DocAve® 6 Platform Backup and Restore

User Guide

Service Pack 8, Cumulative Update 3

Issued April 2017

Table of Contents

What's New in this Guide 8

About DocAve Platform Backup and Restore 9

Complementary Products 9

Submitting Documentation Feedback to AvePoint 10

Before You Begin 11

AvePoint's Testing Policy and Environment Support 11

Supported Software Environments 11

Supported Hardware 11

Supported Backup and Recovery 11

Notable Environment Exceptions 12

Configuration 12

Agents 12

Required Permissions 13

Agent Account Configured on the SharePoint Agents Included in the Agent Group 13

Agent Account Configured on Other SharePoint Web Front-End Servers (Except for SQL Server and FAST Search Server) 14

Agent Account Configured on the FAST Search Server 15

Agent Account Configured on the Index Server 15

Agent Account Configured on the SQL Server 15

SQL Server Service Account Configured on the SQL Server 16

Agent Account Configured on Hyper-V hosted VM 16

Agent Account Configured on VMs hosted by ESX/ESXi or vCenter 17

Host Profile Account configured on ESX/ESXi or vCenter Host Server 17

Local System Permissions 18

Supported Operating System for Hyper-V Host Server 18

Supported ESXi Host Server Versions 19

Supported vCenter Host Server Versions 19

Supported Hardware in DocAve 6 Platform Backup and Restore 19

Health Analyzer 20

Getting Started 21

Launching Platform Backup and Restore 21
User Interface Overview 22
Navigating DocAve 22
Configuring Devices and Setting up Storage Policies 24
About the Staging Policy 25
Configuring a Staging Policy 26
About Command With Operation 28
Configuring a Script Profile 28
Managing Script Profiles 29
Configuring a Command Profile 29
Managing Command Profiles 30
About VM Script Profile 31
Configuring a VM Script Profile 31
Managing VM Script Profiles 31
About Migrator Tools 33
Migrate Database 33
Migrate Index 34
Overview of Backup Types 35
SharePoint Components Supported for Backup 37
SharePoint 2016 37
SharePoint 2013 37
SharePoint 2010 38
Using Plan Builder to Back Up Data 40
Using Wizard Mode to Create a Backup Plan 40
Backup Schedule 51
Manual Maintenance 55
Snapshot Retention Policy 56
Modifying BLOB Backup Settings in Configuration File 61
Using Form Mode to Create a Backup Plan 63
Running a Backup Job Immediately 63
Managing Plans 64
Configuring Run Now Interface 64

About InstaMount 69
InstaMount and Restore Index 69
About the Platform Backup and Restore for SQL Mirroring Database 70
About the Platform Backup and Restore for Databases in AlwaysOn Availability Group 71
About the Platform Backup and Restore for Failover Database 72
Performing a Restore 74
Building a Restore Plan 74
Building an In Place Restore Plan at Database Level 76
In Place Restoring From Third-Party Backup Data at Database Level 79
Building an In Place Platform Granular Restore Plan 79
Building an Out of Place Restore Plan at Database Level 86
Out of Place Restoring From Third-Party Backup Data at Database Level 90
Building an Out of Place Platform Granular Restore Plan 92
Restoring a Raw Database 101
Restoring Backed-Up VMs 102
Restoring Backed-Up Web Front-End Files 104
Options for Restoring Backed-up Web Front-End Files 104
Restoring Backed-Up BLOB Data 104
Restoring Backed-Up Stub Database 105
Restoring Backed-Up Catalog Site Collection 108
Restoring Backed-Up Database Master Key 108
Deselecting the Restore Granular Content Feature 109
Restoring Details for Specific Farm Components 109
Performing a Disaster Recovery 111
About Farm Rebuild 113
Supported Farm Topology 113
Environment Configuration 113
Required Permissions 114
Farm Topologies Supported by Farm Rebuild 114
Farm Rebuild Cases 115
Restoring to the Original Farm 116
Restoring to a New Farm 116

Backing Up the Original Farm 117
Original SharePoint 2010 Farm Environment's Configuration 117
Original SharePoint 2013 Farm Environment's Configuration 121
Backing Up the Original Farm Using Platform Backup 124
Performing a DocAve Disaster Recovery 124
Performing a Farm Rebuild 125
Using VM Backup Data for Farm Rebuild 127
Using SharePoint Farm Backup Data for Farm Rebuild 129
Restoring Other Farm Components 133
Supported and Unsupported List of Farm Rebuild for SharePoint 2010 Farm 136
Supported Backup Methods for Farm Rebuild 136
Supported and Unsupported Farm Features for Farm Rebuild 136
Supported and Unsupported Service Applications for Farm Rebuild 137
Supported and Unsupported List of Farm Rebuild for SharePoint 2013 Farm 137
Supported Backup Methods for Farm Rebuild 137
Supported and Unsupported Farm Features for Farm Rebuild 137
Supported and Unsupported Service Applications for Farm Rebuild 138
Supported and Unsupported List of Farm Rebuild for SharePoint 2016 Farm 139
Helpful Notes When Performing the Farm Rebuild 139
Performing a Farm Clone 145
Restoring or Configuring Specific Components after Farm Clone 151
Restoring Search Service Application 151
Restoring Web Front-End Components 153
Configuring NewsGator after Farm Clone 153
Supported and Unsupported List of Farm Clone for SharePoint 2016 Farm 155
Helpful Notes about Farm Clone 155
Performing a Farm Clone with VM 157
Editing the Configuration File Before Cloning a French-display-language VM 158
Cloning the VM 158
Performing a Farm Repair 165
Checking a Job Status 166
Performing a Full Farm DocAve Platform Out of Place Restore 167

Backing up the Source Farm Using Platform Backup 167
Performing the Out of Place Platform Restore 168
Restoring Solutions, InfoPath Form Services and Global Search Settings 171
Restoring Web Applications and Content Databases 172
Restoring Service Applications 177
Restoring Backed up Web Front-End Servers Data 201
DocAve 6 Platform Backup and Restore Use Case 204
Backing up the Entire SharePoint Farm 204
Restoring the Platform 204
End-User Platform Restore 206
Supported and Unsupported Web Browsers 206
Installing the End-User Platform Restore Solution 206
Activating the End-User Platform Restore Feature 207
Configuring the End-User Platform Restore Settings 208
Using the End-User Platform Restore Feature 211
Appendix A: About Find Site Collection 213
Appendix B: About Advanced Search 214
Appendix C: Accessing Hot Key Mode 219
Backup Tab 220
Restore Tab 221
Time-Based Restore 223
Clone Tab 224
Plan Manager Tab 225
Appendix D: SharePoint 2010 Components Supported in Platform Backup and Restore 226
Supported Web Parts 226
Service Applications Supported for Restore 228
Components Supported for Restore 231
Appendix E: SharePoint 2013 Components Supported in Platform Backup and Restore 234
Supported Web Parts 234
Service Application Supported for Restore 235
Components Supported for Restore 238
Appendix F: SharePoint 2013 Social Features Supported in Platform Backup and Restore 240

Appendix G: SharePoint 2016 Components Supported in Platform Backup and Restore 241
Appendix H: SharePoint Object Security and Property 242
Appendix I: Advanced Settings in Configuration Files 243
AgentCommonWrapperConfig.config 243
Restoring Specified Web Properties 243
SP2010PlatformConfiguration.xml 243
Controlling Agents Backing Up in Parallel 243
Configuring Maximum Amount of Concurrent Threads on Agents 244
Configuring Connecting Media Settings 244
Configuring Maximum Number of Files and Folders to Be Backed up 244
Configuring Index Generation Option 244
Shrinking Transaction Log 245
PlatformRecoveryConfig.Config 245
Changing Incremental Backup Job to Full Backup Job 245
Appendix J: Customization Support Table 246
Notes for Appendix J 270
Workflow Definition and Instance 270
Backup and Restore FAST Search Server for SharePoint 2010 Farms 271
Notices and Copyright Information 275

What's New in this Guide

- Updated the Environment Configuration section to include the Windows Server 2016 as an operating system that Farm Rebuild supports.

About DocAve Platform Backup and Restore

Platform Backup and Restore protects your organization from disasters with a comprehensive toolset for backing up and restoring your entire SharePoint environment. Platform Backup and Restore 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. DocAve Platform Backup and Restore does not function on the SharePoint Online environment.

Complementary Products

Many products and product suites on the DocAve 6 platform work in conjunction with one another. The following products are recommended for use with Platform Backup and Restore:

- DocAve Granular Backup and Restore to back up all farm content and restore content down to the item level
- DocAve Replicator for SharePoint for copying SharePoint content within the same SharePoint farm or from one SharePoint farm to another
- DocAve Content Manager for SharePoint for restructuring or moving SharePoint content
- DocAve Report Center for SharePoint to examine pain points in the SharePoint infrastructure and report on SharePoint user behavior and changes
- DocAve Data Protection for setting backup and restore points prior to adjusting SharePoint governance policies in this product

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.

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 TSM Client 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.

Notable Environment Exceptions

The following are notable exceptions to the supported DocAve environments. The following represent environment level support information, not feature level support. Feature level support, specific to each feature, is described throughout this guide where applicable.

- Platform Backup and Restore only supports Microsoft Clustering Service (MSCS) for SQL Clustering due to a limitation of how SQL Server statements are returned via the API.
- Platform Backup and Restore only supports out-of-place restores of BLOB data to Net Share and IBM Storwize Family devices.

Configuration

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

Agents

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

- The SharePoint Central Administration server
- The Search Service Application server where you want to back up the Search Service Application components
- 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 objects: 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

***Note**: Platform Backup supports SQL clustering, but only MSCS is supported. Failover is not supported for a third party cluster, but there is a manual workaround. If cluster failover support is required, install the DocAve Agent on each SQL cluster node. If it is not required, the DocAve Agent only needs to be installed on the active nodes. When configuring the DocAve Agent, enter the name of local SQL server into text box of DocAve Agent Host.

- 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 job.
- Each node of Hyper-V Failover Cluster if you want to back up VMs in Hyper-V Failover Cluster.

***Note**: The use of system resources on a server increases when the installed Agent is performing actions. This may affect server performance. However, if the Agent installed on a server is not being used, the use of system resources is very low and, therefore, the effect on server performance is negligible.

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 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
    - Member of the **Administrator** local group
2. SharePoint Permissions: This permission must be manually configured prior to using DocAve 6 Platform Backup and Restore; 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; they are not automatically configured.
    - Database Role of **db_owner** for all the databases related with SharePoint, including SharePoint configuration database, Central Administration content database, all of the content databases, and service application databases
    - Server Role of **public** and **Security Admin** to SQL Server
    - Server Role of **dbcreator**, **Alter any database**, or **View any definition** to the SQL Server
    - Database permission of **View server state** to 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**, and this permission must be configured on **all SQL instances** inside the **AlwaysOn Availability Group**.)

***Note**: The Agent account configured on the Agents in the Agent group must have the **View Server State** permission to the SQL Server registered in the staging policy, if the **Enable InstaMount for Generating Granular Index** option is selected in the backup plan settings.

***Note**: The Agent account used to back up and restore the SQL Server Report Service must be a member of the local **Administrators** group on the SQL Report Server.

***Note:** To restore the SharePoint apps, make sure the Agent account is not the SharePoint System Account.

Agent Account Configured on Other SharePoint Web Front-End Servers (Except for SQL Server and FAST Search Server)

1. Local System Permissions
    - Member of the **Administrators** group
2. SharePoint Permissions
    - Member of the **Farm Administrators** group
3. SQL Permissions
    - Database Role of **db_owner** for the SharePoint configuration database

***Note**: In order to back up the SharePoint Help Search, the user who starts the **SharePoint Foundation Search V4** service must be added to the **Administrators** group on the corresponding machine.

***Note**: In SharePoint 2010, in order to back up the SharePoint Search Service Application, the user (logon user) who starts the **SharePoint Server Search 14** service must be added to the **Administrators** group on the corresponding machine. In SharePoint 2013 and SharePoint 2016, the user (logon user) who starts the **SharePoint Search Host Controller** service must be added to the **Administrators** group on the corresponding machine. To configure the equivalent permissions of local Administrator, refer to the following section:

- Full Control to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VSS\Diag*
- Full Control to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VSS\VssAccessControl* with **Value data** of **1**
- Member of following local groups: Distributed COM Users, Certificate Service DCOM Access, and WSS_WPG(default)
- Allow access, launch and activation to the logon user for COM security

***Note**: After you have added these permissions to the logon user, restart the services.

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** to SQL Server (this permission is only required for the Agent Account configured on the **Fast Search Administration** server)

Agent Account Configured on the Index Server

The Agent account configured on the server where index components reside must be a member of the local **Administrators** group.

Agent Account Configured on the SQL Server

1. Local System Permissions
    - Backup Operators
    - IIS WPG (for IIS 6.0) or IIS IUSRS (for IIS 7.0)
    - Performance Monitor Users
    - DocAve Users

- DocAve Agent service logon user
- **Full Control** to the directory of the database files in both of the source and the destination

  ***Note**: User who can enable the InstaMount must be a member of the local **Administrators** group.

2. SQL Server Permissions
   - Database role of **db_owner** for master database.
   - Database role of **db_owner** for all the databases included in the backup plan.
   - Server role of **dbcreator** and **processadmin** permission to SQL server.
   - Database permission of **Control server** to SQL Server.

     ***Note**: The user used to back up and restore the certificate encrypted by TDE must have the server role of **securityadmin**.

     The user who restores the SQL logins must have the server role of **securityadmin**.

     ***Note**: If the user who ran the platform granular restore job is different from the user who run the platform backup job, the user performing the platform granular restore must have the database role of **sysadmin** to SQL Server of the destination.

     The user who performed an out of place database level platform restore job must have the database role of **sysadmin** to SQL Server.

     The user who ran the platform in place restore with a staging policy using the SQL server of another farm must have the database role of **sysadmin** to SQL server used by the staging policy.

     ***Note**: To back up and restore the files in File Share directory, the Agent account must have **Read** and **Write** permissions to the File Share directory, and be a member of the local **Administrators** group on the File Share Server.

SQL Server Service Account Configured on the SQL Server

The SQL Server Service account configured on the SQL server must have **Read** and **Write** permissions to the **Temporary Buffer**, which is configured in **Control Panel** > **Agent Monitor** > **Configure**.

Agent Account Configured on Hyper-V hosted VM

1. Local System Permission:
   - Member of the local **Administrators** group
2. Hyper-V VM Permission:

- Full Control to the folders where the specific VMs are stored
- Full Control to all of the VMs virtual hard disks

Agent Account Configured on VMs hosted by ESX/ESXi or vCenter

Local System Permissions

- Member of the local **Administrators** group

Host Profile Account configured on ESX/ESXi or vCenter Host Server

The account entered in the host profile used to connect ESX/ESXi or vCenter host server must have the **Administrator** role to the ESX/ESXi or vCenter host server.

***Note:** If the user does not have the Administrator role to the ESX/ESXi or vCenter host server, ensure that this user is assigned by a role with at least the privileges in the following table enabled:

Privileges		
Datastore	Allocate space	
	Browse datastore	
	Low level file operations	
	Remove file	
Folder	Create folder	
Resource	Assign vApp to resource pool	
	Assign virtual machine to resource pool	
	Create resource pool	
vApp	Add virtual machine	
	Assign resource pool	
	Assign vApp	
	Create	
	vApp application configuration	
	vApp instance configuration	
Network	Assign network	
Virtual machine	Configuration	
	Interaction	Answer question
		Configure CD media
		Configure floppy media
		Device connection
		Power On
		Power Off
	Inventory	Create new
		Register
		Remove
		Unregister
	Snapshot management	Create snapshot
		Remove Snapshot
	Provisioning	Allow disk access

Privileges		
		Allow read-only disk access
		Allow virtual machine download
	Guest Operations	Guest Operation Modifications
		Guest Operation Program Execute
		Guest Operation Queries
Permission	Modify permissions	
	Modify role	
Alarms	Create Alarm	
	Disable alarm action	
Host	Inventory	Modify cluster
Datastore cluster	Configure a datastore cluster	
Global	DisableMethods	
	EnableMethods	
	License	

Local System Permissions

The following Local System Permissions are automatically configured during DocAve 6 installation. User is a member of the following local groups:

- **IIS WPG** (for IIS 6.0) or **IIS IUSRS** (for IIS 7.0)
- Performance Monitor Users
- **DocAve Users** (the group is created by DocAve automatically; it has the following permissions):
  - Full Control to the Registry of *HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6*
  - Full Control to the Registry of *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog*
  - Full Control to the Communication Certificate
  - Permission of Log on as a batch job (it can be found within **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **User Rights Assignment**)
  - Full Control Permission for DocAve Agent installation directory

Supported Operating System for Hyper-V Host Server

VM backup and restore supports the following English-language operating system editions for the Hyper-V host server:

- Windows Server 2008 R2
- Windows server 2012
- Windows Server 2012 R2
- Microsoft Hyper-V Server 2012 R2
- Windows Server 2016

***Note**: If the operating system of Hyper-V host server is **Windows Server 2016**, Platform Backup does not support backing up shared disk VHDS files when backing up VMs in Hyper-v Failover Cluster.

***Note:** If the operating system of your Hyper-V host server is **Windows Server 2008 R2** or **Windows server 2012**, in order to ensure that the VMs on this host server keep functioning properly during the backup process, the following must be in place:

- The **Backup (volume snapshot)** service is offered to these Hyper-V VMs.
- The operating system for these Hyper-V VMs supports VSS snapshot.
- The **Hyper-V Volume Shadow Copy Requestor** service in these VMs is running during the backup process.

Supported ESXi Host Server Versions

VM backup and restore supports the following ESXi host server versions:

- VMware ESXi 5.0
- VMware ESXi 5.5
- VMware ESXi 6.0

Supported vCenter Host Server Versions

VM backup and restore supports the following vCenter host server versions:

- VMware vCenter server 5.5
- VMware vCenter server 6.0

Supported Hardware in DocAve 6 Platform Backup and Restore

Windows Storage Server 2008 R2 Enterprise, Dell EqualLogic FS7500, HP 3PAR, and NetApp Data ONTAP are supported.

Health Analyzer

AvePoint recommends using Health Analyzer to check the prerequisites required to correctly use DocAve Platform Backup and Restore.

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

***Note:** You can ignore the **Agent Account Cannot be SharePoint System Account** rule if you are not going to back up and restore SharePoint apps.

For more information about Health Analyzer, refer to the DocAve 6 Installation Guide.

Getting Started

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

Launching Platform Backup and Restore

To launch Platform Backup and Restore and access its functionality, complete the following steps:

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 & Restore** to launch this module.

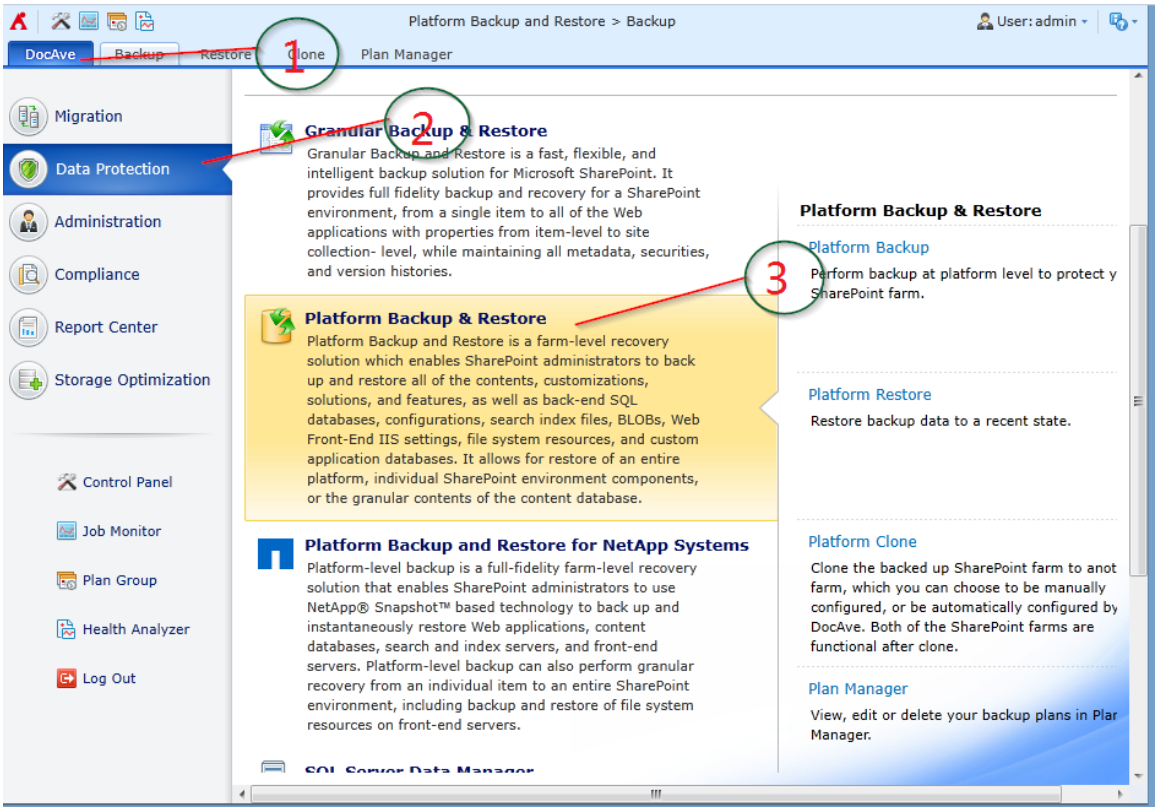


Figure 1: DocAve module launch window.

User Interface Overview

The Platform Backup and Restore 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 features.

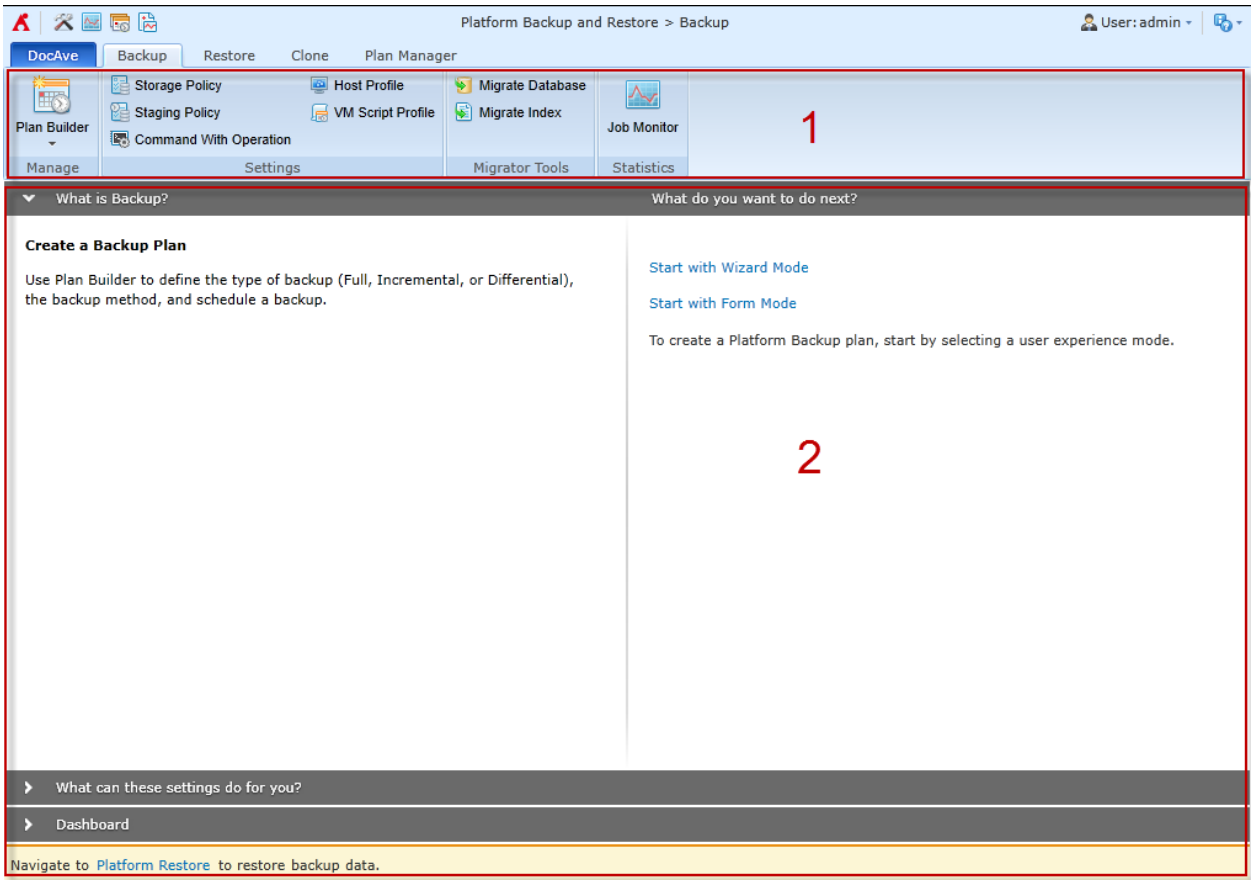


Figure 2: Platform Backup and Restore user interface.

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**: The Maintenance jobs will not be 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.

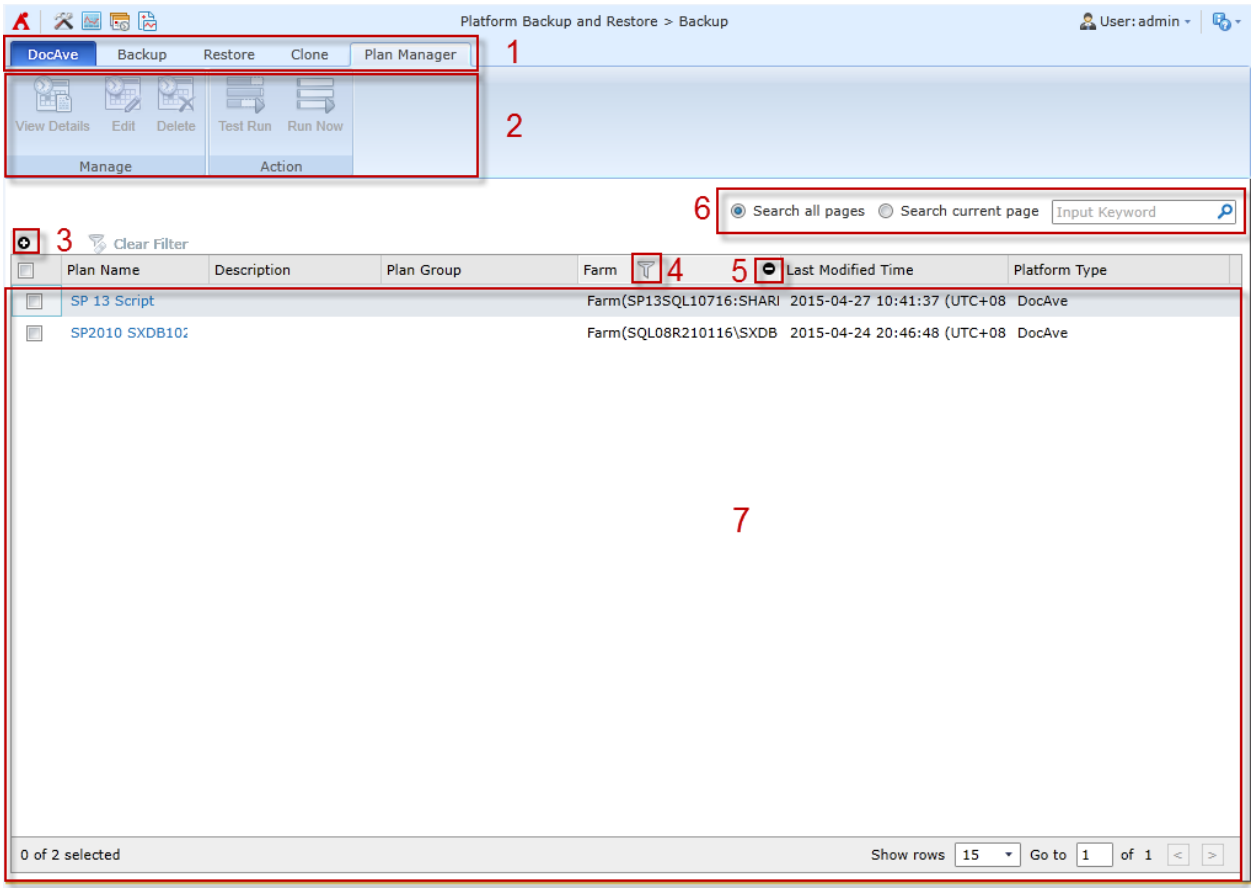


Figure 3: Navigating DocAve.

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, 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 storage devices 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.

Platform Backup and Restore can write to any of the following:

- Net Share
- FTP
- Amazon S3
- AT&T Synaptic
- Caringo Storage
- Dell DX Storage
- EMC Atmos
- EMC Centera
- HDS Hitachi Content Platform
- Rackspace Cloud File
- TSM
- IBM Storwize Family
- IBM Spectrum Scale Object
- Microsoft Azure Storage

For instructions on defining devices and setting up storage policies, refer to the DocAve 6 Control Panel Reference Guide.

***Note:** If the storage type of the physical devices is Net Share or IBM Storwize Family, for the best performance use the Concurrent storage device as the Data Storage Type of the logical device to store the backup data.

About the Staging Policy

The staging policy determines where to store the temporary databases generated during backup, maintenance, and restore. When you perform the Platform granular level restore that do not use InstaMount, the data is first restored to a temporary database in SQL. If there is insufficient space on the SQL Server you are restoring to, you can define a staging policy, thus the required temporary database will be stored on the SQL Server configured in the staging policy. When you perform the Platform granular level restore that uses InstaMount, the SQL Server entered in the staging policy is used to store the InstaMount temporary database.

