Test Run		T			
				Cancel		C						
				Form Mode		F	Storage Policy		SP			
							Staging Policy		A			
							Custom Database		U			
							Command With Operation		ZO			
							Save		V	Save		S
										Save and Run Now		R
				Save and Test Run		T						
Cancel		C										
Storage Policy	SP											
Verification and Index Policy	A	Create	N	Verification and Index Server		S		OK	O			
						Cancel		C				
				Verification and Index Server Group		G		OK	O			
						Cancel		C				
		Edit		E	OK		O					
					Cancel		C					
Delete		D										
Close		C										
Command With Operation	CO	Create	N	Configure		C		OK	O			
						Cancel		B				
				OK		O						
						Cancel		B				
		Edit		E	Configure		C		OK	O		
					Cancel		B					
					OK		O					
		Cancel		B								
Delete		D										
Close		C										
Migrate Database	MD	Back		B								
		Next		N								
		Start		F								
		Cancel		C								

Functionality Name and Hot Key			
Migrate Index	MI	Back	B
		Next	N
		Start	F
		Cancel	C
Job Monitor	J		

Restore Tab

The following is a list of hot keys for the **Restore** tab functions.

Functionality Name and Hot Key			
Restore	R		
Farm Rebuild	FB	Disconnect	D
		Restore	R
		Verify	V
		Connect	CO
		Back	B
		Next	N
		Finish	F
		Cancel	C
Farm Repair	FP	Repair	FP
		Close	C
Generate Index	GI	Verification and Index Policy	A
		Back	B
		Next	N
		Finish	F
		Cancel	C
Verification and Index Policy	A		
Command With Operation	ZO		
Job Monitor	J		

Time-based Restore

Functionality Name and Hot Key				
Time-based Restore	T	Create Container	OK	O
			Cancel	C
		Destination Physical Device	DP	
Load Remote Backups	L			

Functionality Name and Hot Key					
		Advanced Search	AS	Search	S
				Cancel	C
		Find Site Collection	Q		
		Verification and index Policy	ZC		
		Installed Programs	I	Close	X
		Download Backup List	DB	OK	O
				Cancel	C
		Back	B		
		Next	N		
		Finish	F		
Cancel	C				

Clone Tab

Functionality Name and Hot Key					
Farm Clone	FC	SQL Server Mapping	SM	Save	O
				Cancel	C
		SharePoint Server Mapping	SP	Save	O
				Cancel	C
		Index Location	I	Save	O
				Cancel	C
		Destination Physical Device	P	Save	O
				Cancel	C
		Back	B		
		Next	N		
Start	ST				
Cancel	CX				

Plan Manager Tab

The following is a list of hot keys for the **Plan Manager** tab functions.

Functionality Name and Hot Key					
View Details	V	Edit	E	Storage Policy	ZP
				Verification and Index Policy	ZC

Functionality Name and Hot Key							
				Custom Database	ZD		
				Command With Operation	ZO		
				Save	S	Save and Test Run	T
						Save and Run Now	R
						Save	S
				Save As	A		
				Cancel	C		
Plan Group	P						
Close	C						
Edit	E			Storage Policy	ZP		
				Verification and Index Policy	ZC		
				Custom Database	ZD		
				Command With Operation	ZO		
				Save	S	Save and Test Run	T
						Save and Run Now	R
						Save	S
Save As	A						
Cancel	C						
Delete	D						
Test Run	T						
Run Now	R	OK	O				
		Cancel	C				

Notices and Copyright Information

Notice

The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright

Copyright © 2016-2017 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks

AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes

The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor Jersey City, New Jersey 07311
USA