Refer to the scenarios below for details regarding when to use the staging policy.

Scenario 1 – A Platform backup job with the **Generate granular index during the backup job** option enabled. The backup data index used in the granular restore is generated from the InstaMount temporary database.

- If a staging policy is selected in the backup plan, the InstaMount temporary database is created on the SQL Server that you entered in the staging policy.
- If the staging policy is not selected in the backup plan, the InstaMount temporary database is created on the SQL Server whose data is being backed up.

Scenario 2 – A Platform maintenance job with the **Generate granular index** or **Verify database backup data** option enabled and selecting a custom SQL server for InstaMount.

- If you select the **Remote SQL Server** option and select a staging policy, the InstaMount temporary database is created on the SQL Server that you entered in the staging policy.
- If you select the **SQL Server used for backup** option, the InstaMount temporary database is created on the SQL Server whose data is being backed up.

Scenario 3 – A Platform granular restore job that browses the index in InstaMount. In the **Data Selection** step for restoring the granular content, browse the backup data tree using the index generated by InstaMount.

- If the staging policy is selected when browsing the index in InstaMount, the InstaMount temporary database is created on the SQL Server that you specified in the staging policy.
- If the staging policy is not selected when browsing the index in InstaMount, the InstaMount temporary database is created on the original SQL Server whose data has been backed up by DocAve.

Scenario 4 – A Platform granular restore job with the **Use InstaMount** option enabled. The InstaMount temporary database is used to restore the granular content.

- If the staging policy is selected when running the restore job, the InstaMount temporary database is created on the SQL Server that you entered in the staging policy.

- If the staging policy is not selected when running the restore job, the InstaMount temporary database is created on the SQL Server you are restoring to.

In the following situations, the temporary database cannot be stored on the default SQL Server. To ensure the proper execution of Platform Backup and Restore jobs, a staging policy must be used when:

- The SQL Server of a farm you want to restore is corrupted.
- You do not have the appropriate permissions required for the SQL Server being restored to.
- There is not enough space on the SQL Server to store the temporary database.

Configuring a Staging Policy

To configure a staging policy:

1. Click **Staging Policy** in the **Settings** group on the **Backup** or **Restore** tab. The **Staging Policy Configuration** window appears.
2. Click **Create** from the **Manage** group. The **Staging Policy Configuration** page appears. Configure the following settings:
    a. **Staging Policy Name** – Enter a **Name** and optional **Description** for the staging policy.
    b. **SQL Agent Name and Instance Name** – Select a **SQL Agent name** (a DocAve Agent that is installed on the SQL Server database). Select the **SQL instance name** (where to save a temporary database).
        - **SQL Agent name** – All of the DocAve Agents that are installed on the SQL database servers are listed in the drop-down box.
        - **SQL instance name** – All instances of SQL Server databases that have a DocAve Agent installed are listed in the drop-down box.
    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 entered Managed Account. The account must be added to the **sysadmin** role in SQL Server.

          Click **Validation Test** to verify the access to the SQL Server.
    d. **Temporary Database Configuration** – Set up the configuration of the temporary database.
        - **Minimum amount of free space to leave** – Enter the minimum amount of space to leave for the database file location and log file location. DocAve ensures that

the entered amount exists in the corresponding location before starting a job. If the free space entered here does not exist in the location before a job starts, or if the entered amount will not exist after the temporary database is stored to the entered location, then the corresponding job will fail.

- **Temp database file location** – Enter a local path on the SQL Server to store the temporary database data file (.mdf). The format of the path is **C:\data**. The default location is the database data default location of SQL Server, for example: *C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data*.
- **Temp log file location** – Enter a local path on the SQL Server to store the temporary database log file (.ldf). The format of the path is **C:\data**. The default location is the database log default location of SQL Server, for example: *C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data*.

  ***Note**: For a clustered SQL Server instance, the temporary database file and log file location must be shared by all nodes of this cluster.

About Command With Operation

Before or after the backup snapshot creation and the Platform Restore job, you have the option to automatically run a command profile before the operation starts or after the operation completes. The Command With Operation feature can realize advanced features using predefined scripts. When configuring the Platform Backup plan or the Platform Restore wizard, you can select a command profile to realize more advanced features before or after the backup snapshot creation or before or after the restore job.

Configuring a Script Profile

Create and manage the script profiles to perform the advanced features before or after the backup snapshot creation or restore using predefined script.

To configure a script profile, complete the steps below:

1. In the **Command With Operation** interface, click the **Script Profile** button, and then click **Create** to create a script profile.
2. In the pop-up window, enter the profile name and an optional description to the **Script Profile Name** field.
3. **Operation Timing** – Select when to execute this script from the drop-down list.
    - **Before Creating Backup Snapshot**– The script will be executed before creating the backup snapshot.
    - **After Creating Backup Snapshot**– The script will be executed after the backup snapshot creation.
    - **Before Restoring Data** – The script will be executed in the Platform Restore job before starting the restore process.
    - **After Restoring Data** – The script will be executed in the Platform Restore job after the restore process is finished.
4. **Agent Selection** – Select an Agent from the drop-down list for where you want to run this script.

    ***Note**: The script you want to run must be predefined and stored in the selected Agent.

5. **Script File** – All of the script files (.bat, .ps1, .exe) stored in the *…\AvePoint\DocAve6\Agent\data\SP2010\Platform\Scripts* directory on the selected Agent will be loaded. Select a script profile from the drop-down list that you would like to execute.
6. **Provider** – This field is only available when you select the **Before Restoring Data** or **After Restoring Data** as the **Operation Timing**. Select a provider that you want to use to execute the script.
7. **Should DocAve wait for the script to complete?** – Select **Yes** to let DocAve wait while the script is running. Otherwise, select **No**. If you select **No**, the script will be executed at your selected operation timing. Platform Backup and Restore will update a message into the Backup or

Restore job report to indicate the script process status. If the status of the script in the job report is **Skipped**, which means the script execution is not completed, DocAve will not interfere the operation of the script until it finishes. If you select **Yes**, DocAve process and the script process will go after the operation timing you have selected to run. DocAve process will continue after the script is complete.

8. **Session Time Out** – If you have selected **Yes** to let DocAve wait while script is running, designate a session time-out value. The script process will be ended automatically if it is not finished in the configured period.
    - **No time limit** – The script will not be interrupted until it finishes.
    - **After _ Minutes/Hours** – The script will be stopped if the running time exceeds the configured time period.
9. Click **OK** to save the configured script profile. Click **Cancel** to return to the script profile managing interface.

Managing Script Profiles

For the created script profiles, you can manage them on the **Command With Operation** window. In the **Backup** or **Restore** tab, click **Command With Operation** in the **Settings** group. The Command With Operation window appears. All of the previously created **Command Profiles** are displayed in the main display pane. Click **Script Profile** on the ribbon to display all of the created script profiles.

In this interface, you can change the number of script profiles displayed per page. To change the number of the script profiles displayed per page, select the desired number from the **Show rows** drop-down menu in the lower right-hand corner. To sort the script profiles, click the column heading such as **Name**, **Description**, **Script File**, **Operation Timing**, and **Agent**.

Perform the following actions from the ribbon to manage the script profiles:

- **Create** – Click the **Create** button on the ribbon to create a script profile.
- **Edit** – Select a script profile and click **Edit** on the ribbon to change the configurations for the selected script profile. You can change the settings and then click **OK** to save the modification, or click **Cancel** to exit without saving any changes.
- **Delete** – Select the script profile 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 script profile, or click **Cancel** to return without deleting the selected script profile.

Configuring a Command Profile

Create and manage the command profiles to configure how to run the scripts included. To configure a command profile, complete the steps below:

1. In the **Command With Operation** interface, click the **Command Profile** button, and then click **Create** to create a command profile.
2. In the pop-up window, enter a profile name and an optional description to the **Command Profile Name** field.
3. **Processing Commands** – Choose the type you want to run the included scripts profiles. To execute the included scripts in sequential, select **Sequential**. To execute the included scripts in parallel, select **Parallel**.

   ***Note**: If you select **Sequential** as the way to run the scripts, you can define the order of the scripts being executed in the **List of Scripts to Run** table. Select the ordinal number of the corresponding script profile as desired from the drop-down list in the **Order** column.

4. **Add Script Profile** – Add the previously created script profiles that you want to use into the command profile. Select one or more script profiles in table on the left. Click **>>** to add it or them to the table on the right. Click **<<** to remove the selected script profiles from the table that are added to the command profile to execute.
5. To create a new script profile to add to the current command profile, click the **Create a new script profile** link. Configure the script profile settings, and then save the profile. For details, refer to Configuring a Script Profile.
6. Click **OK** to save the configuration to the command profile. Click **Cancel** to return to the command profile managing table.

Managing Command Profiles

For the created command profiles, you can manage them on the **Command With Operation** window. In the **Backup** or **Restore** tab, click **Command With Operation** in the **Settings** group. The **Command With Operation** window appears. All of the previously created command profiles are displayed in the main display pane. If you are already on the **Command With Operation** interface, click **Command Profile** on the ribbon to display all of the previously created command profiles. In this interface, you can change the number of command profiles displayed per page. To change the number of the command profiles displayed per page, select the desired number from the **Show rows** drop-down menu in the lower right-hand corner. To sort the command profiles, click the column heading such as **Name**, **Description**, and **Type**. Perform the following actions from the ribbon to manage the command profiles:

- **Create** – Click the **Create** button on the ribbon to create a command profile.
- **Edit** – Select a command profile and click **Edit** on the ribbon to change the configurations for the selected script profile. You can change the settings and then click **OK** to save the modification, or click **Cancel** to exit without saving any changes.
- **Delete** – Select the command profile 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 command profile, or click **Cancel** to return without deleting the selected command profile.

About VM Script Profile

You have options to configure the scripts to perform VM backup or VM restore using third-party tool. VM Script Profile feature allows you to run the user-defined scripts on the selected Agent to back up VM or restore VM, instead of using DocAve.

Configuring a VM Script Profile

Create or configure a VM script profile to perform the VM backup or VM restore using third-party tool with predefined scripts. The created VM script profile can be used in the Backup plan or Farm Rebuild wizard for the VM backup or VM restore.

To configure a VM Script Profile, complete the steps below:

1. In the **Backup** or **Restore** tab, click the **VM Script Profile** button, and then click **Create** to create a script profile.
2. In the pop-up window, enter the profile name and an optional description to the **Profile Name** field.
3. **Operation Timing** – Select when to execute this script from the drop-down list.
    - **VM Backup** – The script will be executed to back up VMs designated in the script file.
    - **VM Restore** – The script will be executed to restore the VMs designated in the script file during Farm Rebuild.
4. **Agent Selection** – Select an Agent from the drop-down list for where you want to run this script.

    ***Note**: The script you want to run must be predefined and stored in the selected Agent.
5. **Script Selection** – All of the script files (.bat, .ps1, .exe) stored in the *…\AvePoint\DocAve6\Agent\data\SP2010\Platform\Scripts* directory on the selected Agent will be loaded. Select a script profile from the drop-down list that you would like to execute. Click **Refresh** to reload the scripts under the directory of the selected Agent.
6. Click **Save** to save the configured VM Script Profile. Click **Cancel** to return to the VM Script Profile managing interface.

Managing VM Script Profiles

You can manage the created VM Script Profiles in the **VM Script Profile** window. In the **Backup** and **Restore** tab, click **VM Script Profile** on the ribbon. The **VM Script Profile** window appears.

In this interface, you can change the number of VM script profiles displayed per page. To change the number of the VM script profiles displayed per page, select the desired number from the **Show rows** drop-down menu in the lower right-hand corner. To sort the VM script profiles, click the column heading such as **Name**, **Description**, **Script File**, **Operation Timing**, and **Agent**.

Perform the following actions from the ribbon to manage the script profiles:

- **Create** – Click the **Create** button on the ribbon to create a VM script profile.
- **Edit** – Select a VM script profile and click **Edit** on the ribbon to change the configurations for the selected script profile. You can change the settings and then click **Save** to save the modification, or click **Cancel** to exit without saving any changes.
- **Delete** – Select the VM script profile that you want to delete and click **Delete** on the ribbon. If the profile is currently being used, a window will pop up and inform you that the profile cannot be deleted.

About Migrator Tools

Use DocAve Migrator tools to migrate the SQL Server database and index from the source storage location to the local storage system, as well as separate the database files and log files onto separate local path.

Migrate Database

The Migrate Database tool migrates the SharePoint databases to a local destination. Such databases include the SharePoint Configuration database, service application database, or Web application content database.

***Note**: Migrate Database tool does not support migrating the system database, databases in the AlwaysOn Availability Group, and the SQL Mirroring Databases.

***Note**: The database will be unavailable during the migration process.

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 following steps:

1. **Migrate Database** – Complete the following steps:
    a. Choose one Agent from the **Agent selection** drop-down list to migrate the databases on the selected Agent server.
    b. Click **Next**. The **Database Association** page appears.
2. **Database Association** – Complete the following steps:
    a. Select the checkbox next to the database or the database file that you want to migrate. The **To** field becomes enabled.
    b. Select a disk from the **To** drop-down list.
    c. Enter the destination path where to store the database files. The selected database will be migrated from the location displayed in **From** to the path entered in the **To** field.
    d. Click **Next**. The **Active Connection** page appears.
3. **Active Connection** – Complete the following steps:
    a. Click **Next**. A pop-up window appears to inform you that all of the active connections of the selected databases that will be cut off after you start the migrations. The databases will not be usable until the job is finished.
    b. Click **OK**. The **Notification** page appears.
4. **Notification** – Complete the following steps:

a. To inform users of the database migration job, 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.

b. Click **View** to view the detailed configuration of the selected notification profile.

5. Click **Start** to start the database migration job.

Migrate Index

The Migrate Index tool is used for migrating the SharePoint Foundation Help Search index and Search Service Application index to a local destination.

1. Click **Migrate Index** in the **Migrator Tools** group on the **Backup** tab. The **Migrate Index** page appears.
2. **Migrate Index** – Complete the following steps:
    a. In the **Farm Selection** field, select the farm that contains the SharePoint indexes you want to migrate. The SharePoint Foundation farm will not be loaded in the drop-down list, as the Migrate Index tool does not support migrating the index files of the SharePoint Foundation farm.
    b. In the **Agent Group** field, select an Agent group from the drop-down list to execute the index migration job for load balancing and performance improvements.
    c. Click **Next**. The **Index Association** page appears.
3. **Index Association** – Complete the following steps:
    a. Select the checkbox of the index you want to migrate. The **To** field is enabled.
    b. Select a disk from the **To** drop-down list. The selected index will be migrated from the location displayed in **From** to the path entered in the **To** field.
    c. Click **Next**. The **Notification** page appears.
4. **Notification** – To inform users of the index migration job, complete the following steps:
    a. 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.
    b. Click **View** to view the detailed configuration of the selected notification profile.
5. Click **Start** to start the index migration job.

Overview of Backup Types

DocAve Platform Backup and Restore uses Microsoft Volume Shadow Copy Services (VSS) snapshot technology to generate snapshots (VSS shadow copies) and then protects your SharePoint farm. When configuring a backup schedule or running a backup plan, you can select the type of backup to perform: **Full**, **Incremental**, or **Differential**.

***Note**: Platform Backup does not support backing up databases with names that contain leading spaces, trailing spaces, or non-printable characters due to a known issue of Microsoft Volume Shadow Copy Services (VSS). For more information, see Microsoft's Backing up a SQL Server database using a VSS backup application may fail for some databases article.

***Note**: The VMs hosted by ESX/ESXi or vCenter support the Full Backup, Incremental Backup, and Differential Backup, but the VMs hosted by Hyper-V only support Full Backup. If the backup type of the backup job is set to Incremental or Differential Backup, you can choose whether or not to perform a full backup on the Hyper-V hosted VM.

Full – Backs up all of the selected content, including transaction log files, each time a backup is performed. This option requires the most storage space because each backup file can be large, depending upon the size of your SharePoint environment. Unlike Incremental and Differential backups, all Full backups are independent of one another and are not dependent on other backup data files. Each of the backups is comprehensive, therefore, Full backup jobs take the longest to complete of the three available options.

Incremental – Backs up only the transaction log, drastically reducing the size of the backup file created. Note that an Incremental backup is the only backup option that truncates the transaction log. To trigger the truncating function, edit the **SP2010PlatformConfiguration.xml** configuration file. For more details, refer to Shrinking Transaction Log. This backup requires less storage than a Full or Differential backup. Incremental backups reduce execution time, thereby allowing for shorter backup windows. It is important to note, however, that in order to recover all of the most recent SharePoint data from an Incremental backup, the latest Full backup in the Full backup cycle must be available. If the Incremental backup is based on a former Incremental backup, the former must be available. Consider each Incremental backup file as a piece of the whole SharePoint environment. If one of these files is not available, the full SharePoint environment cannot be restored.

For example, if the following backups are performed in this order–Full Backup, Incremental Backup, Incremental Backup, Incremental Backup:

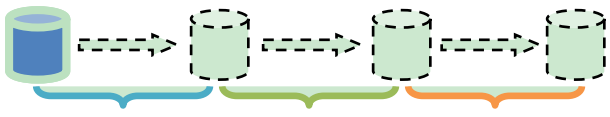


Figure 4: One Full backup followed by three Incremental backups.

1. The first Incremental Backup backs up the newly added data in blue period.
2. The second Incremental Backup backs up the newly added data in green period.
3. The third Incremental Backup backs up the newly added data in orange period.

***Note**: If an Incremental Backup job is failed, the later Incremental Backup jobs will be failed by default. You can also, if necessary, enable the Full Backup feature to replace the failed Incremental Backup by creating the **PlatformRecoveryConfig.config** file. For more information, refer to PlatformRecoveryConfig.Config.

Differential – Backs up all content that has been updated since the last Full backup. These backup files are larger in size than Incremental files, but smaller than Full backup files. In order to recover all of the most recent SharePoint content, the original Full backup file and latest Differential backup file are required.

For example, if the following backups are performed in this order – Full Backup, Differential Backup, Differential Backup, Differential Backup:

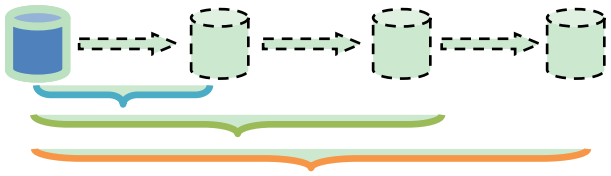


Figure 5: One Full backup followed by three Differential backups.

1. The first Differential Backup backs up the newly added data in blue period.
2. The second Differential Backup backs up the newly added data in green period.
3. The third Differential Backup backs up the newly added data in orange period.

SharePoint Components Supported for Backup

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

SharePoint 2016

DocAve Platform Backup and Restore supports backup of the SharePoint 2016 components. For more details, refer to Appendix G: SharePoint 2016 Components Supported in Platform Backup and Restore.

SharePoint 2013

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

- All SharePoint databases – The configuration database, 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 Member Agent using Platform Backup. VSS method does not support to back up data on the FAT 32 formatted disks and the backup of the content database in the cluster shared volume. VSS method supports the backup of the database whose database location is in UNC path whose format is *IP or servername**sharename**directory**filename* on the Windows Server 2012 (or later) using SMB 3.0 (or later), however, the database files in the UNC path whose format is *IP or servername**C$**directory**filename* are not supported for backup.

  ***Note**: To ensure data integrity, when you add more data files (.mdf/.ndf) and log files (.ldf) to a backed-up database, Platform Backup and Restore runs a full backup, regardless of whether an Incremental or Differential was selected or not.

  ***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 Index Member Agent.
- SharePoint components and settings – This includes Web applications, InfoPath Forms Services, State Service, SharePoint Apps and AppData, 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 configuration database, content database, and solutions.

- NewsGator 4.0 – This includes the Enrich Service, News Stream Service, Social Platform Service, and Video Steam Service (including corresponding databases), proxies, and solutions.

  ***Note**: Social Sites (NewsGator) 4.0 for SharePoint 2013 is supported from DocAve 6 SP4 and later. Social Sites (NewsGator) 5.0 for SharePoint 2013 is supported in DocAve 6 SP6 and later.

- SharePoint front-end resources – The front-end Member Agent backs up the IIS settings (both metadata and files), SharePoint site definitions, SharePoint hive files, Global Assembly Cache files, custom features, and extra file system folders.

***Note**: To back up and restore the Office 2013 Web Apps Server using DocAve Platform Backup and Restore, you must perform a Platform Backup job to back up the whole farm with VM by adding the VM of the Web Apps Server in the backup list.

SharePoint 2010

DocAve Platform Backup and Restore 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 are supported. These databases are backed up by the SQL Member Agent using Platform Backup. The VSS method does not support the backup of data on the FAT 32 formatted disks and backup of the content database in the cluster shared volume. The VSS method supports the backup of databases whose location is in UNC path formatted as follows: *IP or servername**sharename**directory**filename* on the Windows Server 2012 (or later) using SMB 3.0 (or later), however, the database files in the UNC path whose format is *IP or servername**C$**directory**filename* are not supported for backup.

  ***Note**: To ensure data integrity, when you add more data files (.mdf/.ndf) and log files (.ldf) to a backed-up database, Platform Backup and Restore runs a full backup, regardless of whether an Incremental or Differential was selected.

  ***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 Index Member 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, Application Registry Service, Shared Service Applications, Shared Service Proxies, Global Search Settings, and Managed Metadata Service.

***Note**: When you are backing up service applications, the platform incremental backup job will not back up the service applications using any database in the Simple recovery mode. DocAve recommends that you perform the full backup job on the service applications using database in Simple recovery mode, or make sure all of the databases used by the service application are in the Full recovery mode if you want to perform the incremental backup.

***Note**: To successfully back up the SQL Server Reporting Services for SQL Server 2008 R2, the Agents included in the Agent group for performing the backup job must be the servers where the SQL Server Reporting Services feature is configured or the servers that have the same SQL Server Reporting Services add-in version as the SQL Server Reporting Services feature installed on another server. .

- 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 configuration database, content database, and solutions.
- NewsGator 1.2 and 2.5 – 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 Service Pack 1 and later.

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

  ***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. Using Plan Builder to Back Up Data

Using Plan Builder to Back Up Data

Use the **Plan Builder** to schedule a backup and define the type of backup (Full, Incremental, or Differential).

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 an Agent group to browse the farm tree and execute the backup job.

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

   ***Note**: Platform Backup and Platform Restore support backing up and restoring the components of your SharePoint farm whose SharePoint servers and SQL servers are all on Azure VMs.

   ***Note**: If the selected farm contains a large number of components, browsing the farm tree may take a long time. Navigate to **Control Panel** > **System Options** > **Security Settings** to configure the **Session Timeout**. For more details, refer to DocAve 6 Control Panel Reference Guide.

3. In the **Backup Components Selection** field, choose the components scope for backup.

   ***Note:** Any time the scope of a plan is changed, refresh the tree before continuing to use the plan.

   - **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 the SharePoint configuration database, administration database, and Web front-end servers.

- **Back up the whole farm with VM** – All of the farm components will be automatically selected for backup in the farm tree of the **Data Selection** step, and as well you can add the desired VM into this plan for backup. In the farm tree of the **Data Selection** step, you can deselect the components that you do not want to include for backup, except the SharePoint configuration database and administration database.

  ***Note**: Platform Backup supports backing up the VMs hosted by ESX/ESXi, Hyper-V, Hyper-V Cluster and vCenter. For details, refer to Supported Operating System for Hyper-V Host Server, Supported ESXi Host Server Versions, and Supported vCenter Host Server Versions.

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

   To select the 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 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.

      Optionally, select the **Include New** node to include any recently created SharePoint objects (child nodes) in the Platform backup 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

      ***Note**: When backing up Social Sites (NewsGator) 5.0 in the farm, **Start** the Microsoft SharePoint Foundation Web Application in all servers where the Agents in the selected Agent Group are located.

   b. In the screenshot below, the following SharePoint objects will be backed up by the Platform backup 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 and/or newly created Web applications under the **Microsoft SharePoint Foundation Web Application** node
- The below example, the **Finance Web** and **HR Web** Web applications

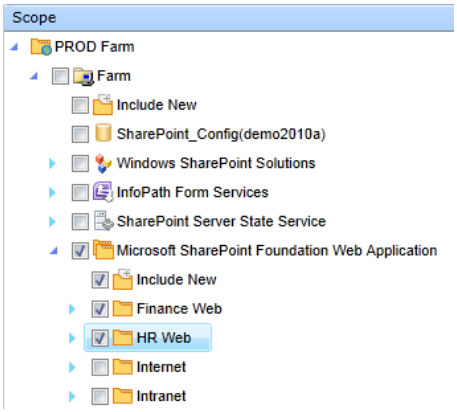


Figure 6: Selecting SharePoint farm content.

In addition, you can manually add any custom databases that are not listed to the SharePoint component tree. Such databases include solution databases, third-party software databases, etc. Once a custom database is added to the tree, it can be backed up as normal using a Full, Incremental, and Differential backup.

Complete the steps below to add custom database to the 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 installed are listed under the corresponding SQL instance node in the tree.

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

***Note**: The databases in **Restoring** status do not support being 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**. If you have selected the **Back up the whole farm with VM** option in the **Backup Component Selection** field, the **VM Backup Settings** step will appear. You are required to choose to use Platform Backup to back up VM or use third-party tool to back up VM. By default, the **Use Platform Backup to back up VM** option is selected.

Use Platform Backup to back up VM – This method requires to add the VMs you are about to back up into the **VM Backup List**, select host profiles and Agents for the VM to back up, and test the configured information.

***Note**: Does not support backing up and restoring VMs with the same name stored on the datastores that are in vCenter datastore cluster.

- **Add VMs** – Add the VMs in the server roles with DocAve Agent installed to this backup plan.

    i. Click **Add VMs** above the table in the **VM Backup List** field. The **Add VMs** window appears.

    All of the VMs available for this backup are listed in the **Add VMs** window. Select the checkboxes ahead of the server names, and then click **Add** on the ribbon to add the selected VMs to the backup list. The VMs in the following server roles with DocAve Agent installed can be displayed in the **Add VMs** window:

Server Role	SharePoint 2010	SharePoint 2013	SharePoint 2016
SharePoint Web Front-End Server	Supported	Supported	Supported
Application Server	Supported	Supported	Supported
Central Administration	Supported	Supported	Supported
Office Web Application Server	Supported	Supported	Supported
Related SQL Server (Installed alone)	Not Supported	Not Supported	Not Supported
FAST Search Server	Supported		
Project Server	Supported	Supported	Supported
Apps Server		Supported	Supported
Azure Workflow Server		Supported	Supported
Distributed Cache			Supported
Custom			Supported

***Note**: The VM in **Central Administration** role must be added to the backup list.

    ii. In the **VM Backup List** field, select a created host profile, or create a new host profile for the added VM. For details on configuring the host profile, refer to DocAve 6 Control Panel Reference Guide. Select an Agent to perform the backup for the corresponding VM. **Batch Settings** ( ) is supported.

***Note**: The VM hosted by Hyper-V will use the Agent designated in the selected host profile to execute the VM backup. The host profile is created to include VM host server information to allow DocAve to communicate with the host server for VM backup and restore.

***Note**: If the added VM is hosted by Hyper-V Cluster, the selected Agent must be on the node in the Hyper-V Cluster.

***Note**: If the added VM is hosted by ESX/ESXi or vCenter host server, AvePoint recommends you do not select the Agent on the VM that is in the backup list.

iii. Click **Test** to test the backup settings for backing up the corresponding VM, or click **Test All Selected** on the column header to test configurations for all of the selected VMs. If the server you added is not a VM, or the VM is not on the host server designated in the host profile, the test will fail. In addition, you can click **Remove VMs** to remove the selected VMs from the backup list.

***Note**: If the ESX/ESXi host server is managed by vCenter host, you must select a host profile for this vCenter host. The test will fail if the selected host profile is configured for ESX/ESXi host.

***Note**: If multiple VMs are using same parent disk, the parent disk will not be backed up again once the parent disk is successfully backed up while backing up one of the VMs.

- **Add Custom VMs** – Add custom VMs to this backup plan.

  ***Note**: DocAve does not support backing up the custom VM that has already been added to the backup list as a SharePoint server VM.

  i. **Host Profile** – Select a host profile. The VMs managed by the host selected in the host profile will be loaded as the backup scope.

  ***Note**: When backing up VMs on the Hyper-V host server that is in Failover Cluster, select Hyper-V Cluster type as the host profile.

  ***Note**: When backing up VMs on the Hyper-V host server and the snapshots are not successfully created, the backup job will fail.

  ***Note**: When backing up VMs on the Hyper-V host server, the VHD and VHDX files that are stored in the root path of a device will be not be successfully snapshotted. To successfully back up the selected VMs, please do not choose root path to store VHD and VHDX files.

  ii. **Agent Selection** – Select an Agent for connecting to the host server in the selected host profile and executing the backup job.

***Note**: If the VM host type of the selected host profile is Hyper-V, the Agent selected for this host profile will be retrieved automatically. The **Select an Agent** field will be disabled.

***Note**: If you select Hyper-V Cluster as the host profile for backing up VMs on the Hyper-V host server that is in Failover Cluster, the selected Agent must be in the cluster that is specified in the selected host profile.

iii. **VM Selection** – Select one or more VMs in the loaded tree. Expand the loaded VM tree and then select the VMs you want to back up. After expanding the tree, use the **Search** text box and then click the magnifying glass ( ) button to find specific VMs.

***Note:** When you hover the mouse over one of the VMs, the information about the VM operating system and memory will appear. For a Hyper-V VM that has a Windows operating system installed, the VM that is powered-on with setting **Integration Services** > **Data Exchange** selected will display the specific information of the operating system.

***Note**: Does not support backing up the VM configuration file and VM disk file, whose name contains # { }.

***Note**: When selecting VMs on the Hyper-V host server that is in the failover cluster to back up, the tree can only be expanded to Roles of Virtual Machine and Other type.

***Note**: If the VMs on the ESX/ESXi or vCenter host server have configured either the **Physical** or **Virtual** options of **SCSI Bus Sharing**, they cannot be snapshotted and backed up.

***Note**: After you added the VMs to the **VM Backup List**, whether or not you need to click **Test** depends on the following situations:

- If the VM is in Hyper-V Cluster, you must click **Test** to check if the selected Agent is in the cluster that is specified in the host profile.
- If the VM is not in Hyper-V Cluster, the **Test** is grayed out and you do not need to test.

Use third-party tool to back up VM – Selecting this method to perform the VM backup using the third-party tool via predefined scripts, instead of Platform Backup. Select a previously created VM script profile from the drop-down list to execute the VM backup, or create a new VM script profile by clicking the **New VM Script Profile** link from the drop-down list. For details on configuring VM script profile, refer to Configuring a VM Script Profile.

6. Click **Next**. The **Backup Options** page appears.

7. Select the backup option. Refer to Overview of Backup Types for supplemental information on backup types.
8. **Backup Options** – Choose whether or not to use Platform Backup and Restore as the only backup method.

    - **Use DocAve Platform Backup and Restore as the only backup method for SharePoint databases** – Select this option only when you are using DocAve Platform Backup and Restore as the only backup method for SharePoint databases. Selecting this option runs a Full, Incremental, or Differential backup upon initiating the job; this backs up both the database's data file and the log file.

      If you select this option, all of the DocAve Platform Backup options can be used, making the backup process more flexible and efficient. In order to record the backup time and trace the backup, this method will change the log sequence number (LSN) of the database during the backup.

    - **Use DocAve Platform Backup and Restore with other SQL backup methods for SharePoint databases** – Select this option if DocAve Platform Backup and Restore is being used with other SQL backup methods. Selecting this option only supports Full backups of databases. This will result in long backup times, rapidly growing backup data, and low system efficiency.

      This option is the equivalent of **Copy only Backups** in SQL Server. A copy-only backup is a SQL Server backup that is independent of the sequence of conventional SQL Server backups for a special purpose without affecting the overall backup and restore procedures for the database. With this option, Platform granular restore is still available, but only from each Full backup (as there are no Incremental or Differential backups for DocAve to reference).

      ***Note:** If you select Use DocAve Platform Backup and Restore with other SQL backup methods for SharePoint databases, only Full backup is supported.

9. **Log Backup** – Choose whether or not to perform a log backup in a full backup job. The default setting of this option is **No**. Selecting **Yes** for **Perform log backup after full backup** option will run an Incremental backup immediately after a Full backup. Incremental backups back up and truncate the log file. To prevent log files from growing too large in the database, it is recommended that you select this option. When backing up a very large database while users are still making modifications to data residing in the database, the Incremental backup ensures that the backup data is up to date.

    If you do not select this option, use the **Schedule** step to schedule Incremental backups. Note that failure to schedule Incremental backups will result in very large log files.

    ***Note**: AvePoint does not recommend using InstaMount with this option selected.

10. **Click Next**. The **Storage Policy** page appears.
11. 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. Refer to Configuring Devices and Setting up Storage Policies

for more information. 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**: If you have selected **Back up the whole farm with VM**, only the storage policies with logical device of **Concurrent storage device** are supported.

***Note**: Platform Backup and Restore does not support storage policies for **Cleversafe** physical devices.

12. Select any optional operations to perform on the backup data.
    a. Select an optional **Data Compression** setting. Select the **Compression** checkbox to enable data compression, and then choose a compression level using the slider. A low compression level results in a faster compression rate, but a larger data set; while, a high compression level results in a slower compression rate, but a smaller data set. Note that high compression level may take longer backup and restore time than a low compression level. Select whether to leverage DocAve Media Server (**Media Service**) resources or SharePoint Server (**SharePoint Agent**) resources for compression.
    b. Select the **Encryption** checkbox (optional) to enable data encryption. Encryption protects sensitive materials; however, encrypting data causes slower backup and recovery. Select whether to leverage DocAve Media Server (**Media Service**) resources or SharePoint Server (**SharePoint Agent**) resources for encryption. Then select a security profile for use in the encryption from the **Security profile** drop-down list, or click the **New Security Profile** link to create a new security profile. For more information on the security profile, refer to the DocAve 6 Control Panel Reference Guide.

    ***Note**: If the storage policy you selected for this backup plan is using logical device of **Concurrent storage device** type, the **Compression** and **Encryption** are not supported to configure and the two fields are hid

    ***Note**: If both **Compression** and **Encryption** are enabled, the two operations can only be performed together by selecting the same resources (the DocAve Media Server [**Media Service**] or SharePoint Server [**SharePoint Agent**]) for both.

13. Click **Next**. The **Backup Method** page appears.
14. Choose whether or not to **Create Persistent Snapshots** of the selected objects. Snapshots contain the content database's files and transaction log that will be backed up. By default, the selected option is **No**, and the snapshots will be deleted after copying backup data from snapshot to corresponding storage policy. Selecting **Yes** will create persistent snapshots to retain the snapshot after the backup job is completed. DocAve saves a snapshot on the hardware when each full backup or differential backup is initiated.

    It is recommended that you use persistent snapshots when you have a hardware provider on your SQL server. If the **Create Persistent Snapshot** is enabled and your SQL server is clustered, only the hardware provider will create persistent snapshots.

After you select **Yes**, the following options appear and must be configured.

a. Configure the **Snapshot Retention Policy** to delete previous snapshots. Enter in the textbox the maximum number of snapshots the current plan can take. By default, the number is **32**. It is not recommended that this value be larger than **64**.

b. Click **Advanced Settings** to further customize the threshold policy. Define which policy DocAve will apply when the amount of snapshots per volume in the storage location exceeds the entered value. For more information, refer to Snapshot Retention Policy.

If you enabled the **Create Persistent Snapshot** feature with a hardware provider installed, you can choose when to transfer backup data from snapshot to media server in **Maintenance** step. For more information, refer to Maintenance Options.

15. You can also configure when to transfer backup data from snapshot to backup data storage in **Run Now** interface. For more details, refer to Configuring Run Now Interface. Click **Next**. The **Advanced** page appears.

16. **ODX Compatibility Mode** – If your environment is configured with ODX (Offloaded Data Transfer), it is recommended to use this setting to speed up copy and move operations. To use this setting, select **Yes**; otherwise, select **No**. For more details on ODX Compatibility Mode, refer to http://msdn.microsoft.com/en-us/library/windows/hardware/hh833784.aspx.

    ***Note**: If you have selected the **Back up the whole farm with VM** option for this backup plan, the **ODX Compatibility Mode** feature will be unavailable for use.

    ***Note:** If you selected **Yes**, you can perform a test run job for the backup plan to check whether or not your environment can support ODX Compatibility Mode. Refer to Managing Plans for details on Test Run.

    ***Note**: ODX Compatibility Mode supports Web front-end data, BLOB data, and FAST Search data, but does not support the data in the database snapshot. For details on the limitations, refer to Microsoft's "Offloaded Data Transfers" article.

    ***Note**: This setting only works with specific storage devices and operating systems that are related to ODX. For more information, refer to Windows Offloaded Data Transfers Overview.

17. Choose whether or not to **Enable InstaMount for Generating Granular Index**. InstaMount makes item-level restore more efficient, because using a mapping file to record the relationship between the InstaMount temporary database and backup data. Note that the use of InstaMount requires minimal disk space. Refer to About InstaMount for more information.

    ***Note**: InstaMount can be used with the following storage types: Net Share, IBM Storwize Family, IBM Spectrum Scale Object, TSM, DELL DX Storage, or HDS Hitachi Content Platform.

    If you select **Yes**, you can choose a **Staging Policy** for storing the InstaMount temporary database. If you do not configure a staging policy, the SQL instance where the backed-up data

resides will be used for InstaMount. For more information on staging policies, refer to Configuring a Staging Policy.

18. **Options for Broken Log Chain** – Choose whether or not to perform a full backup on the database or fail the incremental or differential backup you are going to run, when the database log chain is broken by a third-party application.

    ***Note**: You can only configure the **Options for Broken Log Backup** field when you select the Use DocAve Platform Backup and Restore as the only backup method for SharePoint database option.

    - **Perform a full backup on the database** – If the database log chain is broken, perform a full backup on the database.
    - **Fail the backup on the database** – If the database log chain is broken, let the incremental or differential backup fail on the database.

19. **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 group, refer to the DocAve 6 Control Panel Reference Guide.
20. To inform users of the Platform Backup job, configure the **Notification** settings. Select a previously configured notification profile from the **Select a profile with address only** 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.
21. Click **Next**. The **Schedule** page appears.
22. Define the **Schedule type** selection:
    - **No schedule** – Select this option to run the backup job 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. In the **Backup Options** section, select a backup type from the drop-down list. For more information, see Overview of Backup Types and Backup Schedule.
        - **Full Backup** – A full backup of the selected objects and log files.
        - **Incremental Backup** – A fractional backup; backs up and truncates only the transaction log. This is the only backup that truncates the transaction log.
        - **Differential Backup** – A fractional backup; backs up only the data that has been added since the last Full backup.

    After configuring the schedule for the Platform Backup, 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 the delete (**X**) button to delete a schedule.

***Note**: Frequent consecutive Differential backups have a tendency to repeatedly back up the same data, which fills disk space quickly. For best results when conducting high frequency backups, it is recommended to use Incremental backups. Incremental backups save time and storage space by backing up only the differences between this Incremental backup and the last backup, instead of backing up all of the selected objects in their entirety.

23. Click **Next**. The **Maintenance** page appears.

    ***Note**: The maintenance job details will be added to the job details of the corresponding backup job, displayed in the **Maintenance Details** tab.

24. Configure the following maintenance settings:

    a. **Maintenance Options** – Choose the operations performed on the persistent snapshots and backup data during the maintenance.

        - **Transfer snapshot data to media server for last … backup(s)** – The snapshot data of the entered number of latest backups is sent to the storage policy selected in the Storage Policy step.

          ***Note**: This option only appears when you choose to create persistent snapshots.

        - **Generate granular restore index for last … backup(s)** – Generates the granular restore index for the entered number of latest backups in the selected Storage Policy. The index is used in Platform granular restore.
        - **Verify database backup data for last …backups** – Validates the database backup data for the entered number of latest backups in the selected Storage Policy.

    ***Note**: If you select **Generate granular restore index for last … backup(s)** or **Verify database backup data for last …backups**, you must configure the **Staging SQL Server** for running the maintenance jobs.

    b. **Staging SQL Server** – Choose the SQL server instance used to perform the database backup verification or generate the granular restore index. By default, the **SQL server used for backup** is selected. You can choose to use a **Remote SQL server** by selecting a staging policy from the drop-down list, or click New Staging Policy to create a new one. For Details of New Staging Policy, refer to Configuring a Staging Policy. Using a remote server can reduce the performance impact on the production.

    ***Note**: If you select a **Maintenance Option**, you must configure a schedule for running the maintenance jobs.

    c. **Maintenance Schedule** – Define the **Schedule type selection** for the scheduled maintenance jobs. Note that you can only perform a maintenance job on **Finished** and **Finished with Exception** backup jobs. These backup jobs must either defer copying data

from persistent snapshot, defer generating InstaMount mapping, or defer generating a granular restore index. A maintenance job performs deferred operations.

- **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 set up 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**. Only one schedule can be added and displayed in the **Summary** table. Click the delete (**X**) button to delete a schedule.

d. **Maintenance Notification** – To inform users of a maintenance job, configure a notification. Select a previously configured notification profile from the **Select a profile with address only** 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.

***Note**: You can also perform maintenance jobs manually in Job Monitor. For more information, refer to Manual Maintenance.

25. When finished, click **Next**. The **Overview** screen appears.
26. 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.
27. Check the **Save current plan as plan template** checkbox to save the current plan as a template. Enter the template name in the textbox. The plan template will be saved as this plan is saved. Next time, you can select this plan template to create a new plan.
28. 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
    - 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.
    - Click **Finish and Test Run** to save the configuration and then perform a test run job, based on the plan, immediately. The backup plan is now listed in **Plan Manager**.

Backup Schedule

Configure the following settings to build a new backup schedule. Users can configure the schedule settings in both **Basic** and **Advanced** tabs.

1. Configure the basic settings in the **Basic** tab. In the **Backup Type** field, choose a backup type for the scheduled backup job. Refer to Overview of Backup Types for additional information.

   ***Note**: DocAve performs a **Full** backup when running any Platform backup plan for the first time, regardless of the backup plan chosen. An initial Full backup is mandatory for all plans.

***Note**: The VMs hosted by ESX/ESXi or vCenter support the Full Backup, Incremental Backup, and Differential Backup, but the VMs hosted by Hyper-V only support Full Backup. If the backup type of the backup job is set to Incremental or Differential Backup, you can choose whether or not to perform a full backup on the Hyper-V hosted VM or skip backing up the Hyper-V VMs in the **Back up Hyper-V VMs** field.

2. **Restore Granularity Level** – Select a granularity level from the drop-down list. The generated granular index will be used for recovery to browse the backup data tree and search for the granular contents using Advanced Search feature. You can select **Site Collection Level**, **Site Level**, **Folder Level**, **Item Level**, **Item Version Level**, and **None**.
3. **Verify Database Backup Data** – Choose whether or not to verify the database backup data after a backup job has finished to ensure that the backup data can be used for recovery.
4. **Check Agent Account Permission for Backup** – Choose whether or not to check the Agent Account permissions for backup in the Platform Backup job. 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, 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.
5. **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.
6. **Type –** Select the recurring schedule to use. You can select the radio button of **By hour**, **By day**, **By week**, or **By month**.
7. **Schedule Settings** – Set up the frequency for the scheduled backup job. If you select the **Type** as **By hour**, **By week**, or **By month**, enter an integer greater than zero to set up a recurring frequency. To use the advanced settings to configure the job frequency, select the **Advanced** checkbox to show 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, and then 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 add more than one start time.
    - Advanced settings for **By week** – Enter an integer greater than zero into the text box of **Run every: _ week(s)** and then select the days of the week from the **on:** _drop-down list. For example, Run every **2** weeks on: **Tuesday and Thursday**, which means the backup job will run on Tuesday and Thursday every two weeks.
    - Advanced settings for **By month**

- **On day _ of _** – Run the backup job on the month and date you selected. For example, On day **1** of **February**, **March**, and **April**, which means the backup job will run on the 1th February, 1th March, and 1th April.
- **Day: _ of every _ month(s)** – Run the backup job on the selected date every the number of weeks you entered. For example, **Day: 1 of every 2 months**, which means the backup job will run on the 1th of this month, and on the 1th of the month after next month, and on the 1th of the month after next three months, until the configured end time.
- **The: _ _ of every _ month(s)** – Run the backup job on the numbered date of week every the number of months you entered. For example, **The: Second Monday of every 2 months**, which means the backup job will run on the second Monday of every 2 months.
- **The: _ _ of _** – Run the backup job on the numbered date of the week in the entered month. For example, **The: Second Monday of February, March, and April**, which means the backup job will run on the second Monday in February, second Monday in March, and second Monday in April.

8. **Range of Recurrence** – Select the start time and end time for the schedule.
9. Select the **Advanced** tab to configure the advanced settings of the backup schedule.
10. **Granular Index Options** – Choose when to generate the granular index. The index allows you to search the content database during recovery. Selecting **Generate granular index during the backup job** can be resource intensive. To avoid resource conflicts, select **Generate granular index during a maintenance job**.
11. **Back up Web Front-End Servers in Parallel** – Choose whether or not to back up the Web front-end servers in parallel. Selecting the **Back up Web Front-End servers in parallel** option requires you to enter in the text box the number of Web front-end servers that you want to back up in parallel.

    ***Note**: Backing up too many Web front-end servers in parallel can overload the Media Service.

    ***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**.

12. **Granular Index Method** – Choose how to generate the granular index for the backup data. 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**, Platform Backup will by default generate (at most) five database indices at the same time on a SQL Server.

13. **Run Command With Operation** – Select a command profile from the drop-down list to execute before or after the snapshot creation in the backup job. If you do not select the **Create Persistent Snapshots** option, this field will not be available to configure.

14. **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 the granular level restore to restore the stubs from the backed up stub database.

    Back up BLOB for Selected Scope – Choose whether to back up the BLOB content generated by Storage Manager and the files in the connected path of Connector. Select the corresponding checkboxes if you wish to back up the BLOB data: the BLOB data will be backed up in parallel. The Connector BLOB will be backed before the Storage Manager BLOB. By default, at most five Connector BLOBs or Storage Manager BLOBs will be backed up at the same time. You can navigate to the *…\AvePoint\DocAve6\Agent\data\SP2010\Platform\SP2010PlatformConfiguration.xml* directory to configure the maximum amount of BLOB data to back up in parallel. For more information, refer to Defining the Maximum Number of BLOB Backups Running in Parallel.

    ***Note:** The default value is set to **5**, which means there will be at most five BLOB backups running in parallel.

    ***Note**: The BLOB data in NFS storage cannot be backed up or restored using Platform Backup and Restore.

    ***Note**: Platform Backup and Restore supports the Storage Manager BLOBs that are stored on the **Cleversafe** devices.

    ***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 Archiver, select **Back up Storage Manager BLOB** option. In the same way, if you have BLOB data generated through Archiver in the backup scope, selecting **Back up Storage Manager BLOB** option will also back up the Archiver BLOB data together with the Storage Manager BLOB data during the backup job.

    ***Note**: If you want to back up BLOB data from the file share using VSS, the File Server VSS Agent Service must be enabled on the file server.

    ***Note**: Cannot back up the Storage Manager BLOB data stored in synchronous storage groups when:

    - The computer where the devices reside is powered-off, or
    - The computer where the devices reside is offline.

15. **BLOB Data Compression** – If you choose either or both of **Back up Storage Manager BLOB** and **Back up Connector BLOB**, this field will appear. Selecting the checkbox enables BLOB data compression when performing a backup job for this plan.

***Note**: This option supports Net Share and IBM Storwize Family devices; the data that is compressed or encrypted in Storage Optimization will not be compressed again.

16. **Job Time Limit** – Choose a time limit for this backup job.
    - **No time limit** – There is no time limit imposed on any backup job.
    - **Stop after _** (**Minutes**, **Hours** or **Days**) – DocAve will automatically stop this backup job if its running time exceeds the entered time limit.
17. Click **OK** to save the configurations as a schedule, or click **Cancel** to exit the current page without saving any changes.

Manual Maintenance

A maintenance job performs any operations deferred during backup jobs; including: transferring snapshot data to media sever, generating granular index, or verifying database backup data. You can only perform a maintenance job on **Finished** and **Finished with Exception** backup jobs.

In addition to a scheduled maintenance job (which can be configured in the backup plan), you can perform a maintenance job manually, in **Job Monitor**, on jobs that have already finished or finished with exception.

To inform 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 with address only** 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 more information, refer to the DocAve 6 Job Monitor Reference Guide. The maintenance job details will be added to the job details of the corresponding backup job, displayed in the **Maintenance Details** tab.

***Note**: You can only perform a maintenance job on **Finished** and **Finished with Exception** backup jobs. These backup jobs must defer copying data from persistent snapshot, defer generating InstaMount mapping, or defer generating a granular restore index. A maintenance job performs deferred operations. When a maintenance job is complete, the corresponding maintenance options/buttons will be greyed out. The Generate InstaMount mapping feature and the Generate index mapping feature only function on the content database, and the Generate InstaMount mapping feature does not support the incremental backup job.

***Note**: If you backed up the content database with file stream data using persistent snapshot, the maintenance job for generating index may fail.

Snapshot Retention Policy

If you apply a retention policy to snapshots, both the **MaxSnapshotCount** rule in the configuration file and the snapshot threshold rule configured in the Plan Builder are checked after the backup job is finished. For information on configuring snapshot retention rules, refer to the information in this section as well as the Setting up Snapshot Retention Rules in the Configuration File section.

***Note**: The snapshots of the failed and stopped jobs will be deleted right away. Only the finished backup job can apply the retention policy.

***Note**: DocAve counts snapshots taken by third party software towards the number of current snapshots stored on the hardware. However, snapshots taken by third party software or other plans cannot be deleted when executing retention policies.

***Note**: If you do not choose **Transfer data from snapshot to Media server** option when running the backup job, the corresponding snapshot will be deleted during snapshot retention with **Policy 1** enabled in Plan Builder.

During a backup job, DocAve checks the configured retention rules twice. The following information describes the retention rule logic in detail.

1. The first check occurs before the backup of the desired data. DocAve compares the current snapshot number on the hardware with the configured maximum number of snapshots you want to keep on the hardware, which is the **MaxSnapshotCount** in the configuration file.

   After the first check, DocAve then executes snapshot retention according to the **Snapshot threshold policy** configured in DocAve Platform Backup and Restore Plan Builder. There are three policy options:

   - **Policy 1: Schedule the data transfer for the oldest job snapshot, after data transfer then delete snapshot and start new job** – The oldest snapshot from the current plan's data is transferred to the configured logical device immediately and the snapshot is deleted from the hardware. A new job for the current plan then starts.
   - **Policy 2: Fail the new job, do nothing to the oldest snapshot and job** – The current plan's new job fails, and all of the snapshots that have been saved on the hardware are kept.
   - **Policy 3: Directly fail the oldest job corresponding to the snapshot, delete the snapshot without data transfer and start new job** – At first, the current job's oldest snapshots that have been transferred are deleted directly from the hardware; next, the snapshots of the differential backup jobs followed by a full backup job or differential backup job are deleted, the snapshots of the oldest differential backup jobs are deleted, and all jobs related to the deleted snapshot will fail. A new job for the current plan then starts.

     ***Note**: The snapshots of the full backup jobs whose snapshot data has not been transferred will not be deleted.

***Notes**:

- If the current snapshot number on the hardware is greater than or equal to (≥) the **MaxSnapshotCount** configured in the configuration file, DocAve executes the policy you selected in Platform Backup and Restore Plan Builder.
- DocAve will simulate the execution of the retention job to determine if enough space for the new snapshot will exist after the retention. If there is not, the exceeded snapshots are not deleted and the new backup job fails.
    - If you select **Policy 1** or **Policy 3**, DocAve deletes the current plan's oldest exceeding snapshots to ensure that there is space for the new backup data, and then runs the backup job.
    - If you select **Policy 2**, the backup job fails.
- If the current snapshot number on the hardware is smaller than (<) the **MaxSnapshotCount** value in the configuration file, DocAve runs the new backup job directly.

2. The second check occurs after backup of the desired data.

   DocAve compares the number of backup jobs that the current plan has taken with **The number of backup jobs you want to retain snapshots for is …** value configured in Plan Builder.

   After the check, DocAve then executes snapshot retention according to the **Snapshot threshold policy** below.

   - **Policy: Schedule the data transfer for the oldest job snapshot, after data transfer then delete snapshot** – The current plan's oldest snapshot is transferred to the logical device immediately and the snapshot is deleted from the hardware.

   ***Notes**:

   - If the number of backup jobs that the current plan has taken is greater than (>) **The number of the backup jobs you want to retain snapshots for is …** value configured in Plan Builder, DocAve copies the current plan's oldest snapshots to the logical device, and then deletes it (them) from the hardware.

     ***Note**: DocAve determines the snapshots that the current plan has taken still exceeds the threshold (**The number of the backup jobs you want to retain snapshots for is …** value in the Plan Builder) after the retention; if it does, the exceeded snapshots are not deleted. However, the new backup job completes since the new snapshot has been taken.

   - If the number of backup jobs that the current plan has taken is smaller than or equal to (≤) **The number of the backup jobs you want to retain snapshots for is …** value in Plan Builder, DocAve completes the new backup job.

Setting up Snapshot Retention Rules in the Configuration File

Use the **SP2010PlatformConfiguration.xml** file to configure the maximum number of snapshots that can be saved on the hardware. The file is located in the DocAve Agent installation path, which is *…\AvePoint\DocAve6\Agent\data\SP2010\Platform* by default.

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

You must modify the value of the following attributes in the configuration file that resides on the Agent server connected to the hardware; otherwise, the customized configuration will not take effect and the default configuration will be used.

Add multiple nodes in the red box in the following format:

```
<HardWareProviderConfig MaxSnapshotCount="64" AlwaysSendPartialData="false">
        <!--  providerOption 0-vss default, 1-Force system provider,2-set a prefer vss provider. default to 0
  MaxSnapshotCount max snapshot can be done on the volume for the provider
          Example, NetApp H/W luns configuration
        <VolumeConfig providerOption="2" providerId="ddd3d232-a96f-4ac5-8f7b-250fd91fd102" MaxSnapshotCount="255" >
                <DriverLetter path="N:"/>
                <DriverLetter path="N:/MointPointForNetApp/"/>
        </VolumeConfig>
-->
        <VolumeConfig providerOption="0" MaxSnapshotCount="32">
                <DriverLetter path="c:"/>
        </VolumeConfig>
</HardWareProviderConfig>
```

Figure 7: Modified configuration file.

```
<VolumeConfig providerOption="0" MaxSnapshotCount="32">
       <DriverLetter path="c:"/>
</VolumeConfig>
```

To configure the attributes in the red box above, refer to the information below.

- **providerOption** – Enter the provider to use for taking snapshots.
  - **0** – Use the default provider of the hardware. For system disks, the system VSS provider is used, while for other hardware disks, the hardware provider is used.
  - **1** – Use the system VSS provider.
  - **2** – Use the entered provider. The provider ID in **providerId** attribute must be entered if this option is used.

  To view the provider IDs, run the Command Prompt using **Run as administrator** option and enter the commands in Figure 8.

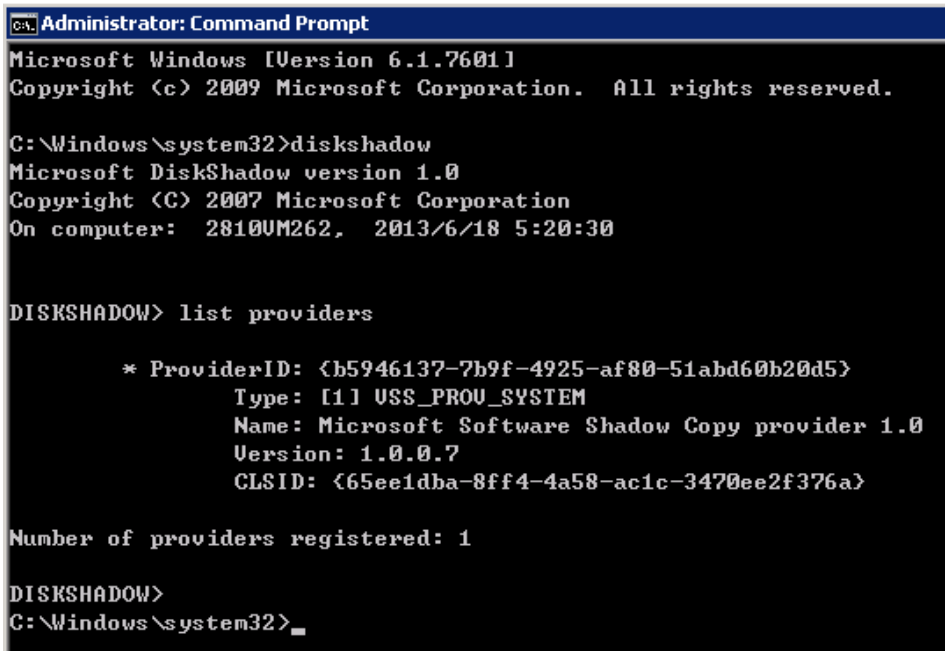


Figure 8: Viewing the provider IDs.

- **MaxSnapshotCount** – The maximum number of snapshots that can be saved on the hardware. For the Microsoft Windows system disk, it is not recommended that the value of this attribute be larger than 32 to ensure acceptable performance of the operating system.
- **path** – The name of the drive that links to the hardware.

Transportable Snapshot Configuration

DocAve supports using transportable snapshots to enhance the backup job performance and efficiency.

Environment Requirement:

- Install the Hardware Provider on the servers where the data to back up reside.
- Establish the same iSCSI session for the servers above with the storage server.

Configuring Configuration File

To enable the transportable snapshot feature, complete the following steps to configure the configuration file:

1. Navigate to *…\AvePoint\data\SP2010\Platform*. Find the **SP2010PlatformConfiguration.xml** file.
2. Open the **SP2010PlatformConfiguration.xml** file with Notepad. Find the <**BackupConfig**> element.
3. Modify the **<DataTransferOptionConfig TransferOption>** attribute. There are two meaningful values:
    - **0** – Disable the transportable snapshot feature.
    - **1** – Enable the transportable snapshot feature.
4. Save the configuration and then close this file.

If all of the environment requirements are met, the transportable snapshot feature will function when performing the Platform Backup jobs with VSS.

Modifying BLOB Backup Settings in Configuration File

Refer to the sections below to modify the BLOB backup settings in the configuration file if necessary.

Defining the Maximum Number of BLOB Backups Running in Parallel

If you selected the **Back up Storage Manager BLOB** option and **Back up Connector BLOB** option in the backup plan schedule or the **Run Now** interface, BLOB data will be backed up in parallel during the Platform Backup job.

The Platform Backup job will back up Connector BLOB data before backing up Storage Manager BLOB data (assuming the data is on the same server). At most, five Connector libraries' BLOB data can be backed up in parallel. After Connector BLOB data backup on a server completes, the Storage Manager site collections' BLOB data is backed up. At most, five Storage Manager site collections' BLOB data can be backed up in parallel.

***Note:** The default value is set to **5**, which means there will be at most five BLOB backups running in parallel.

To configure the maximum number of BLOB backups running in parallel, complete the steps below:

1. Log into the SQL server where a DocAve Agent is installed.
2. Find the **SP2010PlatformConfiguration.xml** file in the directory of *…\AvePoint\DocAve6\data\SP2010\Platform*.
3. Open the file with Notepad.
4. Find the **ParallelConfig BackupLimit** attribute.
5. Change the value as desired.
6. Save the configurations to the file and then close it.

Defining Where the BLOB Data will be Backed up

By default, the Storage Manager BLOB data can be backed up only on the SharePoint Agent server, and the Connector BLOB data is backed up on the server where the Media Service is installed.

You can modify the **SP2010PlatformConfiguration.xml** file to back up the Connector BLOB data on the SharePoint Agent server if necessary. For more information on modifying the configuration file, refer to the steps below:

1. Log into the SQL server where a DocAve Agent is installed.
2. Find the **SP2010PlatformConfiguration.xml** file in the directory of *…\AvePoint\DocAve6\data\SP2010\Platform*.
3. Open the file with Notepad.
4. Configure the **<BlobService useControlServiceExtender="true" useControlServiceConnector="false"/>** node by referring to the information below:

- The **useControlServiceExtender** attribute indicates that the Storage Manager BLOB data on the SharePoint Agent server is backed up. The value is **true** and cannot be changed.
- The **useControlServiceConnector** attribute has two values:
    - The default value is **false**, which means that the Connector BLOB on the server where the Media Service is installed is backed up.
    - Set the value to **true** to back up the Connector BLOB on the SharePoint Agent server. AvePoint recommends you not changing the value of the **useControlServiceConnector** attribute to **true**.

5. Save the configurations to the file and close it.

***Note**: To support writing the backup data of the Storage Manager BLOB or the Connector BLOB to a storage device that is TSM server 6.3.x, the TSM Client 7.1.2 is required on the DocAve Agent server where the BLOBs are backed up.

Using Form Mode to Create a Backup Plan

Form Mode is recommended for users who are familiar with building DocAve backup plans. To build a backup plan in Form Mode, select the content to be backed up, then click **Plan Builder** > **Form Mode**. 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.

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.

Managing Plans

For the created platform backup plans, you can use **Plan Manager** to manage them. After launching the **Platform Backup and Restore** interface, click **Plan Manager** next to the **Restore** tab. In the Plan Manager interface, all of the previously created plans are displayed in the main display pane.

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

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

***Note:** Any time the scope of a plan is changed, refresh the tree before continuing to use the plan.

- **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 backup 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 Platform Backup plan settings. Besides, you can click **Storage Policy, Staging Policy,** or **Customized Database** 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 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 of the settings on **Run Now** interface, see Configuring Run Now Interface.

Configuring Run Now Interface

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

***Note:** Any time the scope of a plan is changed, refresh the tree before continuing to use the plan.

- **Backup Type** – Select the type of the backup job you want to run on the selected plan. You can select **Full Backup**, **Incremental Backup**, or **Differential Backup** from the drop-down list. Refer to Overview of Backup Types for additional information.

***Note**: DocAve performs a **Full** backup when running any Platform backup plan for the first time, regardless of the backup plan chosen. An initial Full backup is mandatory for all plans.

***Note**: The VMs hosted by ESX/ESXi or vCenter support the Full Backup, Incremental Backup, and Differential Backup, but the VMs hosted by Hyper-V only support Full Backup. If the backup type of the backup job is set to Incremental Backup or Differential Backup, you can choose if to perform a full backup on the Hyper-V hosted VMs or skip backing up the Hyper-V VMs in the **Back up Hyper-V VMs** field.

- **Restore Granularity Level** – Select the granular index level for index generation in the backup job. You can select **Site Collection Level**, **Site Level**, **Folder Level**, **Item Level**, **Item Version Level**, and **None** as the granular restore index level.
- **Verify Database Backup Data**– Choose whether or not to verify the database backup data after a backup job has finished.

  ***Note**: If you select the checkbox for verifying database backup data, you must configure the **Staging SQL Server** setting.

- **Staging SQL Server** – Choose the SQL Server instance used to perform the database backup verification. By default, the **SQL server used for backup** is selected. You can choose to use **Remote SQL server** by selecting a staging policy from the drop-down list.
- **Check Agent Account Permissions for Backup** – Choose whether or not to check the Agent Account permissions for backup in the Platform Backup job. Select **Yes** to check the Agent account permissions in the backup job. If you are sure that your Agent Account has the required permissions for using Platform Backup and Restore, 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.
- **Job Report** – Select 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, the **BLOB Details** tab will be shown in the Job Monitor Job Details interface.
- **Would you like to remember these settings for future plans**? – Select **Yes, remember these settings** to remember these settings for the future usage when the current user performs any backup jobs. Otherwise, select **No, I will configure these settings again the next time I run a plan**.

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

- **Data Transfer Options** – Select when to transfer data from snapshots to backup storage. Transferring backup data from snapshots ensures the availability of the backup data for recovery when the production server is offline. It may use some resources to transfer. This field is only available when **Create Persistent Snapshot** is set to **Yes**.

- **Transfer data from persistent snapshots to backup data storage during the backup job** – Transfers the snapshot data immediately from the hardware to the corresponding storage device after the snapshot is complete. If this option is unchecked, no backup data is written to the storage device.

  ***Note**: If no persistent snapshot is created during the backup job, the snapshot data is always copied to the corresponding logical device regardless of whether this option is selected or not.

- **Transfer data from persistent snapshots to backup data storage during the maintenance job**– The snapshot data is not transferred to the storage device during the backup job. If you select this option, the snapshot data is transferred to the corresponding storage device in a scheduled/manual maintenance job that is run after the backup job completes.
- **Do not transfer data from persistent snapshots to backup data storage and only use snapshot for backup data** – Does not transfer the snapshot data to the media server.

- **Granular Index Options** – Choose when to generate the granular index. Selecting **Generate granular index during a backup job** can be resource intensive. To avoid resource conflicts, select Generate granular index during a maintenance job.
- **Back up Web Front-End Servers in Parallel** – Choose whether or not to back up the Web front-end servers in parallel. Selecting the **Back up Web Front-End servers in parallel** option requires you to enter in the text box the number of Web front-end servers that you want to back up in parallel.

  ***Note**: Backing up too many Web front-end servers in parallel can overload the Media Service.

  ***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**.

- **Granular Index Method** – Choose the way to generate index. **Sequential** will generate the index for the databases one by one. **Parallel** will generate the index for the databases simultaneously.
- **Run Command With Operation** – Select a command profile from the drop-down list to execute before or after the snapshot creation in the backup job. If you do not select the **Create Persistent Snapshots** option, this field will not be available to configure.
- **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.

*__Note:__ Any time the scope of a plan is changed, refresh the tree before continuing to use the plan.

Back up BLOB for Selected Scope – Choose whether or not to back up the BLOB content generated by Storage Manager and the files in the connected path of Connector. Select the corresponding checkboxes if you wish to back up the BLOB data. The BLOB data will be backed up in parallel. The Connector BLOB will be backed before the Storage Manager BLOB. By default, at most five Connector BLOBs or Storage Manager BLOBs will be backed up at the same time. You can navigate to the *…\AvePoint\DocAve6\Agent\data\SP2010\Platform\SP2010PlatformConfiguration.xml* directory to configure the maximum amount of BLOB data to back up in parallel. For more information, refer to Defining the Maximum Number of BLOB Backups Running in Parallel.

*__Note:__ Any time the scope of a plan is changed, refresh the tree before continuing to use the plan.

__Note:__ The default value is set to **5**, which means there will be at most five BLOB backups running in parallel.

__Note__: The BLOB data in NFS storage cannot be backed up or restored using Platform Backup and Restore.

__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 Archiver, select **Back up Storage Manager BLOB** option. In the same way, if you have BLOB data generated through Archiver in the backup scope, selecting **Back up Storage Manager BLOB** option will also back up the Archiver BLOB data together with the Storage Manager BLOB data during the backup job.

__Note__: If you want to back up BLOB data from the file share using VSS, the File Server VSS Agent Service must be enabled on the file server.

__Note__: The Storage Manager BLOB data stored in synchronous storage groups cannot be backed up when the computer where the devices are located is powered-off or is off-line.

- **BLOB Data Compression** – If you choose either or both **Back up Storage Manager BLOB** and **Back up Connector BLOB**, this field will appear. Selecting the checkbox enables BLOB data compression when performing a backup job for this plan.

  __Note__: This option supports Net Share and IBM Storwize Family devices; the data that is compressed or encrypted in Storage Optimization will not be compressed again.

- **Job Time Limit** – Select whether or not to define a time limit for the running time of this backup job.

    - **No time limit** – No matter how long this backup job will cost, DocAve will not stop this job automatically.
    - **Stop after _** (**Minutes**, **Hours** or **Days**) – DocAve will automatically stop this backup job after its running time exceeds the entered time limit.
- **Would you like to remember these settings for future plans**? – Select **Yes, remember these settings** to remember these settings for the future usage when the current user performs any backup jobs. Otherwise, select **No, I will configure these settings again the next time I run a plan**.
- Click **Ok** to run a platform backup job immediately based on the plan, click **Cancel** to return to the **Plan Manager** interface without running the platform backup job.

About InstaMount

It is recommended that you enable the InstaMount function to restore items that are small in file size. An InstaMount temporary database is much smaller (and uses less space on SQL Server) than a temporary database used during an ordinary restore. As a result, a Platform granular restore can be much faster when using InstaMount.

The InstaMount function can be enabled in either a backup or restore job. If you did not select **Yes** in **Enable InstaMount for Generating Granular Index** field when creating a backup plan, you still can use the **Browse the index in InstaMount** or **Use InstaMount** function when creating a restore plan.

However, if you are restoring large amounts of data, the advantages of InstaMount are not significant; it is not recommended that you use InstaMount in such cases. If the read speed of your device is slow, using InstaMount may lead to a session timeout. DocAve recommends not using InstaMount in this case.

***Note**: InstaMount can be used with the following storage types: Net Share, IBM Storwize Family, IBM Spectrum Scale Object, TSM, DELL DX Storage, or HDS Hitachi Content Platform.

InstaMount and Restore Index

The granular restore index is used for Platform granular restore. The granular restore index can be generated during a Platform Backup job or by a maintenance job.

- When running a Platform backup job with **Enable InstaMount for Generating Granular Index** not enabled, an index is generated directly from the databases being backed up. This may occupy more system resources on the corresponding SQL Server.
- The InstaMount function is used to generate a granular restore index during a maintenance job.

About the Platform Backup and Restore for SQL Mirroring Database

For your SharePoint environment, if there are principal databases and mirroring databases in the SQL Server, you can use the full/incremental/differential platform backup to back up your principal databases for ensuring safety in production. When the principal databases are switched to the corresponding mirroring databases which are used as failover databases, the incremental/differential platform backup job will be forced to the full platform backup job since the failover breaks the log chain.

***Note:** If you choose SQL authentication as the database authentication of a content database in SharePoint, make sure that the Agent account has the permission to login SQL Server of the destination. Otherwise the mirroring databases cannot be backed up when being used as failover databases.

***Note:** Before performing an In Place Restore at database level, you must manually terminate the mirroring relationship because a database cannot be deleted or overwritten when it is occupied, then the databases must be deleted to make the In Place Restore available. After completing the In Place Restore at database level, you can manually recover the mirroring relationship.

About the Platform Backup and Restore for Databases in AlwaysOn Availability Group

If you have enabled the AlwaysOn Availability Group feature and your SharePoint environment has configured primary replicas and secondary replicas in the SQL server, you can use Full, Incremental, and Differential Platform Backup to back up your databases in AlwaysOn Availability Groups for ensuring safety in production.

***Note**: To back up databases that reside on replicas, you must install DocAve Agents to each replica of the AlwaysOn Availability Groups.

***Note**: The Incremental or Differential backup jobs will be forced to Full backup jobs after a failover of the AlwaysOn Availability Group, since the failover breaks the log chain.

***Note**: When backing up secondary replicas, the Full Backup, Differential Backup, and Incremental Backup types are as follows:

- The data will be backed up via the copy-only SQL server backup method when using Full Backup and Differential Backup types.
- The data will be backed up via the log backup method when using the Incremental Backup types. .

About the Platform Backup and Restore for Failover Database

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

- 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.

- 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
- Machine Translation Service Database

Performing a Restore

Both Platform backup and Platform restore use Microsoft Volume Shadow Copy Services (VSS) snapshot technology to protect your SharePoint farm. A Platform restore can be performed only on data backed up using DocAve Platform Backup and Restore. Before building a restore plan, refer to Restoring Details for Specific Farm Components for important information regarding the restore of farm components.

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 database level or 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).
3. **Restore raw database** – Restores only the database to SQL Server.

***Note**: For information regarding the SharePoint components supported in Platform Backup and Restore, refer to Appendix D: SharePoint 2010 Components Supported in Platform Backup and Restore and Appendix E: SharePoint 2013 Components Supported in Platform Backup and Restore.

***Note**: The Platform Backup and Restore Agent account configured 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. The default filter rule filters the all of the backup jobs from the last seven days.
    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 Types** to list backup jobs for all levels.

b. **Filter by Job** – Limit the backup jobs by job type using the drop-down list.

   - **Backup Type** – Select the backup type from the drop-down list; only backup jobs of the selected type are displayed. Select **All Types** to list backup jobs for all three types.

c. **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.

2. 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.

   ***Note**: If the search scope of backup jobs is very large and some backup data is unavailable, loading the backup jobs may take a long time. Navigate to **Control Panel** > **System Options** > **Security Settings** for configuring **Session Timeout**. For more details, refer to DocAve 6 Control Panel Reference Guide.

   ***Note**: If you select a differential backup job to restore, the backup data of the full backup job that this differential job is based on will also be restored. If you select an incremental backup job to restore, there will be the following two scenarios:

   - If there are differential backup jobs performed before the selected incremental backup job in this backup cycle (a full backup job always starts a new cycle), the backup data of the full backup job and the latest differential backup job will be restored and the backup data of the incremental backup jobs between the latest differential backup job and the selected incremental backup job will also be restored.
   - If there is no differential backup job performed before the selected incremental backup job in this backup cycle, the backup data of the full backup job in this backup cycle, the selected incremental backup job, and all of the incremental backup jobs between the full backup job and the selected incremental backup job will be restored.

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 a backup job to display job information such as the Plan Name, Job ID, Backup Option, Restore Granularity Level, Backup Method, Create Persistent Snapshot, InstaMount Enabled, Index Status, Copy Data, Generate InstaMount Mapping, and Job Status. Click **Day**, **Week**, or **Month** to change the view to see all the available jobs during that time period.

- Click the page turn button ( ) on the top-left corner of the calendar to turn the page.

3. Now that you've 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 an In Place Restore Plan at Database Level
    - Building an In Place Platform Granular Restore Plan
    - Building an Out of Place Restore Plan at Database Level
    - Building an Out of Place Platform Granular Restore Plan
    - Restoring a Raw Database
    - Restoring Backed-Up VM
    - 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

***Note**: When restoring a database to the Microsoft SQL **AlwaysOn Availability Groups** in SQL Server 2012, make sure the database you are restoring to has been removed from the **AlwaysOn Availability Groups** before the restore. Be sure to add the restored database back to the **AlwaysOn Availability Groups** after finishing the restore.

Building an In Place Restore Plan at Database Level

After DocAve completes each In Place Platform restore job of a SharePoint database at the database level, a full backup of the restored SharePoint databases is performed automatically in the next backup job. This ensures data integrity and protects your farm.

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** – If the **Back up the whole farm with VM** option is selected in the backup plan of the selected backup job, you are required to choose the SharePoint farm backup data or VM backup data to restore. In this case, select **Restore SharePoint farm backup data**.
3. 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 in your selected Web applications or content databases. For more details, refer to Appendix A: About Find Site Collection.

4. **Restore Type** – Configure the restore type and select the Agent group to perform the restore job in this page.

    a. **Restore Type –** Choose where the content will be restored.

        - **Restore SharePoint farm components** – Select the location where to restore the backup data. In this case, select **In place restore** to restore the database to the original SharePoint location.
        - **Restore raw database** – Choose this option to restore the database in the backup to another SQL Server. Refer to Restoring a Raw Database for more information on performing this option.

    b. **Agent Group** – Select an Agent group to run the restore job for load balancing and performance. Click **View** to view the details of the selected Agent group.

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

    c. **Restore Option** – Select to restore the Platform Backup data or restore the third-party backup data of the component to the target. The Restore wizard that follows will vary depending to the restore option you selected. If you select to restore the third-party backup data of the component, refer to In Place Restoring From Third-Party Backup Data at Database Level.

    ***Note**: The **Restore from third-party backup data** feature does not support restoring the BLOB data.

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 first performs an incremental backup for the selected databases, restores the backed-up database from the backup job selected in the Job Selection step, and then modifies the database to its most recent status using the log files that were backed up during last Incremental backup. Select No to restore only the backed up database.

    ***Note**: If there are new database file added to your content database not being backed up, please pay attention to the following known issue: When performing the restore job of **Restore Database to Most Recent State** to restore the database with **Safe Restore** option selected, the restore job will fail to restore the database to its most recent state and the newly added database file will be deleted after the restore.

    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. **Safe Restore** – A Safe Restore keeps the destination intact in the event that the restore job fails.

   - In an **Overwrite** restore job, selecting **Yes** restores the databases to a temporary database first (as a safety precaution in the event that the restore job fails). If the restore job completes successfully, the original database is deleted. Then, the temporary database is renamed to the original database name and it is connected to the SharePoint farm. If you select **No**, the original database is deleted as soon as the **Overwrite** restore job begins.
   - In the case of a **Skip** restore job at the database level, the restore job performs no action on the database in question if the original database has the same name as the one in the backup.

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. **Run Command With Operation** – This field is only available when the backup job selected for performing this restore has the **Create Persistent Snapshot** feature enabled. Select a command profile from the drop-down list to execute before or after the restore job.

f. Configure the email **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.

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

6. **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.

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

7. Review and edit the **Data Selection**, **Restore Type**, **Restore Settings**, and **Schedule** for the restore job. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
8. 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.

In Place Restoring From Third-Party Backup Data at Database Level

Complete the steps below to restore the third-party backup data of the components:

1. **Notification** – Configure the email 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.
2. Click **Next**. A message will pop up to inform you that the databases you select to restore will be disconnected for a moment, and the databases will be reconnected after being successfully verified in the **Verification** step. Click **OK** to proceed.
3. **Verification** – Ensure the backup data of the databases listed in the table has been placed in the location displayed under **Original Location** column, and then click **Verify and Restore** in the lower-right corner. After successfully verified and restored the databases, click **Finish**.

Building an In Place Platform Granular Restore Plan

To build and run in place restore of the granular data, complete the steps below:

1. Follow the instructions in Performing a Restore to begin building the plan.
2. **Data Selection** – If the **Back up the whole farm with VM** option is selected in the backup plan of the selected backup job, you are required to choose the SharePoint farm backup data or VM backup data to restore. In this case, select **Restore SharePoint farm backup data**.
3. 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 Content** link beside the content database to view detailed information about the selected database. For details about searching the granular data using the **Advanced Search** feature, refer to Appendix B: About Advanced Search.

***Note**: If you want to restore the forms-based authentication users in the site collection that has the forms-based authentication enabled, you must configure the **Web.Config** files in every

Web front-end server in the farm. For more information, refer to Configure forms-based authentication for a claims-based web application in SharePoint 2013.

4. You can navigate directly to the **Backup Data** tab to expand the granular data tree. The stored index of the backup data 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 inform you to select the **Browse the index in InstaMount** option to continue loading the tree.

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

   - **Restore Granular Content**– Select this option to restore granular content. If you start 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 will be reloaded and you can only browse the tree to the site collection level without the **Restore Granular Content** option is selected. Refer to Deselecting the Restore Granular Content Feature for detailed information.
     - **Browse Method** – Choose whether or not to browse the tree from the index generated using InstaMount. The current granular level of your stored index in the backup data will be displayed on the left in bold.
     - **Browse the index in InstaMount** – Browse from the index generated using InstaMount. When **Restore Granular Content** is selected and you select this option, the tree is generated on the fly and can be displayed down to item version level regardless of the database's original restore granularity.

       By default, the InstaMount temporary database is stored on the SQL Server that DocAve has backed up. To change the location of the InstaMount temporary database, select a staging policy from the drop-down list for storing the InstaMount temporary database generated during browsing. For more information, refer to About the Staging Policy.
   - **Container Selection** – Select the **Global setting for container configuration** checkbox to enable the container's global settings.
     - **Restore container** – Restore the container and 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 H: SharePoint Object Security and Property.
     - **Only restore security –** Only restore 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 only takes effect when the selected nodes in the backup data stop inheriting 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** – Restore the content and select the **Security** checkbox if you want to restore the content's security settings along with. For more information, refer to Appendix H: SharePoint Object Security and Property.
    - **Only restore security** – Only restore 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 only takes effect when the nodes in the backup data stop inheriting 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 only display **Skip** and you will not be able to configure the other Content level conflict resolution through that page.

5. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the **Item Browser** pop-up window. Select the configuration of the content being restored.
    a. **Security** – Refer to Appendix H: SharePoint Object Security and Property for detailed information related to security.
    b. **Property** – Refer to Appendix H: SharePoint Object Security and Property for detailed information related to property.
6. The **Recycle Bin** nodes under the top-level site and the sub site nodes contain the recycle bin content of the restore level that you have selected in this backup job. If you want to restore the deleted content from recycle bin, select the **Recycle Bin** node. The **Item Browser for Recycle Bin** window appears. Select the objects to be restored, and click **OK**.

   Note the following:

    - If the content in the recycle bin is a stub, the stub can be restored but the BLOB cannot be restored by Platform Restore.

- If you select the whole site collection to restore, then the content in the recycle bin cannot be restored.
- The Apps in the Recycle Bin are not supported to be restored.

7. When finished, click **Next**. The **Stub and BLOB Configuration** page appears.
8. **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 have used.
        - **Default Platform Backup** – Use the stub database that has been backed up by a Platform Backup 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 Connector device.

    ***Note**: If the BLOB data has been removed from the device, the restored stub is invalid and cannot link to its related BLOB data.

9. **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 have 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 device.
10. When finished, click **Next**. The **Restore Type** page appears.
11. **Restore Type** – Choose where 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. **Agent Group** – Select an Agent group to perform the restore job for load balancing and performance. Click **View** to view the details of the selected Agent group.

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

12. Click **Next** when finished. The **Restore Settings** page appears.
13. **Restore Settings** – Configure how the content will be restored.
    a. **Conflict Resolution** –Select an option to dictate how to resolve conflicts at the container level and content level.
        - **Container level conflict resolution** – Set the conflict resolution on the site collection, site, list, and folder level.
            - **Skip** – Ignores the source container that has the same name as the destination.
            - **Merge** – Combines the configuration of the source and destination container. If there is a conflict, the source overwrites the destination.
            - **Replace** – Deletes the destination container and then restores the source to the destination. If the selected container is a root site, **Replace** function empties the root site instead of deleting it and restores the source to the destination. This option can only be used at folder/site/site collection level.

            ***Note:** A discussion board item is considered a folder, so it is restored as a container.

        - **Content level conflict resolution** – Sets 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 add a suffix (_1, _2, _3…) to the name of the conflict source item/document.
            - **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** – Select a conflict resolution if the Apps in the source and destination conflict. You can choose "**Skip**", "**Update App Only**", or "**Replace App and AppData**" from the drop-down list.

   - **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 original 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 original SharePoint farm, then 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. **Use InstaMount** – Select whether to use InstaMount when performing the Platform granular Restore. Selecting **Yes** generates an InstaMount temporary database used for the Platform granular restore. Selecting **No** generates an ordinary temporary database used for the Platform granular restore; this temporary database is the same as the backed-up database that stores the granular content. Refer to InstaMount and Restore Index for more information.

f. **Staging Policy** – Select the Staging Policy, which stores the temporary database during the Platform granular restore when necessary. If you select **None**, the temporary database is stored on the SQL Server being restored to. For more information, refer to About the Staging Policy.

g. **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.

h. **Item Dependent Columns and Content Types** – Choose whether to restore item-dependent columns and content types.

***Note:** If you did not select **Property** besides the selected node in the **Data Selection** step, and the dependent column or content type does not exist in the destination, then that 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.

i. **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.

j. **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 selected. The other versions are not restored.

***Note:** The latest version does not take the current version into account.

k. **Notification** – Configure the email **Notification** settings. Select a previously configured notification profile from the **Select a profile with address only** 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.

14. When finished configuring Restore Settings, 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. 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.

16. Review and edit the Data Selections, Restore Type, Restore Settings, and Schedule for the restore job. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
17. 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 Restore Plan at Database Level

***Note**: If you backed up the content database with file stream data using persistent snapshot, the out of place restore job at the database level may fail.

To build and run an out of place restore job at the database level, complete the following steps:

1. Follow the instructions given in Performing a Restore to begin building the plan.
2. **Data Selection** – If the **Back up the whole farm with VM** option is selected in the backup plan of the selected backup job, you are required to choose the SharePoint farm backup data or VM backup data to restore. In this case, select **Restore SharePoint farm backup data**.
3. Expand the farm tree, and select the content you want to restore using the tree. The content in the tree will vary depending upon the type of backup selected. In this case, select the backed-up databases or Web applications. You can restore the backed up Storage Manager BLOB data and stub database together with the selected Web application and content databases to the destination, when you select the Web application node on the backup data tree.
4. **Restore Type** – Choose where the content will be restored.

   ***Note:** Platform Restore 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.

   - **Restore SharePoint farm components** – Select the location where to restore the backup data. In this case, select **Out of place restore** to restore the database to another SharePoint farm. Then, select the **Destination Farm** from the drop-down list.
   - **Restore raw database** – Choose this option to restore the database in the backup to another SQL Server. Refer to Restoring a Raw Database for more information.
   - **Restore BLOB Data and Stub Database** – If you selected the Web applications in the **Data Selection** step and there is Storage Manager BLOB data and a stub database backed up with the Web application, the **Restore BLOB Data and Stub Database** field will appear. Select whether or not to restore the Storage Manager BLOB data and stub

database with the selected content database. Select the **Restore Storage Manager BLOB and Stub Database** option to restore the backed up Storage Manager BLOB data and stub database.

***Note**: If you edit the restored items and/or 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**: You must install the RBS provider in the destination SharePoint farm if your backed up content database contains file stream data.

- **Agent Group** – Select the Agent group that will perform the restore job for load balancing and performance. Click **View** to view the details of the selected Agent group.

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

- **Restore Option** – Select to restore the Platform Backup data or restore the third-party backup data of the component to the target. The Restore wizard that follows will vary depending to the restore option you selected. If you select to restore the third-party backup data of the component, refer to Out of Place Restoring From Third-Party Backup Data at Database Level.

  ***Note**: The **Restore from third-party backup data** feature does not support restoring the BLOB data.

5. Click **Next**. The **Destination Component Options** page appears.
6. **Destination Component Options** – Select the conflict resolutions for the destination component being restored. Display the **Detailed Information** of the database being restored, including its name and type. Click **Edit** in the **Details** column to edit the following properties.

   ***Note**: If you select the **Restore Storage Manager BLOB and Stub Database** option in the **Restore Type** step, you are required to edit the destination settings for the backed up Storage Manager stub database.

   ***Note**: To perform an out of place restore for an entire Web application/service application/service application proxy, detailed information for creating the Web application/service application/service application proxy in the destination must be configured.

   - **Content Database** – The name of the database that has been backed up.
   - **Database Server** – The destination database server for the restore.
   - **Database Name** – The database will be restored using the name entered here.
   - **Database and Log File Mapping** – Click **Details** to enter the name and path of the destination database file/log file.

***Note**: If the specified path does not exist on the destination server, DocAve builds the path automatically during restore.

- **Parent Web Application URL** – The database will be restored to the Web application entered here.
- **Database Access Credentials** – Select the authentication method used to create the database.
    - **Windows authentication (recommended)** (the default option) – Use this method if you want the user identity to be confirmed by Windows.
    - **SQL authentication** – SQL Server confirms the user identity itself according to the entered Account. The entered account must be added to the **sysadmin** role in SQL Server.
    - **Stored credentials** – This method appears when authenticating a SQL Server Reporting Services (SSRS) Service Database. To use SQL authentication, specify the stored authentication that will be used to connect to the database and if the stored credentials should be used as Windows Credentials.

      ***Note**: The account that is used to provision the database is the application pool identity of SharePoint Central Administration.
- **Failover Database Server** – Choose whether or not to associate the database being restored with a specific failover SQL Server that is used in conjunction with SQL Server database mirroring.

  ***Note**: Only the configured Failover Database Server property can be restored to the destination. After the restore job you must manually perform the Failover configurations in SQL server to realize the Failover feature.

7. **Physical Device Mapping** – If you select the **Restore Storage Manager BLOB and Stub Database** option in the **Restore Type** step, 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.

   ***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.

   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:

   a. Select the checkbox beside a physical device mapping item, and then click **Destination Physical Device** on the ribbon. The BLOB Batch Settings Page appears.

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**: DocAve does not support the out-of-place restore of BLOB data to physical devices other than Net Share and IBM Storwize Family devices.

8. Click **Next**. The **Restore Settings** page appears.
9. **Restore Settings** – Choose detailed settings for the restore job.
    - **Safe Restore** – In an **Overwrite** restore job, **Yes** restores the selected database to a temporary database first (as a safety precaution in the event that the restore job fails). After the restore job completes successfully, the **destination** database is deleted, and the temporary database is renamed to the destination database name and then connected to the SharePoint farm. If you select **No**, the destination database is deleted directly when the **Overwrite** restore job begins. In the case of a **Skip** restore job at the database level, the restore job performs no action if the destination database has the same name as the one in the backup.
    - **Conflict Resolution** – Select whether or not to overwrite the destination contents if there is a conflict between the destination 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 destination 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 destination farm, then the destination database is deleted first and the database in the backup is then restored.
    - **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, and does not support mapping two or more source users to one destination user.

        - **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.

- **Run Command With Operation** – This field is only available when the backup job selected for performing this restore has the **Create Persistent Snapshot** feature enabled. Select a command profile from the drop-down list to execute before or after the restore job.
- **Job Report** – Choose the level of reporting for the restore job**. Simplified** creates a summary of the data to restore**. Detailed** creates a full list of all objects to restore at the cost of performance. If you select Storage Manager or Connector BLOB data to restore, the **BLOB Details** tab will be show in the Job Monitor Job Details interface.
- **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.

10. When finished configuring Restore Settings, click **Next**. The **Schedule** page appears.
11. **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.

12. Review and edit the **Data Selection**, **Restore Type**, **Restore Settings**, and **Schedule** for the restore job. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
13. 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.

Out of Place Restoring From Third-Party Backup Data at Database Level

Complete the steps below to continue the wizard for an out of place restore from third-party backup data at database level:

1. **Destination Component Options** – Select the conflict resolutions for the destination component being restored. Display the **Detailed Information** of the database being restored, including its name and type. Click **Edit** in the **Details** column to edit the following properties.

***Note**: To perform an out of place restore for an entire Web application, service application, or service application proxy, detailed information for creating the application in the destination must be configured.

- **Content Database** – The name of the database that has been backed up.
- **Parent Web Application URL** – The database will be restored to the Web application entered here.
- **Database Server** – The destination database server for the restore.
- **Database Name** – The database will be restored using the name entered here.
- **Database Access Credentials** – Select the authentication method used to create the database.
    - **Windows authentication (recommended**) (the default option) – Use this method if you want the user identity to be confirmed by Windows.
    - **SQL authentication** – SQL Server confirms the user identity itself, according to the entered Account. The entered account must have the **sysadmin** role in SQL Server.
    - **Stored credentials** – This method appears when authenticating a SQL Server Reporting Services (SSRS) Service Database. To use SQL authentication, specify the stored authentication that will be used to connect to the database and if the stored credentials should be used as Windows Credentials.

      ***Note**: The account that is used to provision the database is the application pool identity of SharePoint Central Administration.
- **Failover Database Server** – Choose whether or not to associate the database being restored with a specific failover SQL Server that is used in conjunction with SQL Server database mirroring.

  ***Note**: Only the configured Failover Database Server property can be restored to the destination. After the restore job you must manually perform the Failover configurations in SQL server to realize the Failover feature.

2. Click **Next**. The **Restore Settings** page appears.
3. **Restore Settings** – Choose detailed settings for the restore job.
    - **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.

- **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**: 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.

4. Click **Next**. A message will pop up to inform you that the databases you select to restore will be disconnected for a moment, and the databases will be reconnected after being successfully verified in the **Verification** step. Click **OK** to proceed.
5. **Verification** – Ensure the backup data of the databases listed in the table has been placed in the location displayed under **Original Location** column, and then click **Verify and Restore** in the lower-right corner. After successfully verified and restored the databases, click **Finish**.

Building an Out of Place Platform Granular Restore Plan

To build and run an out of place Platform granular restore plan, complete the following steps:

1. Follow the instructions given in Performing a Restore to begin building the plan.
2. **Data Selection** – Configure the following settings:
    a. Select the database that includes the granular content to restore.
    b. Click **View Granular Content** next to the selected database to view the detailed backup data for the selected database. For details about searching the granular data using the Advanced Search feature, refer to Appendix B: About Advanced Search.
    c. Navigate directly to the **Backup Data** tab to expand the granular data tree. The stored index of the backup data will be used to load the backup data tree.
    d. Select your desired granular level nodes to restore. If no stored index is detected, DocAve will inform you to select the **Browse the index in InstaMount** option to continue loading the tree.

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

- **Restore Granular Content**– Select this option to restore granular content. If you start 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 will be reloaded and you can only browse the tree to the site collection level without the **Restore Granular Content** option is selected. Refer to Deselecting the Restore Granular Content Feature for detailed information.
- **Browse Method** – Choose whether or not to browse the tree from the index generated using InstaMount. The current granular level of your stored index in the backup data will be displayed on the left in bold.
    - **Browse the index in InstaMount** – Browse from the index generated using InstaMount. When **Restore Granular Content** is selected and you select this option, the tree is generated on the fly and can be displayed down to item version level regardless of the database's original restore granularity.

      By default, the InstaMount temporary database is stored on the SQL Server that DocAve has backed up. To change the location of the InstaMount temporary database, select a staging policy from the drop-down list for storing the InstaMount temporary database generated during browsing. For more information, refer to About the Staging Policy.
- **Container Selection** – Select the Global setting for container configuration checkbox to enable the container's global settings:
    - **Restore container** – Restore the container and 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 H: SharePoint Object Security and Property.
    - **Only restore security –** Only restore 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 only takes effect when the nodes in the backup data stop inheriting 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 though that page.
- **Content Selection** – Select the **Global setting for content configuration** checkbox to enable the content's global settings.

- **Restore content** – Restore the content. Additionally, select the **Security** checkbox if you want to restore the content's security settings along with. For more information, refer to Appendix H: SharePoint Object Security and Property.
- **Only restore security** – Only restore 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 only takes effect when the nodes in the backup data stop inheriting 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 only display **Skip** and you will not be able to configure the other Content level conflict resolution though that page.

3. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the **Item Browser** pop-up window. Select the configuration of the container being restored.
   - **Security** – Refer to Appendix H: SharePoint Object Security and Property for detailed information related to security.
   - **Property** – Refer to Appendix H: SharePoint Object Security and Property for detailed information related to property.
4. The **Recycle Bin** nodes under the top-level site and the sub site nodes contain the recycle bin content of the restore level that you have selected in this backup job. If you want to restore the deleted content from recycle bin, select the **Recycle Bin** node. The **Item Browser for Recycle Bin** window appears. Select the objects to be restored, and click **OK**.

   Note the following:
   - You can only select one object in the **Item Browser for Recycle Bin** window to perform an out-of-place restore. If you select more than one object, the **Out of place restore** type will be grayed out.
   - If the content in the recycle bin is a stub, the stub can be restored but the BLOB cannot be restored by Platform Restore.
   - If you select the whole site collection to restore, then the content in the recycle bin cannot be restored.
   - The Apps in the Recycle Bin are not supported to be restored.
5. When finished, click **Next**. The **Stub and BLOB Configuration** page appears.

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 have used.
        - **Default Platform Backup** – Use the stub database that has been backed up by Platform Backup job to restore.
        - **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 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 select which backup method you have 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 storage device.
8. When finished, click **Next**. The **Restore Type** page appears.
9. **Restore Type** – Choose where the content will be restored.

    ***Note:** Platform Restore 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.

- **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.
- **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, select a node with a blank text box, and then enter the URL of the destination node into the text box following the format displayed in the text box. 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 text box to create the node in the destination farm. Alternatively, click **Create Container** in the **Manage** group on 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 the instructions in Appendix B: About Advanced Search.
- **Agent Group** – Select the Agent group that will perform the restore job for load balancing and performance. Click **View** to view the details of the selected Agent group.

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

- **Action** – Select how the data will be restored to the destination.
  - **Merge** – Merge will add the contents to the destination node.
  - **Attach** – Attach will restore the contents as children beneath the selected node.

  To see what the data tree of the destination node 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. The

screenshot below shows that the source site collection is attached to the destination Web application:

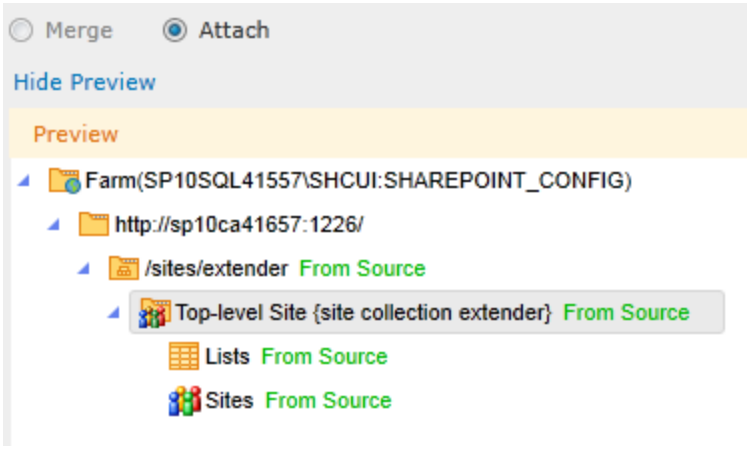


Figure 9: Attaching site collection backup data of DocAve 6 to the destination Web application.

***Note**: For the backup data imported from DocAve 5, when attaching the site collection to the destination Web application, the source Web application URL will be attached to the site collection URL. Refer to the screenshot below:

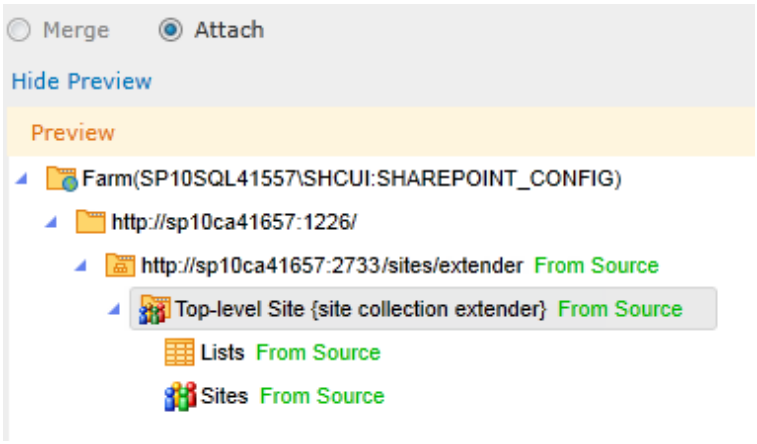


Figure 10: Attaching the site collection backup data imported from DocAve 5 to the destination Web application.

- **Mapping Settings** (Optional) – Configure 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.
    - **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.

- **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.

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

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

10. Click **Next** when finished. The **Restore Settings** page appears.
11. **Restore Settings** – Configure how the content will be restored.
    a. **Conflict Resolution** –Select an option to dictate how to resolve conflicts at the container level and content level.
       - **Container level conflict resolution** – Set the conflict resolution on the site collection, site, list, and folder level.
         - **Skip** – Ignores the source container that has the same name as the destination one.
         - **Merge** – Combines the configuration of the source and destination container. If there is a conflict, the source overwrites the destination.
         - **Replace** – Deletes the destination container and then restores the source to the destination. If the selected container is a root site, **Replace** function empties the root site instead of deleting it and restores the source to the destination. This option can only be used at folder/site/site collection level.

         ***Note**: A discussion board item is considered a folder, so it is restored as a container.

       - **Content level conflict resolution** – Sets 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. I
         - **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 add a suffix (_1, _2, _3…) to the name of the conflict source item/document.

- **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** – Select a conflict resolution if the Apps in the source and destination conflict. You can choose "**Skip**", "**Update App Only**", or "**Replace App and AppData**" from the drop-down list. To successfully restore SharePoint Apps, make sure the Agent account that will 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 previous 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 **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, then 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. **Use InstaMount** – Select whether to use InstaMount when performing the Platform granular Restore. Selecting **Yes** generates an InstaMount temporary database used for the Platform granular restore. Selecting **No** generates an ordinary temporary database used for the Platform granular restore; this temporary database is the same as the backed up database where the granular content is stored. Refer to InstaMount and Restore Index for more information.

f. **Staging Policy** – Select the Staging Policy, which stores the temporary database during the Platform granular restore when necessary. If you select **None**, the temporary database is stored on the SQL Server being restored to. For more information, refer to About the Staging Policy.

g. **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.

h. **Item Dependent Columns and Content Types** – Choose whether to restore item-dependent columns and content types.

   ***Note:** If you did not select **Property** besides the selected node in the **Data Selection** step, and the dependent column or content type does not exist in the destination, then that 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.

i. **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.

j. **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 selected. The other versions are not restored.

   ***Note:** The latest version does not take the current version into account.

k. **Notification** – Configure the email **Notification** settings. Select a previously configured notification profile from the **Select a profile with address only** 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**. The **Schedule** page appears.
13. **Schedule** – Choose whether or not to create the restore job based on a schedule. Select **Restore once finish the wizard** 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.

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

14. Review and edit the Data Selection, Restore Type, Restore Settings, and Schedule for the restore job. 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.
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.

Restoring a Raw Database

This option must be used to restore the SharePoint configuration database in the backup to another SQL Server. To restore only the database to a SQL Server, select **Restore Raw Database** as the Restore Type and then configure the **Destination Component Options**:

***Note**: If you backed up the content database with file stream data using persistent snapshot, the restore job using **Restore Raw Database** as the **Restore Type** may fail.

1. **SQL Agent** – All of the SQL Agents (DocAve Agents that are installed on the SQL database servers) are listed in the drop-down box. Select one SQL Agent to restore the backed-up database to the selected SQL instance.
2. **SQL Instance** – Select an SQL Instance to store the restored content database.
3. **Database Access Credentials** – Select the authentication method used to create the database.
    - **Windows authentication (recommended)** (the default option) – Use this method if you want the user identity to be confirmed by Windows.
    - **SQL authentication** – SQL Server confirms the user identity itself according to the entered Account. The entered account must be added to the **sysadmin** role in SQL Server.
4. **Detailed Information** – Displays the detailed information of the database to be restored, including its name and type. Click **Edit** in the **Details** column to edit the following properties.
    a. **Database Name** – The database is restored using the name entered here.

    ***Note**: If you select the **Restore raw database** type to restore the selected content database, please do not change the name when you deselect the **Safe Restore** option. Otherwise, the database will be deleted and the restore job fails.

    b. **Database and Log File Mapping** – Click **Details** to enter the name and path of the destination database file/log file.

    ***Note**: If the entered path does not exist on the destination server, DocAve creates the path automatically during the restore job.

Restoring Backed-Up VMs

To restore the backed-up VMs, complete the steps below:

1. Follow the instructions provided in Performing a Restore to begin building the plan. Select a backup job with VM that up.

   ***Note**: When restoring ESX/ESXi VMs in vCenter host cluster, please pay attention to the following conditions:

   - If the original host in the cluster is not available, the VM will be restored to the host that contains all of the databases used by the VM in the cluster.
   - When restoring DRS rule, DocAve uses the names of DRS group and DRS rules to check if the DRS group where the backed up VM resides still exists. If the DRS group still exists, the VM will be restored to this DRS group. If the DRS group does not exist, it skips restoring the DRS group.

   ***Note**: When restoring ESX/ESXi VMs in the datastores that are in vCenter datastore cluster, DocAve supports restoring datastore rules of **VMDK anti-affinity** and **VMDK affinity** for virtual disks, but does not support restoring datastore rules of **VM anti-affinity** or **VM affinity**.

2. **Data Selection** – Select **Restore VM backup data**. The backed up VMs are listed in the table of the **Backup Data** tab.
3. Select an Agent for each VM to execute the restore job. By default, the Agent in the host profile used by the backup plan is selected. Also choose if you want to power on the target VM after the restore.

   ***Note**: The Hyper-V hosted VMs will use the Agent that has been used to execute the backup job for the restore, and the Agent cannot be changed in the restore wizard.

   ***Note**: When restoring the VMs in the Hyper-V Cluster, the selected Agent must be on the node in the cluster.

   ***Note**: When restoring the VMs on ESX/ESXi or vCenter host server, AvePoint recommends you do not select the Agents on the VMs to be restored.

4. Click **Next**. The **Restore Settings** page appears.
5. **Restore Settings** – Configure the detailed settings for restoring VM.
6. **VM Conflict Resolution** – Define the VM conflict resolution behavior.

   For the ESX/ESXi or vCenter hosted VMs, if a **.vmx** configuration file in the target resides in the same location as the **.vmx** configuration file in the backup, it is considered as a conflict.

   For the VMs stored on the datastores that are in vCenter datastore cluster, if there is a VM whose name is the same as the backed up VM in the datastore cluster, it is considered as a conflict.

For the Hyper-V hosted VMs, if a VM ID same as the one in the backup already exists in the destination, it is considered as a conflict.

- **Skip** – Do not restore the source conflicting VM, and keep the destination VM intact.
- **Replace Virtual Disk Only** – Delete the data in the virtual disks of the target conflicting VM and then restore the data in the virtual disks of the backed up VM to the destination VM, without the VM configurations.

  ***Note: Replace Virtual Disk Only** is invalid for the VMs managed by the Hyper-V host. If you set the VM conflict resolution to **Replace Virtual Disk Only** when restoring VM on Hyper-V host, the conflicting VM will be removed, and the backup data of the VM will be restored.

- **Overwrite** – Delete the conflicting VM in the destination and restore the backed up VM.

7. **Hyper-V Parent Disk Conflict Resolution** – Define the Hyper-V parent disk conflict resolution behavior. If the Hyper-V parent disk in the source has the same full path as an existing Hyper-V parent disk in the target, it is considered as a conflict. This option is only functional for the restore of VMs hosted by Hyper-V. Note that if the restore of the Hyper-V hosted VM in the backup is skipped, the Hyper-V parent disk will not be restore, regardless of the selected **Hyper-V Parent Disk Conflict Resolution**.
   - **Skip** – Do not restore the source conflicting Hyper-V parent disk.
   - **Overwrite** – Delete the target Hyper-V parent disk, and restore the backed up parent disk.
8. **Notification** – Configure the email **Notification** settings. Select a 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.
9. When finished configuring Restore Settings, click **Next**. The **Schedule** page appears.
10. **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.

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

11. Review and edit the **VM List** selected to restore, the **Restore Settings**, and **Schedule** for the restore job. To make changes, click **Edit** in the middle of the row on the **Restore Data** tab or **Settings** tab to go to the corresponding page. This links to the corresponding setting page, allowing you to edit the configuration.
12. 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 Backed-Up Web Front-End Files

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

1. Follow the instructions given in Performing a Restore 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 files as you wish, 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 the Web front-end files.

- **Installed Programs** – This function checks the status of the 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 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 detailed lists is downloaded to the entered local path. A zip file that contains a .csv of detailed lists is downloaded to the specified local path.

There is also one special restore setting for restoring the Web front-end files.

- **Restore Web Front-End File Security** – This option only applies to the front-end files backed up, including IIS site files (except the web.config file), SharePoint hive files and extra file system files. When the option is used, both file contents and security permissions are restored. Otherwise, only the file content is restored.

For more information on restoring the backed-up Web front-end files, refer to Appendix I: Advanced Settings in Configuration Files.

Restoring Backed-Up BLOB Data

If you selected to back up Storage Manger 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 at 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**: If you want to perform an out of place restore to restore the stub database, the related BLOB data and content databases, AvePoint recommends performing the out of place restore at database level to select the Web application with **Restore BLOB Data and Stub Database** option enabled. For details, refer to Building an Out of Place Restore Plan at Database Level.

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**.

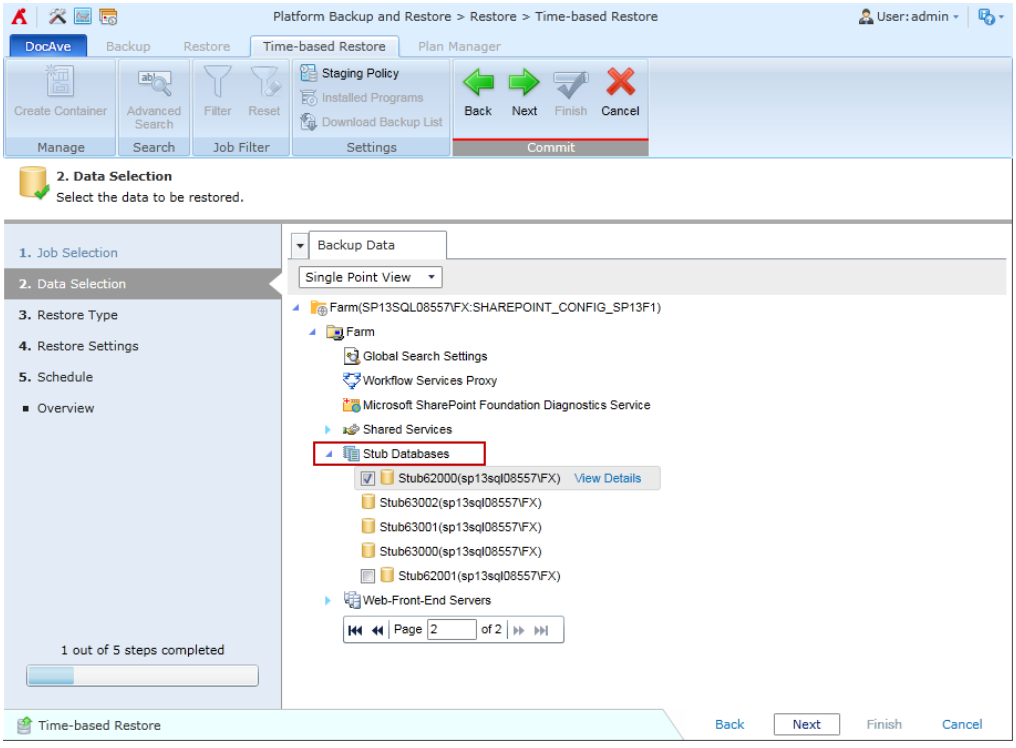


Figure 11: Select a stub database to restore.

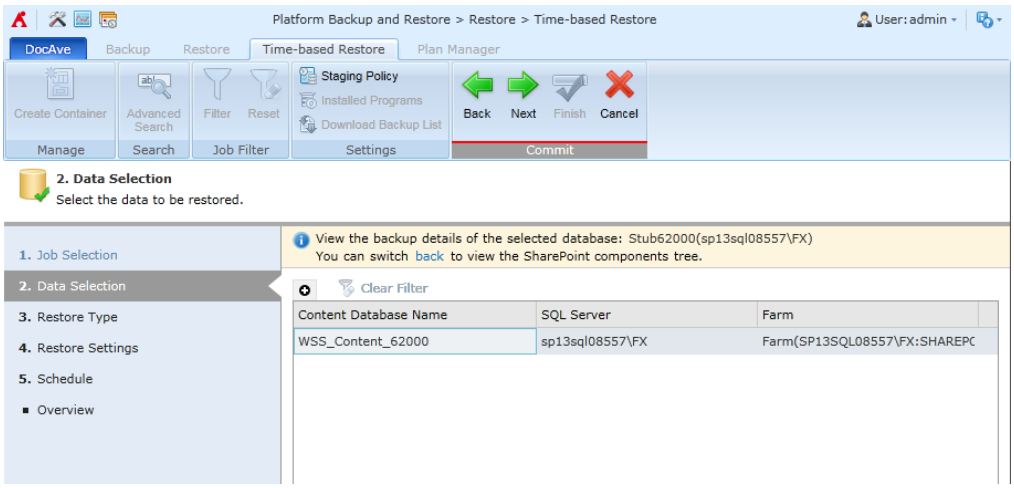


Figure 12: View the details of the stub database.

2. Click the **Next** button at the bottom-right corner to go to the **Restore Type** page.

    - **Restore SharePoint farm components** – Select the location where to restore the backup data. In this case, select **In place restore** to restore the database to the original SharePoint location.
    - **Restore raw database** – Choose this option to restore the database in the backup to another SQL Server. Refer to Restoring a Raw Database for more information on performing this option.
    - **Agent Group** – Select an Agent group to run the restore job for load balancing and performance. Click **View** to view the details of the selected Agent group.

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

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 an In Place 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 selected **Start time** that you configure. For the detailed explanation of each option, refer to Building an In Place 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 Platform Restore 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\DocAve6\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 **Conflict Resolution**.
5. Run the Platform Restore job to restore the backed-up database master key.

   ***Note**: By default, the database master key password will be restored to **1qaz2wsxE**. Please 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 that you perform the restore at the site collection level and deselect the **Restore Granular Content** checkbox. In this case, the restore will be similar to an STSADM site collection level restore. It is faster and can maintain internal document IDs.

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

Restoring 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 the **Restore Database Only** or Restoring a Raw Database. The SharePoint Central Administration Content 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 Content 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 the 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 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. When a SharePoint solution is restored out of place, the status of the solution will be restored to **Not Deployed**.

Depending on the customizations contained in the SharePoint solution, the solution may need to be re-configured after the deployment.

- **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 hive folder, they can be restored as well. Both IIS site files and 14 hive files can be restored out-of-place to another location for further examination.

  ***Note**: Certificates used by the IIS sites will not be backed up when backing up the front-end resources. You must manually backup 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.

Performing a Disaster Recovery

This section describes how to perform a disaster recovery (DR) using full farm backup data from the perspective of both SharePoint and DocAve. It does not include how to recover Active Directory (AD) or any other components not backed up by DocAve. Prior to performing this restore, the following requirements must be met:

- The SharePoint configuration database must be backed up in the backup job that you are about to use for Disaster Recovery.
- At the DR site, all server topology should be identical to the production site, which includes both the SharePoint farm topology and DocAve topology. The system platform must also match the platform at the time of backup. For example, an x64 system should be used if an x64 system was used at the time of backup.

  ***Note**: You must install the DocAve Agents on all of the servers (no matter SharePoint servers or SQL servers) in the disaster recovery environment.

  ***Note**: Make sure the logon user of SQL Writer is not the same as the logon user of Osearch Service and Help Search Service, when the SQL Server is installed on the SharePoint Server. Otherwise, the restoration of databases will fail in the Farm Rebuild wizard.
- All related software installed on the DR side should be the identical version and the patch level as before. Examples of related software are: SharePoint, SQL Server, DocAve, as well as the .NET Framework.
- The hostname of the source and the destination should be the same.

  If you use IP in the configuration, for example, using IP to configure DocAve Media Service, the IP should be the same. For SQL, the instance name and alias of the source and the destination should be the same, but the port can be different. If you install DocAve in other places, you should use identical hostname or IP for DocAve. 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.
- The DR site is in the same AD domain as the original location.

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

1. Install all required software components (for example, SQL Server).

2. Install SharePoint but leave it un-configured when performing an entire farm restore; the entire farm restore will configure your SharePoint farm during the restore process.
3. Install DocAve Manager according to the steps listed in the DocAve 6 Installation Guide.

   ***Note:** The imported platform full backup data of the entire SharePoint 2010 farm are supported to perform the Farm Rebuild only when the imported data are backed up by Platform Backup and Restore of DocAve 6 SP1 or later version.

   The imported platform full backup data of the entire SharePoint 2013 farm are supported to perform the Farm Rebuild only when the imported data are backed up by Platform Backup and Restore of DocAve 6 SP3 or later version.

   ***Note**: DocAve recommends not installing DocAve Manager on the SharePoint server. When disconnecting SharePoint farm, SharePoint will automatically restart the IIS site which will lead to the fact that the DocAve IIS site will be restarted as well. Install DocAve Agents according to the steps listed in the DocAve 6 Installation Guide.
4. Perform a Farm Rebuild.

About Farm Rebuild

The Farm Rebuild feature rebuilds a farm in the event of a farm crash or serious issues in a SharePoint farm that require you to reconfigure the farm. If a farm is corrupted, Farm Rebuild enables you to fully rebuild the farm to a previous time by preparing the environment and installing SharePoint with no further manual configurations needed beyond the Farm Rebuild wizard.

When critical issues occur in the SharePoint farm environment, DocAve will likely also have critical issues. Therefore, AvePoint strongly recommends you protect the DocAve Control database in the daily usage (for example, backing up the Control Database using SQL Server backup method), in case DocAve fails to recover and the Farm Rebuild cannot be used to recover your farm environment.

Farm Rebuild function in DocAve 6 is seamlessly integrated and intelligent. Many operations are integrated into the interface or into a single button; such as, disconnecting the original farm or stopping the SharePoint service. In addition, if the backup job used to perform Farm Rebuild contains VM backup data, you can choose to rebuild the farm using the VM backup data or only rebuilding the farm with backed up SharePoint data. AvePoint recommends using the VM backup data to restore SharePoint server, which will ensure that the third-party software integrated with your SharePoint farm work properly after the Farm Rebuild.

Supported Farm Topology

Refer to the information below for details on the supported farm topology for performing a Farm Rebuild.

Environment Configuration

Refer to the section below for the supported environment configurations for the Farm Rebuild feature:

- **Operating System**:
    - Windows Server 2008 R2
    - Windows Server 2008 R2 SP1
    - Windows Server 2008 R2 SP1 Server Core
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2012 R2 SP1
    - Windows Server 2012 R2 SP1 Server Core
    - Windows Server 2016
- **Web Application**: HTTP/HTTPS, FBA Authentication, User-Defined Host Header

***Note**: After the Farm Rebuild, the FBA database used by the Web applications in FBA authentication must be manually restored again using an **In place restore** with the **Conflict Resolution** of **Overwrite**.

- **User Account**: Domain User

***Note**: Farm Rebuild supports rebuilding your SharePoint farms whose SharePoint servers and SQL servers are all on Azure VMs.

Required Permissions

To use the Farm Rebuild properly, ensure that the Agent account has been granted the required permissions. For details, refer to Required Permissions.

Farm Topologies Supported by Farm Rebuild

Refer to the following two topologies to view an example of a simple/small SharePoint environment versus a complex environment.

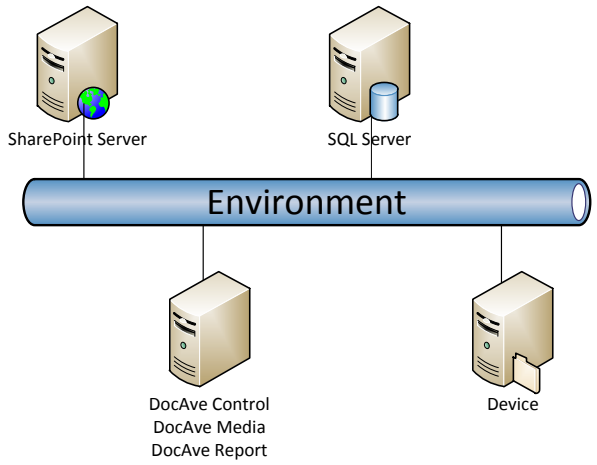


Figure 13: Simple and small topology of a SQL server and SharePoint server.

***Note**: Farm Rebuild supports SharePoint 2016 except SharePoint 2016 Single-Server Farm.

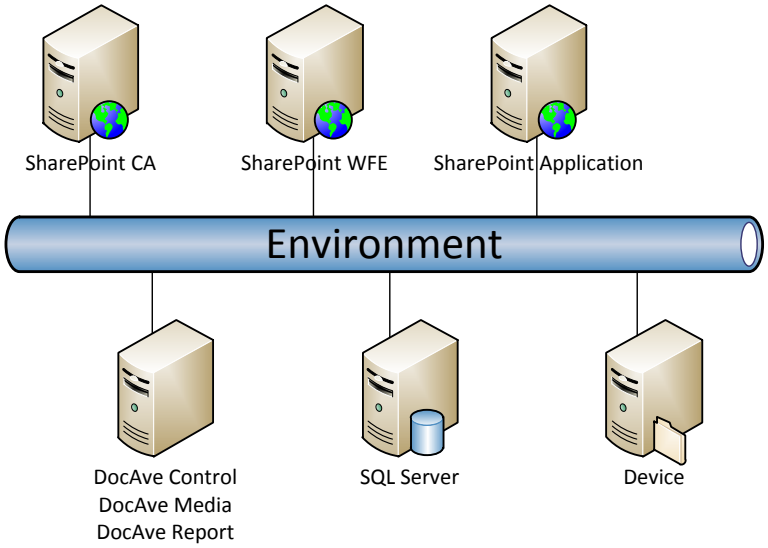


Figure 14: Complex topology of the SQL server, Central Administration, Web front-end server, and the application server.

***Note**: Farm Rebuild supports the SharePoint 2016 farm whose Central Administration website is secured with HTTPS using SSL.

***Note:** AvePoint recommends not installing the DocAve Manager on the SharePoint server. When disconnecting SharePoint farm, SharePoint will automatically restart the IIS site which will lead to the fact that the DocAve IIS site will be restarted as well.

***Note**: You must install the DocAve Agents on all of the servers (including SharePoint servers and SQL servers) in the farm rebuild environment.

Farm Rebuild Cases

When you perform the Farm Rebuild in your environment, refer to the following cases:

1. DocAve functions well, but the farm environment is crashed.
    - In this case, refer to the instructions in Performing a Farm Rebuild to rebuild your environment.
2. DocAve does not work, nor does the farm (for example, the Control database cannot be accessed, DocAve services cannot start, or users cannot save plans or run jobs).
    - In this case, the DocAve Control database required to have been backed up beforehand. Ensure that the data on the Media Server is intact.
    - If the servers in the farm are not crashed, they work well, and the end user is sure that the SharePoint environments on these servers can still work—the end user can restore DocAve by following the instructions on Performing a DocAve Disaster Recovery, and then perform the farm rebuild by using the former backup data. For details, refer to Performing a Farm Rebuild.

- If all of the servers in the farm are crashed, you are required to prepare a whole set of SharePoint environment where the configuration information of the machines is the same as that of the crashed environment, and then refer to the instructions in Performing a DocAve Disaster Recovery to restore DocAve. After the DocAve is restored, perform the farm rebuild. For details, refer to Performing a Farm Rebuild.

Considering the two cases, the Farm Rebuild function supports two restore methods, one is restoring to the original farm; the other is restoring to a new farm.

Restoring to the Original Farm

If the farm does not work or some servers in the farm have crashed, you can rebuild the original farm to the status in the full farm backup. The Farm Rebuild job will disconnect all of the servers from the original farm, and then rebuild the original farm.

1. Back up the whole farm. Refer to Backing Up the Original Farm.
2. Perform the DocAve disaster recovery. Refer to Performing a DocAve Disaster Recovery.
3. Perform the Farm Rebuild. Refer to Performing a Farm Rebuild.

Restoring to a New Farm

To restore to a new farm, you must first set up a new SharePoint environment, and make sure the following information is the same as that of the original farm:

- Machine name and Active Directory configuration
- SQL instance
- SharePoint version
- SQL Server version
- DocAve Manager

  ***Note**: To manage the new farm with the original DocAve Manager that is used to manage the original farm, choose one from the following methods:

  - Register the DocAve Agents in the new farm to the original DocAve Manager, or
  - Install a new DocAve Manager with the backed up Control database of the original DocAve Manager.

***Note**: The SharePoint server topology should be identical to the topology at the time of the full farm backup. The system platform must also match the platform at the time of backup. For example, use an x64 system if you used an x64 system at the time of the full farm backup. All related software to be installed on the rebuilt destination should be the same version and patch level as in the original farm. Examples of related software are: SharePoint, SQL Server, DocAve, and .NET Framework.

You are required to ensure that the DocAve Agent account permission in the new farm is the same as the original farm's Agent account; otherwise, you must make sure that the Agent account have sufficient permissions. Refer to Required Permissions for more information. Install a DocAve Agent on each of the SharePoint Servers and SQL Servers, and then follow the steps below:

1. Back up the farm. Refer to Backing Up the Original Farm.
2. Perform the DocAve Disaster Recovery. Refer to Performing a DocAve Disaster Recovery.
3. Perform the farm rebuild. Refer to Performing a Farm Rebuild.

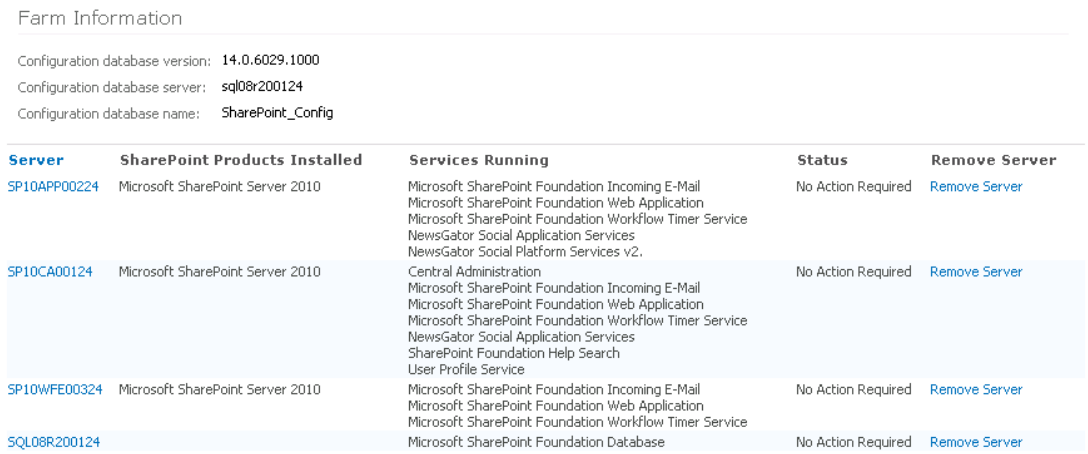
Backing Up the Original Farm

Refer to the section below for more information on your SharePoint farm configurations and how to back up your original farm using Platform Backup and Restore.

Original SharePoint 2010 Farm Environment's Configuration

Refer to the following information for the SharePoint 2010 farm environment, such as servers in the farm, service applications, Search Service Applications, databases, and BLOB data.

Servers in the Farm



Farm Information

Configuration database version: 14.0.6029.1000
Configuration database server: sql08r200124
Configuration database name: SharePoint_Config

Server	SharePoint Products Installed	Services Running	Status	Remove Server
SP10APP00224	Microsoft SharePoint Server 2010	Microsoft SharePoint Foundation Incoming E-Mail Microsoft SharePoint Foundation Web Application Microsoft SharePoint Foundation Workflow Timer Service NewsGator Social Application Services NewsGator Social Platform Services v2.	No Action Required	Remove Server
SP10CA00124	Microsoft SharePoint Server 2010	Central Administration Microsoft SharePoint Foundation Incoming E-Mail Microsoft SharePoint Foundation Web Application Microsoft SharePoint Foundation Workflow Timer Service NewsGator Social Application Services SharePoint Foundation Help Search User Profile Service	No Action Required	Remove Server
SP10WFE00324	Microsoft SharePoint Server 2010	Microsoft SharePoint Foundation Incoming E-Mail Microsoft SharePoint Foundation Web Application Microsoft SharePoint Foundation Workflow Timer Service	No Action Required	Remove Server
SQL08R200124		Microsoft SharePoint Foundation Database	No Action Required	Remove Server

Figure 15: Servers in the SharePoint 2010 farm.

Service Applications in the Farm

Name	Type	Status
Access Services	Access Services Web Service Application	Started
Access Services	Access Services Web Service Application Proxy	Started
Application Discovery and Load Balancer Service Application	Application Discovery and Load Balancer Service Application	Started
Application Discovery and Load Balancer Service Application Proxy_2c4fe7b2-7b53-4913-8d1d-7d80c59aad66	Application Discovery and Load Balancer Service Application Proxy	Started
Application Registry Service	Application Registry Service	Started
Application Registry Service	Application Registry Proxy	Started
Business Data Connectivity Service	Business Data Connectivity Service Application	Started
Business Data Connectivity Service	Business Data Connectivity Service Application Proxy	Started
Excel Services Application	Excel Services Application Web Service Application	Started
Excel Services Application	Excel Services Application Web Service Application Proxy	Started
Managed Metadata Service	Managed Metadata Service	Started
Managed Metadata Service	Managed Metadata Service Connection	Started
NewsGator Social Platform Services	NewsGator Social Platform Services	Started
NewsGator Social Platform Services Proxy	Social Service Application Proxy	Started
PerformancePoint Service Application	PerformancePoint Service Application	Started
PerformancePoint Service Application	PerformancePoint Service Application Proxy	Started
Search Administration Web Service for Search Service Application	Search Administration Web Service Application	Started

Figure 16: Service applications in the SharePoint 2010 farm.

Search Service Application	Search Service Application	Started
Search Service Application	Search Service Application Proxy	Started
Secure Store Service	Secure Store Service Application	Started
Secure Store Service	Secure Store Service Application Proxy	Started
Security Token Service Application	Security Token Service Application	Started
State Service	State Service	Started
State Service	State Service Proxy	Started
UPSA	User Profile Service Application	Started
UPSA	User Profile Service Application Proxy	Started
Usage and Health data collection	Usage and Health Data Collection Service Application	Started
Usage and Health data collection	Usage and Health Data Collection Proxy	Started
Visio Graphics Service	Visio Graphics Service Application	Started
Visio Graphics Service	Visio Graphics Service Application Proxy	Started
Web Analytics Service Application	Web Analytics Service Application	Started
Web Analytics Service Application	Web Analytics Service Application Proxy	Started
Word Automation Services	Word Automation Services	Started
Word Automation Services	Word Automation Services Proxy	Started

Figure 17: Service applications in the SharePoint 2010 farm.

Search Service Application in the Farm

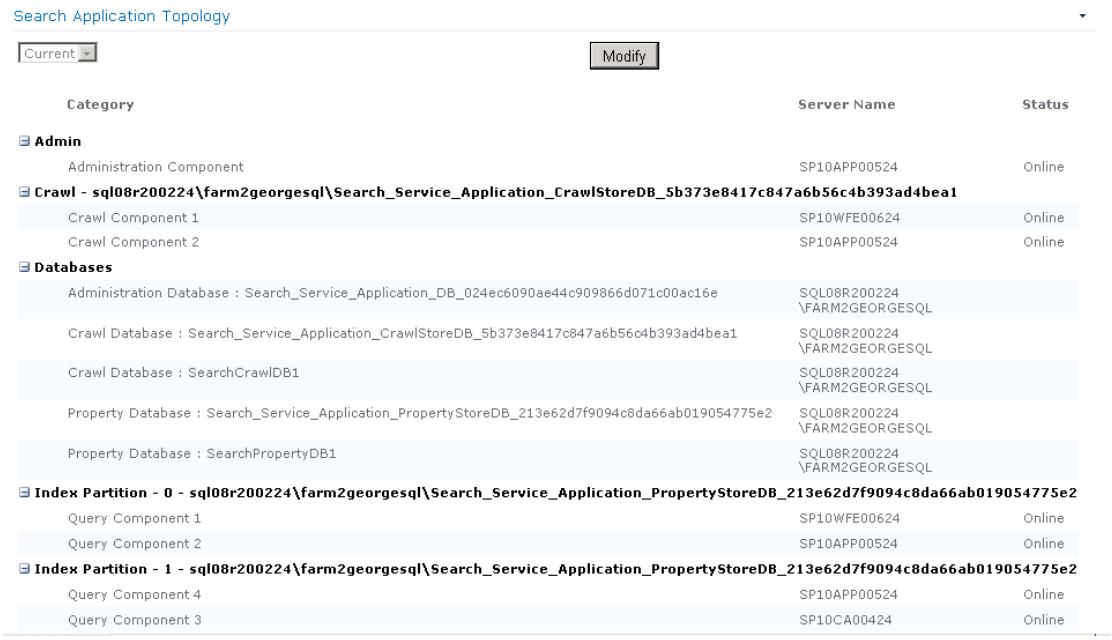


Figure 18: Search Service Application topology in the SharePoint 2010 farm.

Databases in the Farm

Figure 19: Databases in the SharePoint 2010 farm.

BLOB Data in the Farm

Starting with DocAve 6 SP1, Platform Backup and Restore supports the backup and restore of BLOB data. As of the DocAve 6 SP4 release, Farm Rebuild feature now can perform the BLOB data restoration in the Farm Rebuild wizard.

***Note**: The BLOB data in NFS storage cannot be backed up or restored using Platform Backup and Restore.

If your SharePoint farm contains BLOB data, make sure you select the **Back up stub database** option, the **Back up Storage Manager BLOB** option, and the **Back up Connector BLOB** option on the **Run Now** interface when you are about to back up the entire farm.

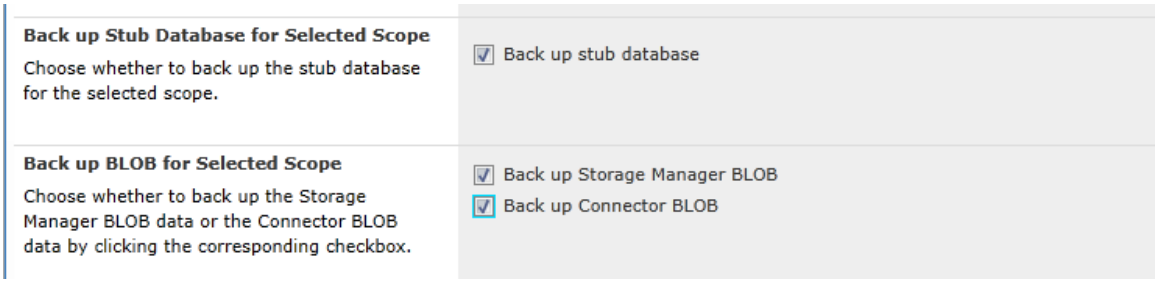


Figure 20: Select to back up the stub database, and the Storage Manager and Connector BLOB data.

***Note**: The BLOB data backup information will be recorded in the **BLOB Details** tab of the backup job details.

Original SharePoint 2013 Farm Environment's Configuration

Refer to the following information for the SharePoint 2013 farm environment, such as servers in the farm, corresponding service applications, Search Service Applications, databases, and BLOB data.

Servers in the Farm

Servers in Farm

Farm Information

Configuration database version: 15.0.4420.1017
Configuration database server: SQL12001CS
Configuration database name: SharePoint_Config

Server	SharePoint Products Installed	Services Running	Status	Remove Server
SP13APP003CS	Microsoft SharePoint Server 2013	Access Database Service 2010 Access Services App Management Service Business Data Connectivity Service Distributed Cache Excel Calculation Services Machine Translation Service Managed Metadata Web Service Microsoft SharePoint Foundation Incoming E-Mail Microsoft SharePoint Foundation Web Application Microsoft SharePoint Foundation Workflow Timer Service PerformancePoint Service PowerPoint Conversion Service Search Query and Site Settings Service Secure Store Service User Profile Service Visio Graphics Service Word Automation Services Work Management Service	No Action Required	Remove Server
SP13CA001CS	Microsoft SharePoint Server 2013	Access Database Service 2010 Access Services App Management Service Business Data Connectivity Service Central Administration Distributed Cache Excel Calculation Services Machine Translation Service Managed Metadata Web Service Microsoft SharePoint Foundation Incoming E-Mail Microsoft SharePoint Foundation Web Application Microsoft SharePoint Foundation Workflow Timer Service PerformancePoint Service PowerPoint Conversion Service Search Host Controller Service Search Query and Site Settings Service Secure Store Service SharePoint Server Search User Profile Service Visio Graphics Service Word Automation Services Work Management Service	No Action Required	Remove Server
SP13WEB002CS	Microsoft SharePoint Server 2013	Access Database Service 2010 Access Services App Management Service Business Data Connectivity Service Distributed Cache Excel Calculation Services Machine Translation Service Managed Metadata Web Service Microsoft SharePoint Foundation Incoming E-Mail Microsoft SharePoint Foundation Web Application Microsoft SharePoint Foundation Workflow Timer Service PerformancePoint Service PowerPoint Conversion Service Search Query and Site Settings Service Secure Store Service User Profile Service Visio Graphics Service Word Automation Services Work Management Service	No Action Required	Remove Server
SQL12001CS		Microsoft SharePoint Foundation Database	No Action Required	Remove Server

Figure 21: Servers in the SharePoint 2013 farm.

Service Applications in the Farm

Name	Type	Status
Access Services 2010	Access Services 2010 Web Service Application	Started
Access Services 2010	Access Services 2010 Web Service Application Proxy	Started
Access Services	Access Services Web Service Application	Started
Access Services	Access Services Web Service Application Proxy	Started
App Management Service	App Management Service Application	Started
App Management Service	App Management Service Application Proxy	Started
Application Discovery and Load Balancer Service Application	Application Discovery and Load Balancer Service Application	Started
Application Discovery and Load Balancer Service Application Proxy_6ed33220-343c-4aeb-9701-955694a89a0c	Application Discovery and Load Balancer Service Application Proxy	Started
Business Data Connectivity Service	Business Data Connectivity Service Application	Started
Business Data Connectivity Service	Business Data Connectivity Service Application Proxy	Started
Excel Services Application	Excel Services Application Web Service Application	Started
Excel Services Application	Excel Services Application Web Service Application Proxy	Started
Machine Translation Service	Machine Translation Service	Started
Machine Translation Service	Machine Translation Service Proxy	Started
Managed Metadata Service	Managed Metadata Service	Started
Managed Metadata Service	Managed Metadata Service Connection	Started
PerformancePoint Service Application	PerformancePoint Service Application	Started
PerformancePoint Service Application	PerformancePoint Service Application Proxy	Started
PowerPoint Conversion Service Application	PowerPoint Conversion Service Application	Started
PowerPoint Conversion Service Application	PowerPoint Conversion Service Application Proxy	Started

Figure 22: Service applications in the SharePoint 2013 farm.

Search Administration Web Service for Search Service Application	Search Administration Web Service Application	Started
Search Service Application	Search Service Application	Started
Search Service Application	Search Service Application Proxy	Started
Secure Store Service	Secure Store Service Application	Started
Secure Store Service	Secure Store Service Application Proxy	Started
Security Token Service Application	Security Token Service Application	Started
State Service	State Service	Started
State Service	State Service Proxy	Started
UPS1206	User Profile Service Application	Started
UPS1206	User Profile Service Application Proxy	Started
Visio Graphics Service	Visio Graphics Service Application	Started
Visio Graphics Service	Visio Graphics Service Application Proxy	Started
Word Automation Services	Word Automation Services	Started
Word Automation Services	Word Automation Services Proxy	Started
Work Management Service Application	Work Management Service Application	Started
Work Management Service Application	Work Management Service Application Proxy	Started
Workflow Service Application	Workflow Service Application	Started
Workflow Service Application Proxy	Workflow Service Application Proxy	Started

Figure 23: Service applications in the SharePoint 2013 farm.

Search Service Application in the Farm

Search Application Topology

Server Name	Admin	Crawler	Content Processing	Analytics Processing	Query Processing	Index Partition 0
SP13CA001CS	✓	✓	✓	✓	✓	✓

Database Server Name	Database Type	Database Name
SQL12001CS	Administration Database	Search_Service_Application_DB_aa1d94b823a44516aac790fe95111780
SQL12001CS	Analytics Reporting Database	Search_Service_Application_AnalyticsReportingStoreDB_ed5c91dfcf164c118556941d50759eb2
SQL12001CS	Crawl Database	Search_Service_Application_CrawlStoreDB_c40f4a8055c94a6ab7e59a2d55543cc2
SQL12001CS	Link Database	Search_Service_Application_LinksStoreDB_e7cf7cbe7aed423593f52e826c24b84b

Figure 24: Search Service Application topology in the SharePoint 2013 farm.

Databases in the Farm

Figure 25: Databases in the SharePoint 2013 farm.

BLOB Data in the Farm

Starting with DocAve 6 SP1, Platform Backup and Restore supports the backup and restore of BLOB data. Farm Rebuild feature now can perform the BLOB data restoration in the Farm Rebuild wizard starting from DocAve 6 SP4.

***Note**: The BLOB data in NFS storage cannot be backed up or restored using Platform Backup and Restore.

If your SharePoint farm contains BLOB data, make sure you select the **Back up stub database** option, the **Back up Storage Manager BLOB** option, and the **Back up Connector BLOB** option on the **Run Now**

interface when you are about to back up the entire farm.

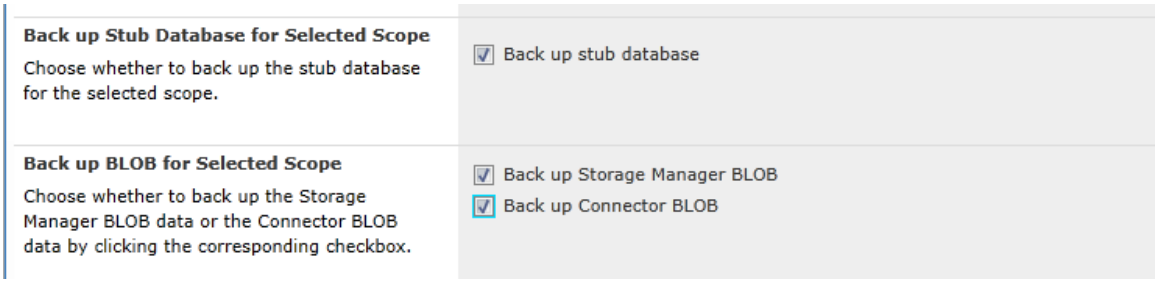


Figure 26: Select to back up the stub database, and the Storage Manager and Connector BLOB data.

***Note**: The BLOB data backup information will be recorded in the **BLOB Details** tab of the backup job details.

Backing Up the Original Farm Using Platform Backup

To back up the original farm, create a new Platform Backup plan. Complete the steps below:

1. Log into DocAve and navigate to **Data Protection** > **Platform Backup & Restore** > **Platform Backup**.
2. Click **Plan Builder** > **Form Mode** on the ribbon and create a new plan.
3. In the left pane, select the farm you are about to back up from the drop-down list, and select the desired backup scope from the **Backup Component Selection** for this backup plan. Click the farm name to load the tree and select the farm node to perform the backup.

   ***Note:** The **Web Front-End Servers** nodes on the backup tree will be selected by default and cannot be unchecked when you back up the whole farm. However, the Web front-end data will not be restored with other components when performing the Farm Rebuild. If the files on the Web front-end Servers have been configured, or some customized features have been updated, we recommend that you back up the Web front-end Servers nodes together with other components in the SharePoint farm. Therefore, the files and features on the Web front-end Servers can be restored to the status when backing up. Otherwise, the modifications on the files and the configurations of the Servers will be lost.

   ***Note:** The Data Source database of the **Business Data Connectivity Service Application** and the custom database of the **PerformancePoint Service Application** must be added to the backup tree as the custom databases.

4. Configure the plan settings, save and run the plan. For more detailed information, refer to Using Form Mode to Create a Backup Plan.

Performing a DocAve Disaster Recovery

DocAve 5 has the System Recovery feature to help you perform DocAve Disaster Recovery. This feature does not exist in DocAve 6.

Although the System Recovery feature is not supported in DocAve 6, you can still achieve Disaster Recovery by establishing a new DocAve environment, and then connecting to the former DocAve Control Database. You must protect the DocAve Control database during the daily usage, for example, backing up the database by using SQL Backup or another third party backup method.

If the DocAve is crashed, but the DocAve Control database can function well, follow the instructions below to perform the DocAve Disaster Recovery:

1. Prepare the Web front-end servers and SQL Servers used for the DocAve Disaster Recovery.
2. Restore or attach the backed up DocAve Control database to the SQL Server.
3. Install DocAve Manager using the SQL installation method and connect to the DocAve Control database. Then install the DocAve Agents on the Web front-end servers and SQL Servers.

This completes the DocAve Disaster Recovery. If the users' data is not damaged, you can select the backup data from the backup data tree in the **Restore** wizard/**Farm Rebuild** wizard to restore the desired data.

Performing a Farm Rebuild

Follow the instructions below to perform a Farm Rebuild step by step:

***Note:** Farm Rebuild will take some time to complete, so please do not close the browser when executing the Farm Rebuild. If the Farm Rebuild process is stopped before it completes, you will have to go through the Farm Rebuild wizard from the beginning because DocAve will not record what you did for the last minute.

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

   ***Note:** In the **Farm Rebuild** tab, only the backup jobs that have successfully backed up the SharePoint Configuration database and administration database can be displayed and filtered in the calendar view for performing Farm Rebuild.

2. **Filter By** – Limit the scope of backup data restored by filtering out desired full farm backup jobs.
   - **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 selected restore granularity levels are displayed. Select **All Types** to list the backup jobs of all levels.

- **Filter by Job** – Limit the full farm backup jobs by job type using this drop-down list.
    - **Backup Type** – Select the backup type from the drop-down list; only the backup jobs of the selected types are displayed. Select **All Types** to list the backup jobs of all three types.
- **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/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 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 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 qualified Platform backup jobs. Place the mouse cursor over the 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**, **Data Transfer Status**, **Verification 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. Select the backup job that you want to use to perform the Farm Rebuild.
4. Click **Next**. One of two wizards will appear, depending on the selected backup job.
    - If the selected backup job did not back up VM data, the **View** interface will appear. For details on rebuilding farm using SharePoint farm backup data, refer to Using SharePoint Farm Backup Data for Farm Rebuild.
    - If the selected backup job contains VM backup data, a window will appear informing you that the VM backup data is detected in the backup job, which is backed up by **Platform Backup** or **a third-party tool**. Additionally, you must choose which method you want to use to restore SharePoint servers.
        - **VM backup data** – Uses VM backup data to restore the SharePoint server and the backed up SharePoint components. This method will ensure the third-party software integrated with your SharePoint farm will work properly after the Farm Rebuild. For details on using VM backup data to rebuild the farm, refer to Using VM Backup Data for Farm Rebuild.
        - **SharePoint farm backup data** – This method will only restore the SharePoint farm backup data without the backed up VM data. For details on rebuilding the farm with SharePoint farm backup data, refer to Using SharePoint Farm Backup Data for Farm Rebuild.

Using VM Backup Data for Farm Rebuild

Complete the steps below to continue the Farm Rebuild using VM backup data:

1. **View** – In the **Farm Components** tab, all of the farm components are displayed in the tree. The backed up components are selected and cannot be deselected. In the **Farm Servers** tab, all of the backed up VMs are displayed and grouped by the VM host.

   ***Note:** Farm Rebuild does not support restoring custom VMs that are in the VM backup data.

   ***Note**: When restoring ESX/ESXi VMs in vCenter host cluster, ensure to the following conditions are met:

   - If the original host in the cluster is not available and there is another host with all of the datastores used by the VM, the VM will be restored to this host in the cluster.
   - If the vCenter host cluster has configured the VM-Host Affinity rules between VM DRS (Distributed Resource Scheduler) group and host DRS group, DocAve uses the names of the VM DRS group to check if the VM DRS group where the backed up VM resides still exists. If the VM DRS group still exists, the VM will be restored to this VM DRS group and the rule will take effect on the restored VM. If the VM DRS group does not exist, skip restoring the VM to the VM DRS group and the rule will not take effect on the restored VM.

   ***Note**: When restoring ESX/ESXi VMs stored by the datastores that are in vCenter datastore cluster, consider the following:

   - DocAve does not support backing up and restoring the VMs with the same name and stored in the same datastore cluster.
   - Support restoring datastore rules of **VMDK anti-affinity** and **VMDK affinity** for virtual disks; does not support restoring datastore rules of **VM anti-affinity** or **VM affinity** for VMs.

2. Click **Next**. The **VM Restore Settings** page appears.

   - If the VM backup data is backed up by Platform Backup, follow the instructions below:

     i. **VM Configuration** – Select an Agent for each VM to execute the restore job. By default, the Agent in the host profile used by the backup plan is selected. The VMs hosted by Hyper-V will use the Agent that performed backup job to execute the restore. If the VM is hosted on Hyper-V Cluster, the selected Agent must be on the node in the cluster.

     ii. **VM Conflict Resolution** – Define the VM conflict resolution behavior. For ESX/ESXi or vCenter hosted VMs, if a **.vmx** configuration file in the target resides in the same location as the **.vmx** configuration file in the backup, it is considered as a conflict. For the VMs stored in the datastores that are in a vCenter datastore cluster, if there is a VM whose name is the same as the backed up VM

in the datastore cluster, it is considered as a conflict. For Hyper-V hosted VMs, if a VM ID same as the one in the backup already exists in the destination, it is considered as a conflict.

- **Skip** – Do not restore the source conflicting VM, and keep the destination VM intact.
- **Replace Virtual Disk Only** – Delete the data in the virtual disks of the target conflicting VM and then restore the data in the virtual disks of the backed up VM to the destination VM, without the VM configurations.

  ***Note: Replace Virtual Disk Only** is invalid for the VMs managed by the Hyper-V host. If you set the VM conflict resolution to Replace Virtual Disk Only when restoring VM on Hyper-V host, the conflicting VM will be removed, and the backup data of the VM will be restored.

- **Overwrite** – Deletes the conflicting VM in the destination and restore the backed up VM.

iii. **Hyper-V Parent Disk Conflict Resolution** – Define the Hyper-V parent disk conflict resolution behavior. If the Hyper-V parent disk in the source is with the same full path as an existing Hyper-V parent disk in the target, it is considered a conflict. This option is only functional for the restore of VMs hosted by Hyper-V. Note that if the restore of the Hyper-V hosted VM in the backup is skipped, the Hyper-V parent disk will not be restore, regardless of the selected **Hyper-V Parent Disk Conflict Resolution**.

- **Skip** – Do not restore the source conflicting Hyper-V parent disk.
- **Overwrite** – Delete the target Hyper-V parent disk, and restore the backed up parent disk.

- If the VM backup data is backed up by a third-party tool, select a predefined VM script profile from the drop-down list to perform the VM restore, or create a new VM script profile by selecting the **New VM Script Profile** link from the drop-down list.

  ***Note**: AvePoint strongly recommends not placing the script in SharePoint server that is going to be restored in this Farm Rebuild.

3. Click **Next**. The **Restore Settings** page appears.
4. **Restore BLOB** – Choose whether or not to restore BLOB data.

   ***Note**: This field only appears when the backed up farm has BLOB backup data.

5. **Agent Selection** – Select an Agent from the drop-down list to execute the job. The selected Agent must be able to communicate with the working Agent.
6. **Database Conflict Resolution** – Select whether or not to overwrite the database in the target farm if a conflict event occurs.

- **Skip** – If a database in the backup has the same name as a database in the target farm, the database in the backup is not restored.

  ***Note**: SharePoint configuration database in the backup will always be restored to the destination, regardless of the selected conflict resolution.

- **Overwrite** – If a database in the backup has the same name as a database in the target farm, the database in the target farm is deleted first and the database in the backup is then restored.

7. **Job Report** – Select the level of reporting for this job. **Simplified** will create a summary of content restored to SharePoint. **Detailed** will create a full list of all objects restored to SharePoint at the cost of performance. If there is any BLOB data selected, the **BLOB Details** tab will show in the **Job Details** and display the detailed information for this data as well.

   ***Note**: This field only appears when **Restore BLOB** option is selected.

8. **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.
9. Click **Next**. The **Schedule** page appears. Choose whether or not to create the farm rebuild with VM job based on a schedule. Select **Restore immediately after wizard finishes** to run the job immediately after finishing the farm rebuild with VM wizard. To configure the schedule yourself, select **Configure the schedule myself** and input a start time in **Schedule Settings** field. Enter an optional **Description** to distinguish the restore job from others.
10. When finished, click **Next**. The **Overview** page appears.
11. Click **Next**. The **Overview** page appears. View the settings you have configured. If you want to modify the settings on specific step, click **Edit** beside that step to go to that page and make changes.
12. Click **Finish** to run the Farm Rebuild.

Using SharePoint Farm Backup Data for Farm Rebuild

Generally speaking, the Farm Rebuild using SharePoint farm backup data 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 backed up databases, mainly the following databases:
   - SharePoint Configuration database
   - Content database of the SharePoint Central Administration
   - Service applications' databases
   - Content database

- Stub database

4. Connecting the Farm – Connect the Servers to the target farm with mainly 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.)

Follow the instructions below to perform a Farm Rebuild step by step:

1. **View** – View all the backed up SharePoint components in the full farm backup job.

    ***Note:** The selection on the tree is disabled and cannot be edited. The **Web Front-End Servers** node and **Custom Database** node are deselected.

2. **Options** – Select whether or not to restore BLOB data.
    - **Restore BLOB** – Select whether or not to restore the BLOB data.
    - **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.

    ***Note:** AvePoint recommends selecting a profile for e-mail notification. The **Disconnect Connection**, **Restore BLOB**, **Restore Database**, **Connect**, **Restore Index** action may take some time, and when each action is finished, DocAve will send you an e-mail to notify you when to execute the next step of farm rebuild job. Otherwise the farm rebuild job may fail.

3. Select **Next**; a pop-up message appears informing you of which services will be restarted. After you select **OK**, the **Disconnect Connection** page will obtain server information from the farm where you want to perform the Farm Rebuild. Select **Cancel** to return to the **Restore** page.
4. **Disconnect Connection** – Disconnect all the SharePoint servers in this farm. All the SharePoint servers which have been 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.

    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 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.

5. **Restore BLOB** – Restore the BLOB data in the farm. It is recommended that you restore all of the BLOB data listed in the table. Configure the Restore Settings to choose whether or not to overwrite the BLOB data in the event that a conflict occurs during a restore.
6. **Restore Database** – Restore all the backed up databases in the full farm backup job. Choose to restore from the Platform Backup data or restore from the third-party backup data. If you choose to restore from third-party backup data, you must restore the database files to the correct location manually, and click **Verify** to verify the backup data of the databases in the target.

   If restoring from Platform Backup data, the databases are all restored with no attempt to connect them to the SharePoint environment according to the selected conflict resolution.

   ***Note**: If the database restoration failed in the scenario that your SQL Server is installed on the SharePoint Server and the logon user of SQL Writer is the same as the logon user of Search Service or Help Search Service, complete the following steps to solve this issue:

   - Go to the **HKEY_LOCAL_MACHINE**>**SYSTEM**>**CurrentControlSet**>**Services**>**VSS**>**VssAccessControl** registry.
   - Right-click **VssAccessControl**, select **New** from the drop-down list, and then select **DWORD Value** type from the drop-down list. Rename it to the domain username of the SQL Writer logon user, and then right-click. Select **Modify** from the drop-down list, and set the **Value data** to **1**. Click **OK**.
   - Restart the **Volume Shadow Copy** service.

   ***Note:** If you want to restore the SQL Server logins when restoring the backed up database, enable the **RestoreLoginsConfig RestoreLogins** parameter in the **SP2010PlatformConfiguration.xml** file (the file is located in the DocAve Agent installation path: …*AvePoint**DocAve6**Agent**data**SP2010**Platform* by default) by setting its value to **True** (the default value is **False**, so by default, the SQL Server logins will not be restored when performing the restore job). It is recommended for you to use the database role of **Sysadmin** to the SQL Server to restore the SQL Server logins, in case any logins in a high-level role cannot be restored.

   - **Conflict Resolution** – Select 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.

***Note**: If you use a full SharePoint 2013 farm backup job data to perform Farm Rebuild twice and you select the **Skip** as the conflict resolution for the database restore at the second Farm Rebuild job, the index restore will fail and the Search Service Application cannot properly work. However, if you select **Overwrite** as the conflict resolution for database restore at the second Farm Rebuild job, the job will succeed. To resolve this failure issue, perform a restore job at database level to restore the backed up Search Service Application again.

7. Select **Restore** to begin the restore process. After the restore of all the databases is finished, the restore status will be updated in the **Status** column and the checkboxes before all the databases will become selectable. When the restore of a specified database is failed, only select this database, configure the restore setting and perform the restore job again.

   ***Note:** Make sure that the SharePoint Configuration database and the Central Administration's Content database have been successfully restored before you go to the next step.

8. **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.
   - **Specify Port Number** – Select the checkbox and you can change the port used by the SharePoint 2010/2013 Central Administration.
   - **Configure Security Settings** – Select a security authentication type for this farm to use after rebuilding. Platform Backup and Restore supports the two following security authentication types: **NTLM** and **Negotiate (Kerberos)**.
   - **Update Settings** – If you are rebuilding farm to a later version, choose whether or not to update SharePoint automatically after connecting servers to the target farm or you will update it later manually.

   Click **Validation Test** to verify the settings you have inputted.

9. **Connect** – Secure the connections of all the SharePoint servers back to this farm. All the SharePoint servers, which have been disconnected from the current farm in Step 4, will be displayed here.

   - **Manage columns** (⊞) – Manage which columns are displayed in the list. 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.

Click **Connect** to connect the connections of all the displayed SharePoint servers back to this farm.

***Note:** The connection process follows a certain sequence. At first, the SharePoint Central Administration server will be connected to the farm, and then the other Web front-end servers will be connected to the farm. If some servers fail to connect to the target farm in this step, you can try to connect them again by selecting **Connect**.

10. Click **Next**. The **Restore Index** page appears. DocAve restores the backed up index components to the target farm.
11. **Restore Index** – Restore all of the index components of the search service applications backed up in the whole farm backup job. If the Search Service Application is not included in the backup, the **Restore Index** step will be skipped. Choose to restore the index components from the Platform Backup data or restore from the third-party backup data.

    ***Note**: If you choose to restore from third-party backup data, you must restore the index components to the correct location manually, and click **Verify** to verify the backup data of the index components in the target.

    The details about restoring the index components are listed in the table. Select a desired number from the **Show rows** drop-down menu to enter the number of index components displayed per page. Select **<** or **>** to turn to the previous or next page. Select **Restore** to restore the selected index components again. Once the restore process is finished, the restore status of each index component will be updated in the **Status** column.

    ***Note**: If some of the Search Service Application index components fail 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. The index components can work well in the SharePoint farm after the restoration.

12. **Overview** – View the current farm settings you have configured in Step 6.
13. Click **Finish** to finish the farm rebuild.

    ***Note:** After the Farm Rebuild is finished, restart the DocAve Agent service in order to obtain the most up to date information of the target farm as soon as possible.

Restoring Other Farm Components

Some of the farm components will not be restored during the Farm Rebuild. After you have finished the Farm Rebuild wizard, there may be several components that are not functional, such as the InfoPath Form Services, SharePoint Foundation Help Search, and FBA database. To make them functional, you must manually restore these components using an **In place restore** with the **Conflict Resolution** of **Overwrite**.

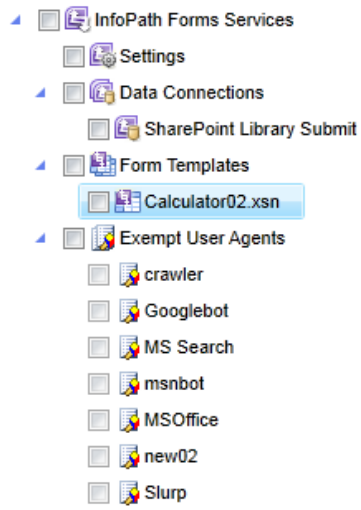


Figure 27: InfoPath Form Services' components.

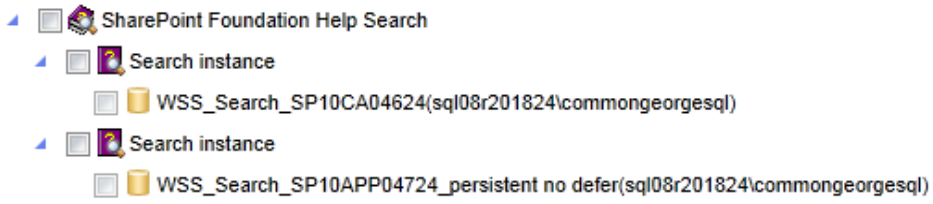


Figure 28: SharePoint Foundation Help Search components.

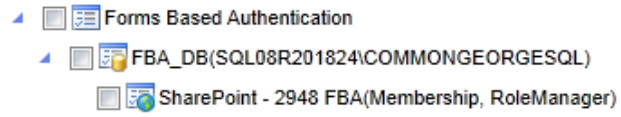


Figure 29: Forms Based Authentication components.

Search Service Application

After the Farm Rebuild, if the Search Service Application cannot be used normally, you must manually restore the specified Search Service Application again. If you want to delete the original Search Service Applications before the restore, follow the instructions below to delete the specified Search Service Applications.

There are two methods of deleting the Search Service Applications, which are provided below: the first, method is to delete the Search Service Applications through SharePoint Central Administration; the second, is to delete the Search Service Applications through the SharePoint Management Shell.

To delete the Search Service Applications through SharePoint Central Administration:

1. Navigate to **SharePoint Central Administration** > **Application Management** > **Manage service applications**.

2. Select the Search Service Application and select **Delete** on the ribbon to delete the selected Search Service Application.

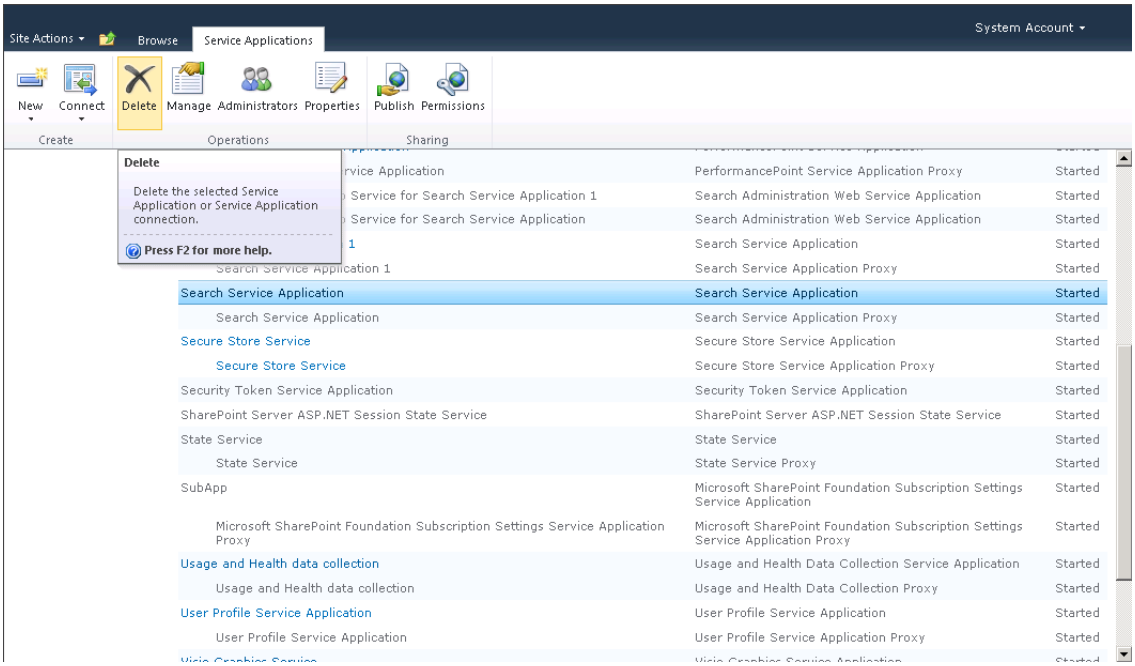


Figure 30: Deleting Search Service Application.

To delete the Search Service Applications through SharePoint Management Shell:

1. Navigate to **Start** > **Microsoft SharePoint 2010 Products** > **SharePoint 2010 Management Shell**. Right-click on the SharePoint Management Shell and then select Run as administrator.
2. Enter the following command to delete the specified Search Service Application:

   ```
   $a = Get-SPEnterpriseSearchServiceApplication -Identity SSAName

   Remove-SPEnterpriseSearchServiceApplication $a
   ```

   SSAName represents the name of the specified Search Service Application that you want to delete.

Web Front-End Components

If you want to restore the configured files or some customized features on the Web front-end servers, you must select the corresponding Web front-end servers' nodes from the backup date tree and then

perform an **In place restore** to restore the data with the **Conflict Resolution** of **Overwrite** after the Farm Rebuild.

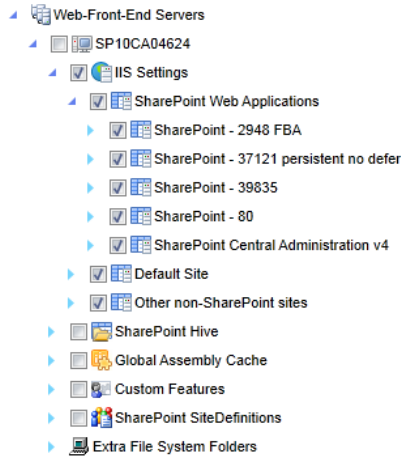


Figure 31: Restoring Web front-end components.

Supported and Unsupported List of Farm Rebuild for SharePoint 2010 Farm

For more detailed information on the supported and unsupported information of Farm Rebuild for SharePoint 2010 farm, refer to the corresponding sections below.

Supported Backup Methods for Farm Rebuild

Backup Method	Supported or Not
VSS	Supported

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	Not Supported
InfoPath Forms Services	Not Supported
FBA Databases	Supported
Solutions	Supported
FAST Search Server	Not Supported

Features	Supported or Not
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
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 Backup Methods for Farm Rebuild

Backup Method	Supported or Not
VSS	Supported

Supported and Unsupported Farm Features for Farm Rebuild

Features	Supported or Not
Configuration Database	Supported
SharePoint Web Service	Supported

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

Helpful Notes When Performing the Farm Rebuild

1. Platform backup jobs do not support to back up the SSL certificate of HTTPS sites. If you want to use the HTTPS sites normally after the Farm Rebuild, you must manually export the SSL certificate from the original farm, and then import the exported SSL certificate to the target farm that is rebuilt. For more information about exporting and importing the SSL certificate, refer to http://technet.microsoft.com/en-us/library/cc731386(v=ws.10).aspx (for IIS 7), or http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/2cfeeba2-511f-47e8-913c-f196b74e6a44.mspx?mfr=true (for IIS 6).

2. If the DocAve Manager is installed on the SharePoint Server, the Farm Rebuild job will fail. When performing the Farm Rebuild, the PSConfig command will be used to disconnect and connect the SharePoint Servers to and/or from the specified farm, and the PSConfig command will perform the IIS Reset (executed inside the SharePoint APIs), which will cause the interruption of the communication between the DocAve Agents and DocAve Manager; consequently, the Farm Rebuild job fails.
3. After the Farm Rebuild job is finished, the Synchronization Connections are not displayed under its User Profile Service Application.

   Solution:

   If the User Profile Synchronization Service is started, manually restart the User Profile Synchronization Service; if the Synchronization Service is not started, manually start this feature. If the User Profile Service cannot be accessed, restart the User Profile Service and the Synchronization Service and then perform the IIS Reset. For SharePoint 2010, if your SharePoint server name is in FQDN (Fully Qualified Domain Name), while your environment machine name is not in FQDN, the Synchronization Connections cannot be restored.

4. If you performed the Farm Rebuild after the DocAve Disaster Recovery, a license expiration message is popped up for the Storage Optimization product suite.

   Solution:

   Restart the Agent service, and then select the corresponding Agent type in **Control Panel** > **Agent Monitor**.

5. If the Security Token Service Application's status is **Stopped** after the Farm Rebuild is finished, SharePoint Central Administration and other SharePoint sites are not functional.

   Follow the instructions below to resolve this issue:

   a. Navigate to **Start** > **Microsoft SharePoint 2010 Products** > **SharePoint 2010 Management Shell**. Right-click on the SharePoint 2010 Management Shell and then select **Run as administrator** to run the SharePoint 2010 Management Shell.

   b. Enter the command line of `$sts1=Get-SPSecurityTokenServiceConfig`, and then press **Enter**.

   c. Enter the command line of `$sts1.Provision()`, and then press **Enter**.

   d. Enter the command line of `$sts2=Get-SPServicehostConfig`, and then press **Enter**.

   e. Enter the command line of `$sts2.Provision()`, and then press **Enter**.

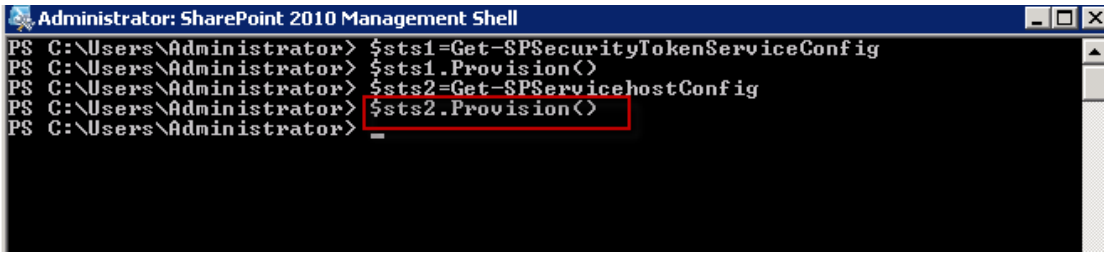


Figure 32: Using the $sts2.Provision() command.

f. Using the **IISReset** command to perform the IIS Reset.

6. Generally speaking, when performing the Farm Rebuild job, all of the service applications in the farm will be provisioned; however, if the SharePoint Timer Service of the target farm is stopped, the provision processing will fail, and some of the service applications may be not functional. In this case, you must manually provision the SharePoint service applications by using the **SharePoint 2010 Management Shell**.

7. After the Farm Rebuild job is finished, the service applications or the SharePoint sites may not be accessible. When you encounter this issue, grant all of the Application Pool users the **Public** role in the SQL Server.

8. When you perform the Farm Rebuild to restore the backed up farm to a new farm, the permission of the Agent account configured on the SQL Server must be the same as that of the original farm. For more information on the required permissions, refer to Required Permissions.

9. After the Farm Rebuild job, if you want to use the restored Secure Store Service, follow the instructions below:

   a. In the SharePoint Central Administration, select the **Manage service application** link and then select the specified Secure Store Service to go to the Secure Store Service's management interface.

   b. Select **Refresh Key** on the ribbon to refresh the key or select **Generate New Key** to create a new key.

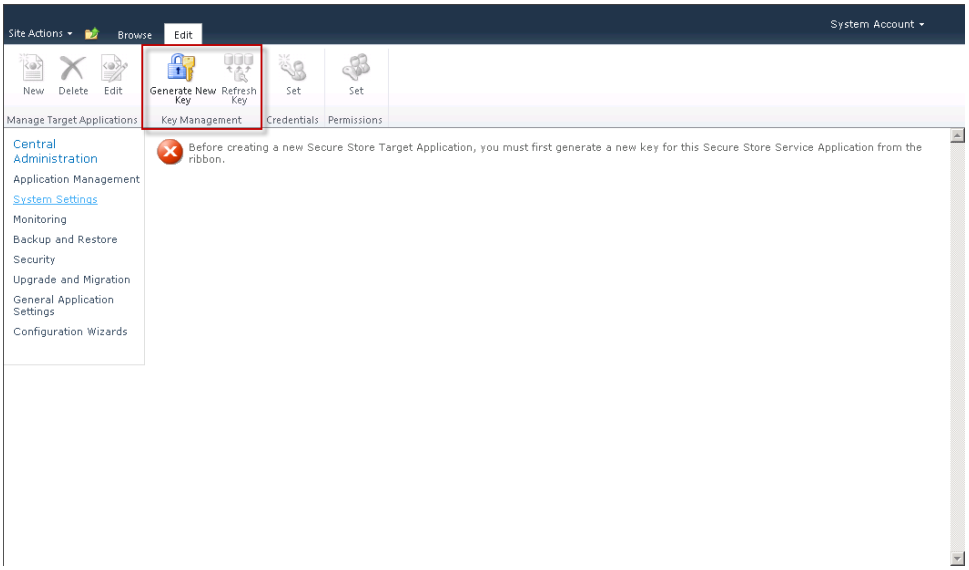


Figure 33: Generating new key.

10. If a Web application or site collection has deployed the custom features or solutions, its child sites may not be accessed after the farm rebuild.

    Solution:

    a. Manually restore the backed up IIS site under the corresponding Web front-end Server's node. For more detailed information, refer to Web Front-End Components.

    b. Manually restore the backed up Custom Web Parts.

    c. Restart the IIS Service.

11. The following error occurred while restoring the index components: The process cannot access the file 'INDEX.000' because it is being used by another process.

    Solution:

    For fear of this issue happening, make sure that the index files under the Crawl Component and Query Component in the target farm have been deleted before the Farm Rebuild.

12. After the Farm Rebuild job, navigate to **Central Administration** > **Manage Service Applications** > **Search Service Application**, then select **Manage** > **Content Source** to go to the Content Source's management page, the status of the content source is **Paused by System**.

Figure 34: The status of the content source.

Solution:

Run a new crawling job, and then the status will be correct.

13. If you have installed the Microsoft Forefront Protection 2010 for SharePoint and has configured the Filter Site, after the Farm Rebuild job is finished, the SharePoint Central Administration and other SharePoint sites may not be accessible. An Error message may prompt, saying **HTTP Error 500 – Internal Server Error**. In the Application Log, the error may be recorded as: **The HTTP Filter DLL C:\\Prgram Files\Microsoft Forefront Protection for SharePoint\FSSPUsernameFilter.dll failed to load. The data is the error.**

    Follow the steps below to resolve this issue in IIS7:

    a. Navigate to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Managers**, and find the websites where the error occurs.

    b. Select this website, and double-click **ISAPI Filters** on the right side.

    c. In the **Filter** pane, select the **FSSP Username Filter**.

    d. In the **Actions** pane, click **Remove**, and then a confirmation message pops up, select **Yes**.

    e. Navigate to *C:\Windows\System32\inetsrv\config*, open the ApplicationHost.config file with the Notepad. Delete the following content: **<filter name="FSSP Username Filter" path="c:\Program Files\Microsoft Forefront Protection for SharePoint\FSSPUsernameFilter.dll" enabled="true" />**

    f. Check whether this issue has been resolved, if it still exists, restart the IIS service of the specified website.

14. In the Farm Rebuild wizard, when you connect the SharePoint Servers to the target farm, some exceptions may occur on some SharePoint Servers, for example, if there are two SharePoint Servers in the target farm, one SharePoint Server is successfully connected to the target farm, while the other server failed to be connected to the target farm.

    Solution:

    This issue may be caused by the fact that the SharePoint Configuration cache files are not deleted when disconnecting the SharePoint Servers from the target farm. Thus, an error occurred when connecting the SharePoint Servers to the farm, saying **An update conflict has occurred when connecting the SharePoint Servers to the farm**. To resolve this issue, manually delete the SharePoint Configuration cache files after disconnecting the SharePoint Servers from the target farm, and then perform the Farm Rebuild job. For more detailed information on deleting the SharePoint Configuration cache files, refer to http://blogs.msdn.com/b/jamesway/archive/2011/05/23/sharepoint-2010-clearing-the-configuration-cache.aspx

15. RBS is enabled for one content database before the Farm Rebuild. After the Farm Rebuild job is finished, the RBS status of the restored content database is changed from **Enabled** to **Disabled** in the Storage Optimization product suite.

Solution:

To resolve this issue, navigate to *C:\Program Files\AvePoint\DocAve6\Agent\bin*, find the **AgentToolSP2010StorageRBS.exe**, and run this tool to enable the RBS for the specified content databases again.

16. The platform backup data updated from DocAve 5 is not supported by the Farm Rebuild.

    The tree structure of DocAve 5 is different than the structure of DocAve 6, and some data required for performing the Farm Rebuild has not been backed up in DocAve 5. We will try to resolve this issue in later releases.

Performing a Farm Clone

You can perform a Farm Clone to clone the SharePoint farm to another one using the backup data of backing up the whole farm. After the Farm Clone job, both of the SharePoint farms are functional at the same time. The cloned farm can be used as an environment for test or development. 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 Share Point 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.

***Note**: When performing a farm clone between different domains, Farm Clone requires source domain and destination domain have the following trust relationships:

- The source domain and the destination domain have a two-way trust, or
- The destination domain trust the source domain.

To perform a Farm Clone, 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 does not support cloning the VM backup data. Only the SharePoint farm backup data can be cloned to the destination farm, even if the selected backup job contains the VM backup data.

   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 Types** to list the backup jobs of all levels.

   b. **Filter by Job** – Limit the full farm backup jobs by job type using this drop-down list.

- **Backup type** – Select the backup type from the drop-down list; only the backup jobs of the specified types are displayed. Select **All Types** to list the backup jobs of all three types.

c. **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 jobs.
- **Backup jobs start within …** – Select this option to specify a time period. All of the Finished and Finished with Exception Platform backup jobs that have a start time within the specified time period will be displayed.

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 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 jobs. 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. Select the full farm backup job that you want to restore.

2. **View** – View all the backed up SharePoint components in the full farm backup job.

   ***Note:** The selection on the tree is disabled and cannot be edited. The **Web Front-End Servers** node and the **Custom Database** node are deselected.

3. **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 databases in different source SQL Instances using same database name, the 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**.

4. Click **Next** to enter the **Database Options** step.
5. **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. 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**.

    ***Note**: Farm Clone does not support **Custom Database** feature. You can perform a restore job at database level to restore the backed up custom databases, after the Farm Clone job is finished.
6. **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** pop-up 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.
7. Click **Next** to go to the **SharePoint Server Mapping** step.
8. **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. When configuring the mapping for SharePoint 2016 farms, only the destination server whose server role is **Custom** or the same as the corresponding source server can be listed. 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.

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.

9. 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.
10. 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.

11. **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.

    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.

12. **Index Option** – 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.

13. Click **Next** to go to the **SharePoint Configuration** step.
14. **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 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.
15. Click **Validation Test** to verify the information you entered. When the test is successful, click **Next** to go to **Clone Options** step.
16. **Clone Options** – Configure the **Conflict Resolution**, **Clone BLOB**, **Mapping Settings**, and **Notification** for the farm clone job.
    - **Conflict Resolution** – Choose a resolution in the event that a conflict occurs during this clone. To skip restoring the backed up database with destination database kept intact, select **Skip**; to remove the conflicting database in the destination, and restore the backup data, select **Overwrite**.
    - **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 have to select **Restoe BLOB by DocAve** or **Only update physical device** additionally. You are also 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:

      i. Select the checkbox beside a physical device mapping item, and then click **Destination Physical Device** on the ribbon. The **BLOB Batch Settings Page** appears.

      ii. Choose a destination physical device from the drop-down list. Click **Show** to view the path and usage information of the selected physical device.

iii. Click **OK** to save the batch settings and return to the **Physical Device Mapping** interface.

***Note**: Farm Clone does not support cloning Connector BLOB data and does not support cloning BLOB data to physical devices other than Net Share and IBM Storwize Family devices.

- **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 configuring restore settings.
    - **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, and does not support mapping multiple source usernames to one destination username.

      ***Note**: The **User Mapping** does not support mapping Central Administration site users. If the source domain and the destination domain do not have the required trust relationships, the Central Administration site may be unable to login. When this happens, you can manually add the user to the destination domain, grant it permissions, and remove the user from the source domain.

    - **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.

  ***Note**: The **Mapping Settings** function support SharePoint 2013 Beta (15.0.4128.1014), SharePoint 2013 RTM (15.0.4420.1017), SharePoint Foundation 2013 RTM (15.0.4420.1017), SharePoint 2013 SP1, SharePoint Foundation 2010 SP1, but does not support mapping the users of Active Directory group for SharePoint 2013.

- **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.

17. Click **Next** to go to **Overview** page.
18. **Overview** – View the current farm settings you have configured. You can click **Edit** to go back to each step to change the settings.
19. Click **Start** to run the farm clone.

Restoring or Configuring Specific Components after Farm Clone

Some of the farm components will not be cloned during the Farm Clone job. After you have finished the Farm Clone wizard, there may be several components that are not functional, such as the InfoPath Form Services. To make them functional, you must manually restore these components using an **Out of place restore** with the **Conflict Resolution** of **Overwrite**.

***Note**: The SharePoint Foundation Help Search database and index components do not support being cloned to the destination farm. After a Farm Clone, a new Help Search database will be created in the destination farm.

***Note**: After a Farm Clone, you must perform an out of place restore job to restore the Web.config file of FBA in IIS Settings of Web front-end server in order to make the FBA database function well.

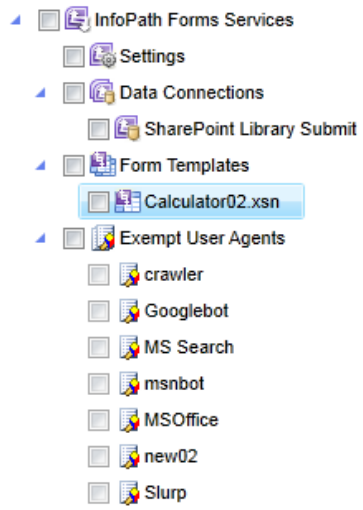


Figure 35: InfoPath Form Services' components.

Restoring Search Service Application

After the Farm Clone, if the Search Service Application cannot be used normally, you must perform an **Out of place restore** job with the **Conflict Resolution** of **Overwrite** to restore the specified Search Service Application again. If you want to delete the original Search Service Applications before the restore, follow the instructions below to delete the specified Search Service Applications.

There are two methods of deleting the Search Service Applications, which are provided below: the first, method is to delete the Search Service Applications through SharePoint Central Administration; the second, is to delete the Search Service Applications through the SharePoint Management Shell.

To delete the Search Service Applications through SharePoint Central Administration:

1. Navigate to **SharePoint Central Administration** > **Application Management** > **Manage service applications**.
2. Select the Search Service Application and select **Delete** on the ribbon to delete the selected Search Service Application.

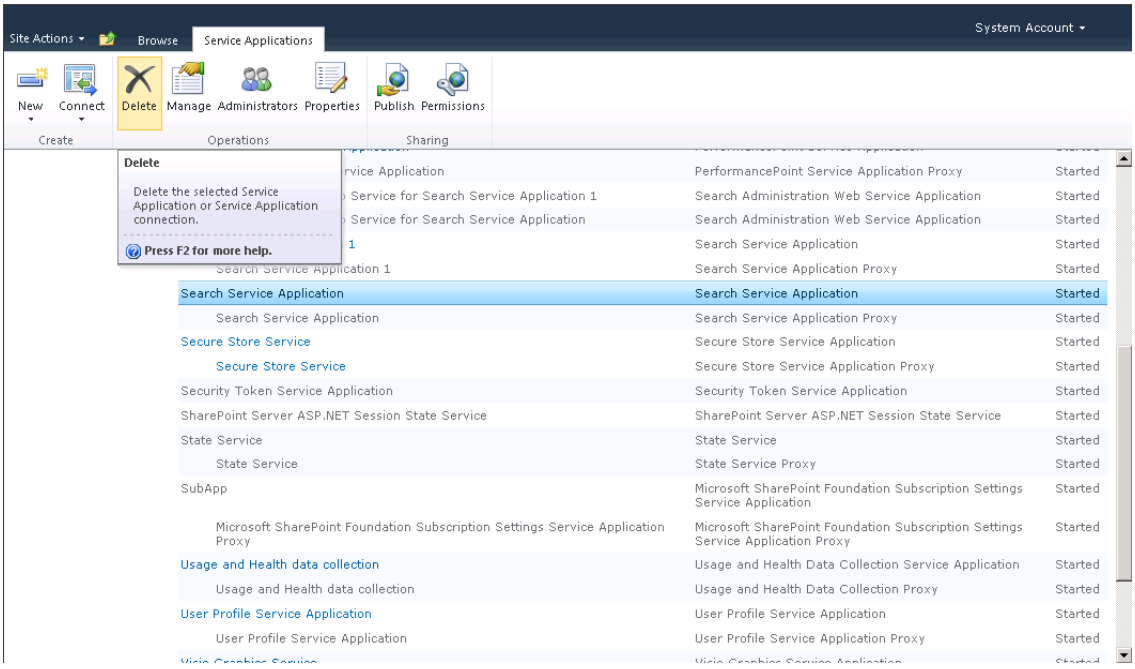


Figure 36: Deleting Search Service Application.

To delete the Search Service Applications through SharePoint Management Shell:

1. Navigate to **Start** > **Microsoft SharePoint 2010 Products** > **SharePoint 2010 Management Shell**. Right-click on the SharePoint Management Shell and then select Run as administrator.
2. Enter the following command to delete the specified Search Service Application:

```
$a = Get-SPEnterpriseSearchServiceApplication -Identity SSAName

Remove-SPEnterpriseSearchServiceApplication $a
```

SSAName represents the name of the specified Search Service Application that you want to delete.

Restoring Web Front-End Components

If you want to restore the configured files or some customized features on the Web front-end servers, you must select the corresponding Web front-end servers' nodes from the backup date tree and then perform an **Out of place restore** to restore the data with the **Conflict Resolution** of **Overwrite** after the Farm Clone.

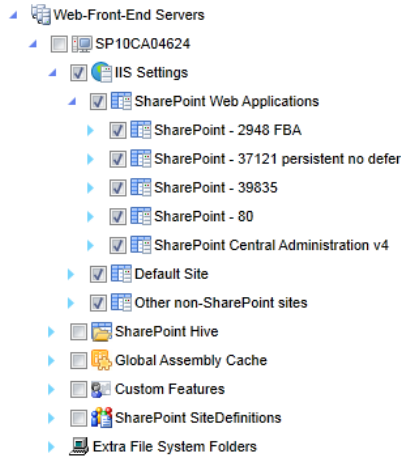


Figure 37: Restoring Web front-end components.

Configuring NewsGator after Farm Clone

After Farm Clone, the NewsGator in the destination farm is not functional. You must perform the following configurations:

1. Make sure the User Profile Service is **Started**.
2. Deactivate the features even though they may already be active after Farm Clone, and then activate the NewsGator features again. Otherwise, the service instance of the NewsGator Service Application cannot be created and the NewsGator site collection cannot function.
3. After successfully activated the NewsGator features, make sure the service instances are created and **Started**.
4. After all of the configurations above, the NewsGator can work well, and the site collections in NewsGator template can be accessed.

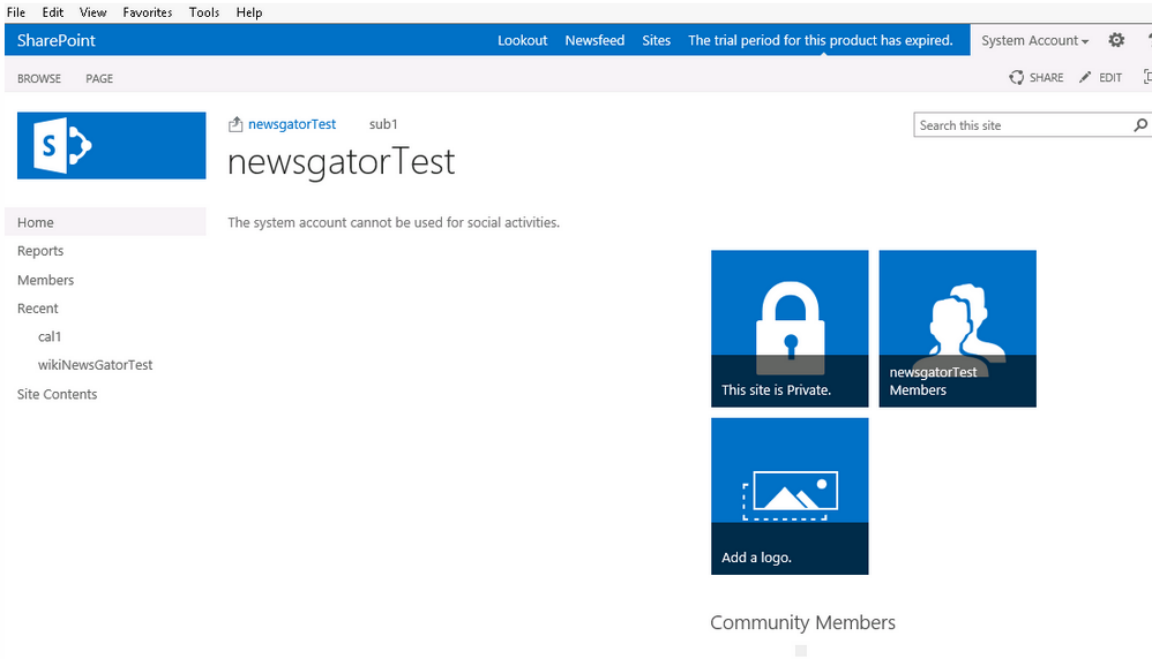


Figure 38: Accessing NewsGator site collection.

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

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.

Helpful Notes about Farm Clone

Pay attention on the following helpful notes before or after Farm Clone:

- **Project Server** – The Project Server must be installed on each SharePoint server of the destination SharePoint farm before performing Farm Clone. If not, the verification of the SharePoint Server Mapping will fail.
- **OWA for SharePoint 2010** – The OWA for SharePoint 2010 must be installed on each SharePoint server of the destination SharePoint farm before performing Farm Clone. If not, the verification of the SharePoint Server Mapping will fail.

- **OWA for SharePoint 2013** – The OWA Server for SharePoint 2013 is independent of the SharePoint farm. After the Farm Clone, configure the destination farm to use the same OWA Server as the source farm, and then no further configurations are required.
- **FAST Search Server** – After the Farm Clone, configure the properties of the FAST Search Connector and Query in the destination farm, and associate them with the newly configured FAST Search Server.
- **Windows Azure workflow** – Windows Azure Workflow Server is independent of the SharePoint farm. After the Farm Clone, 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 server 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 the Farm Clone, the PowerPivot cannot work. You must reinstall the SQL Server PowerPivot Feature and the related Data Providers, retract the solution in SharePoint Central Administration, and then configure the SQL Server PowerPivot using the **PowerPivot Configuration Tool**.
- **SQL Server PowerPivot for SQL Server 2008 and SharePoint 2010** is not supported for Farm Clone. 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 the Farm Clone, install the SQL Server Reporting Services feature and the add-ins. After the Farm Clone 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 job, perform an out of place restore of the Reporting Server, and then configure the Reporting URL of the destination server.
- **KnowledgeLake Imaging** is not tested for Farm Clone.

Performing a Farm Clone with VM

You can perform a Farm Clone with VM to clone the SharePoint farm to another one without manually configuring a farm in advance.

***Note**: Farm Clone with VM does not support cloning SQL server installed on the VM.

To perform a Farm Clone with VM, complete the steps below:

1. Select the **Clone** tab, and click **Start with Farm Clone with VM** on the right of landing page, or click **Farm Clone with VM** in the **Manage** group, The **Farm Clone with VM** page appears.
2. **Job Selection** – Select a backup job with backup data that will be used to restore the farm components.
    a. **Filter By** –Limit the scope of backup data restored by filtering out specified full farm backup jobs.
        - **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. By default, **All Farms** option is selected to display all plans for all farms.
            - **Plan Name** – Select the plan that you want to display from the drop-down list. By default, **All Plans** option is selected 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. By default, **All Types** option is selected to list backup jobs for all levels.
        - **Filter by Job** – Limit the backup jobs by job type using the drop-down list. Select a type from the **Backup Type** drop-down list; only backup jobs of the selected type are displayed. By default, **All Types** option is selected to list backup jobs for all three types.
        - **Filter by Time Range** – Filter backup data by completion time range using the drop-down list. By default, the **Backup jobs start within** option is selected. After you set or customize a time range, all of the Finished/Finished with Exception Platform backup jobs whose start time is within the selected time range are displayed. You can select **All Jobs** option to display all Finished/Finished with Exception Platform backup jobs.

    After the backup job is selected, the **Clone VM Job Selection** field appears.

    b. **Clone VM Job Selection** – Select a Clone VM job from the drop-down list, and you can view the job details by clicking **View**. If no related Clone VM job is finished, there will be a message to inform you to clone a VM at first. For details of cloning VM, refer to Cloning the VM.

***Note**: If you want to clone a VM whose display language is French, modify the **VMConfiguration.xml** file on all of the Agents before cloning the VM. For more information, refer to Editing the Configuration File Before Cloning a French-display-language VM.

3. **View** – View all the farm components that are displayed in the tree.
4. For details of the other steps, refer to Performing a Farm Clone, and continue from SQL Server Mapping step.

   ***Note**: When configuring the SharePoint Server Mapping step, you can click the **Refresh** button ( ) to refresh the destination server. After you finish the configuration, click **Validation Test** to restore the SharePoint Configuration database, which will be used in the following steps to check version and passphrase.

Editing the Configuration File Before Cloning a French-display-language VM

Before cloning a VM whose display language is French, modify the **VMConfiguration.xml** file on all of the Agents by referring to the information below:

1. Navigate to the *…\AvePoint\DocAve6\Agent\data\VM* directory, and find the **VMConfiguration.xml** file.
2. Open the **VMConfiguration.xml** file with Notepad, and find the **IsCloneFREnvironmentVM** attribute under the **<FarmClone></FarmClone>** node.
3. The default value of the **IsCloneFREnvironmentVM** attribute is **false**. To clone a VM whose display language is French, change the value of the **IsCloneFREnvironmentVM** attribute to **true**.

Cloning the VM

Clone VM is the first step of performing a Farm Clone with VM to provide a farm that is the same as the source. Select the **Clone** tab in Platform Backup and Restore wizard, then click **Clone VM** in the lower-left corner of the landing page and you will go to Clone VM wizard.

***Note**: Farm Clone with VM has two sub-jobs: Clone VM; Clone Farm. After cloning VM, the entire job is not actually finished. You may find that the farm is not functional or the Agent Type viewed in Agent Monitor is incorrect. This situation occurs because that the computer names have been changed but the farm still records the original server names. When Clone Farm is finished and the Agent Service is restarted, the farm will be functional and the Agent Type will be correct.

***Note**: DocAve does not support backing up user-defined certificates of the Agent on source VMs. Users need to configure the certificate through DocAve Agent Configuration Tool on the cloned VM.

1. From the **Clone VM** tab, configure the following options in the **Filter By** area.

***Note**: Only the backup jobs that successfully backed up the VM when performing **Back up the whole farm with VM** can be displayed and filtered in the calendar view.

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

- **Filter by Plan** – the full farm backup data by plan information using this drop-down list.
    - **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.
- **Filter by Job** – Limit the full farm backup jobs by job type using this drop-down list.
    - **Backup Job Module** – Select the backup job module from the drop-down list. Select All Modules to display the jobs of all the modules.

      ***Note**: The module can only be Platform Backup.

    - **Backup Type** – Select the backup type from the drop-down list; only the backup jobs of the specified types are displayed. Select All Types to list the backup jobs of all three types.
- **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 jobs.
    - **Backup jobs start within …** – Select this option to specify a time period. All of the **Finished** and **Finished with Exception** platform backup jobs that have a start time within the specified time period will be displayed.

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 whole farm with VM 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 whole farm with backup jobs. Place the mouse cursor over the whole farm with VM backup job to display job information such as the Farm Name, Plan Name, Job ID, Backup Option, Job Status, Data Import, and Backup Job Module. Click on **Day**, **Week**, or **Month** to change the view to see all the available whole farm with VM backup jobs during that time period. Click the page turning buttons ( ) at the top-left corner to turn the page. Select the whole farm with VM backup job that you want to restore.

2. **Data Selection** – Select the VM that you want to clone. You can select several VMs to clone, and make sure that the SharePoint Central Administration server is selected.

   ***Note**: **Clone VM** does not support cloning the backed-up custom VM.

3. **VM Configuration** – Click **Edit** in the **Details** column of the specified VM to edit the following settings.

- **VM Name** – Create the destination VM name. This name used to identify the VM in the inventory. This action does not change the name used as the computer name by the guest operating system.
- **Source Computer Name** – View the source computer name.
- **Destination Computer Name** – Configure the destination computer name of the cloned VM according to your situation. The name must be changed if the VM is cloned to the domain where the original VM resides.
- **Guest Operating System Version** – View the version of the guest operating system.

  ***Note**: This field is only appears while configuring settings for the VMs on ESX/ESXi or vCenter host server.

- **Destination Domain Name** – The source domain name is displayed by default. If you want to restore the VM to another domain, enter the full qualified domain name. Note that the source domain and the destination domain must have one of the following trust relationships: The source domain and the destination domain have a two-way trust, or the destination domain trust the source domain.
- **Host Profile** – Select a host profile for the destination host.

  ***Note: Clone VM** does not support cloning the VMs across Hyper-V/Hyper-V Cluster host server and ESX/ESXi/vCenter host server. If the backed up VM is hosted by a Hyper-V/Hyper-V Cluster host server, the host profile of ESX/ESXi or vCenter type cannot be displayed. If the backed up VM is hosted by a ESX/ESXi or vCenter host server, the host profile of Hyper-V/Hyper-V Cluster type cannot be displayed.

  ***Note**: If the host type of the host profile is ESX/ESXi, and the ESX/ESXi host is currently being managed by vCenter server, update the specific host profile by changing the host server type from ESX/ESXi to vCenter.

  ***Note**: Support cloning VM for VMs that are in Hyper-V Failover Cluster. If the selected host profile is a Hyper-V Cluster type, then the **Role** filed appears.

- **Agent** – Select an Agent to restore the VM in the destination. If the destination VM is on a Hyper-V host server, the Agent is the same as the host profile Agent and cannot be changed.

  ***Note:** If the VM you are about to restore resides in the Hyper-V host server, the Agent drop-down list will be unavailable and you can only use the default Agent to execute the restore job. If you are about to restore the VM to a Hyper-V Failover Cluster, the Agent is able to be chosen from the drop-down list after selecting a Hyper-V Cluster type host profile. The Agent must be in the cluster that is specified in the selected host profile.

- **Role** – Enter the name of a role to organize the restored VM. By default, the name is the same as the VM name. The role can be an existing one in the destination cluster, or can be created.

***Note**: This setting is for cloning VM to Hyper-V Failover Cluster and only appears when you select a Hyper-V Cluster type host profile.

- **Destination VM Location** – Configure the destination location to which the VM will be restored. For different host server of Hyper-V/Hyper-V Cluster, ESX/ESXi, and vCenter, refer to the following steps.
    - **Hyper-V** – For Hyper-V/Hyper-V Cluster VM, the text box of **Destination VM Location** field displays the default destination VM location path automatically after the host profile selection, and you can also customize it according to your situation.
        - **Virtual Hard Disk Location** – Configure the virtual hard disk file mapping. The default destination file path is filled in the text box automatically after the host profile selection, and you can also choose to customize it according to your situation. If the file mapping configuration table is hided, click **Details** to let it appear.
    - **ESX/ESXi and vCenter** – For ESX/ESXi VM, and VMs organized by vCenter, click the VM host server node to expand the tree to display all the VMs on the host server. Select the node of the destination host server where you want the restored VM to reside.
        - **Host Selection** – Select a host that is in the selected cluster, as the destination host where to restore the VM.

          ***Note**: This field appears when you choose a vCenter host cluster as the destination VM location.

        - **Inventory Location** – After selecting the destination VM location, the **Inventory Location** section appears. Click the datacenter node to expand the tree to display all the VM folders, and select the folder that you want to contain the restored VM.

          *Note: This field only appears when the selected host profile is **vCenter** type. When a vApp is selected as the resource pool, the target folder will be ignored.

        - **Datastore Information** – View the information of the datastore, and you can click **Refresh** to retrieve the latest datastore information. You can also view more information through clicking Manage columns ( ), and select **Capacity**, **Provisioned Space**, and **Type** from the drop-down list. You can click the page turning button ( ) to turn page.
        - **Storage Configuration** – Select the object by selecting the corresponding checkbox, and then select a destination storage for each of the virtual machine files in the list. The batch settings of datastore is supported. You can select all of the objects by selecting the checkbox

next to the **Object**, and click the batch settings button ( ), the Datastore Batch Settings page appears.

***Note**: After selecting the datastore, the values in **Require Space for Restore** column will be updated.

- **Storage DRS Settings** – When restoring the VM to a datastore cluster, choose whether or not to disable Storage DRS. By default this option is unchecked. If you choose to disable Storage DRS for this VM, the Automation Level of restored VM's Storage DRS rule will be set as Disable. If this option is selected, the Automation Level will be set as Default.

  ***Note**: This field appears after you select a datastore that is in datastore cluster.

- **Sysprep Settings** – Choose whether or not to enable Sysprep to create a new SID for the cloned VM automatically. It is recommended to enable the Sysprep, if cloning VM to the destination farm in the same domain.

  ***Note**: If you are about to clone the VM to a different domain, after enter a different full qualified domain name as the destination domain name, uncheck this checkbox. The **Unjoin Domain Account** field appears below the **Domain Account** field.

- **Local Account** – The Administrator is the only qualified local account to change the destination computer name, and execute the Sysprep operation. Enter the password of the Administrator, which is the local account of the source computer.
- **Domain Account** – Select a domain account for the cloned VM in the destination domain.
- **Account for Unjoining Domain** – Select a domain account of the source domain that has permission to remove the VMs from their source domain.
- **Agent Account** – Select an Agent account profile for the DocAve Agent that is backed up and cloned with the VM.

  ***Note**: After cloning VM, the farm is not functional and the Agent Type viewed in Agent Monitor is incorrect. This situation occurs because that the computer names have been changed but the farm still records the original server names. When Clone Farm is finished and the Agent Service is restarted, the farm will be functional and the Agent Type will be correct.

- **Network Settings** – Select a network for the adapter from the drop-down list. Click **Configure** in the **TCP/IPv4 and TCP/IPv6** column, then the **TCP/IPv4 and TCP/IPv6 Properties** page appears.

  ***Note**: Clone VM does not support configuring multiple IP addresses for one network adapter. You can manually configure the IP settings after the VM is successfully cloned.

***Note**: If a VM hosted on Hyper-V 2008 R2, Hyper-V 2012 R2, or Hyper-V 2016 server has **Static** MAC address configured, the VM's MAC address will become **Dynamic** after being out-of-place restored to the destination.

Choose to enable at least one IP settings, and then configure the following settings:

- **IP Address Settings** – Choose to obtain an IP settings automatically from the network, or use the following IP settings by configuring IP address, Subnet mask, and Default gateway.
- **DNS Settings** – Choose to obtain a DNS server address automatically from the network, or use the following DNS server address by configuring **Preferred DNS server IP address** and **Alternate DNS server IP address**.

  Click **Save** to save the settings, then the **TCP/IPv4 and TCP/IPv6 Properties** page disappears.

When finished the settings above for VM, click **Validation test** to validate the configured information. If test is successful, click **Save** to save the configuration.

4. When you are finished, click **Next**. The **Restore Settings** page appears.
5. **Restore Settings** – Configure how the content should be restored.
   - **VM Conflict Resolution** – Define the VM conflict resolution behavior. For the ESX/ESXi or vCenter VMs, if the **.vmx** configuration file of the source VM is under the same full path as an existing **.vmx** configuration file in the target, it is considered a conflict. For the VMs stored on the datastores that are in a vCenter datastore cluster, if there is a VM whose name is the same as the backed up VM in the datastore cluster, it is considered as a conflict. For Hyper-V hosted VMs, if a VM ID same as the one in the backup already exists in the destination, it is considered as a conflict.
     - **Skip** – Do not restore the source conflicting VM, and keep the destination VM intact.
     - **Overwrite** – Delete the conflicting VM in the destination and restore the backed up VM.
   - **Notification** – Select a created e-mail notification profile, or create a new one that contains the report settings and the report recipients. You can view the detailed information of the selected profile by clicking **View**. For more information on working with notification policies, refer to the DocAve 6 Control Panel Reference Guide.
6. **Schedule** – Configure the schedule to set the time to restore the content:
   - **Schedule Selection** – Choose Restore immediately after wizard finishes to run the plan immediately, or choose Configure the schedule myself to configure a customized schedule.
   - **Description** – Optionally enter a description of the restore plan in the text box.

   Click **Next** to proceed to the **Overview** interface.

6. **Overview** – Review and edit plan selections. To make changes, click **Edit** in the middle of a heading row under the **Settings** tab. 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 VM tree after the restoration.

***Note**: If the VM will be cloned for more than one time without changing its host name, but the IP address is different, please pay attention to the following known issue: Make sure that before Clone VM, there is no host record in the DNS Hosting Service, or manually execute Flush DNS operation.

***Note**: If operating system for the Hyper-V host server is Windows Server 2012 or Windows Server 2012 R2, and the operating system for the VM is Windows Server 2008 R2, you need to upgrade the Integration Service of the Hyper-V host server to successfully configure the IP settings for VM.

Performing a Farm Repair

When your SharePoint farm is malfunctioning, perform Farm Repair to repair your farm without disconnecting servers from the farm. .

***Note**: AvePoint recommends not using the SharePoint farm when you performing a Farm Repair job.

To repair a farm without disconnecting the servers from 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, you can view and select the following:
    - SharePoint farm servers you wish to repair
    - The services that are running on the corresponding server.

    At the bottom of the table, the selection information is displayed to indicate how many servers are selected. You can deselect the checkboxes by clicking **Clear Selection**.
4. Optionally, select a notification profile from the **Send Notification** drop-down list to select a receiver for the Farm Repair job report.
5. Select the **Repair** button on the ribbon to run the Farm Repair 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 go to Job Monitor to view this information.

Checking a Job Status

Platform Backup and Restore contains a Job Monitor button where users can view the status of jobs. This is useful for monitoring jobs or troubleshooting for errors. For Platform granular restore job, users can check the **Object Details**, **Configuration Details,** and **Security Details** in the Job Monitor for more clarified and detailed information.

For the backup jobs or restore jobs with the BLOB data involved, the **BLOB Details** tab will appear on the **Job Details** page to display the detailed information for the BLOB backup or restore.

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

Refer to the DocAve 6 Job Monitor Reference Guide for more information.

Performing a Full Farm DocAve Platform Out of Place Restore

Refer to the section below for detailed instructions on performing a full farm out of place restore using Platform Backup and Restore.

Backing up the Source Farm Using Platform Backup

To back up the source farm, create a new platform backup plan as follows:

1. Login to DocAve and navigate to **Data Protection** > **Platform Backup & Restore** > **Platform Backup**.
2. Click **Plan Builder** > **Form Mode** on the ribbon and create a new plan.
3. Select a farm from the **Farm** drop-down list, and then select an Agent group to browse the farm tree and execute the backup job. In the **Backup Components Selection** field, select the **Back up the whole farm** option.
4. Run this plan. For more detailed information, refer to Using Form Mode to Create a Backup Plan.

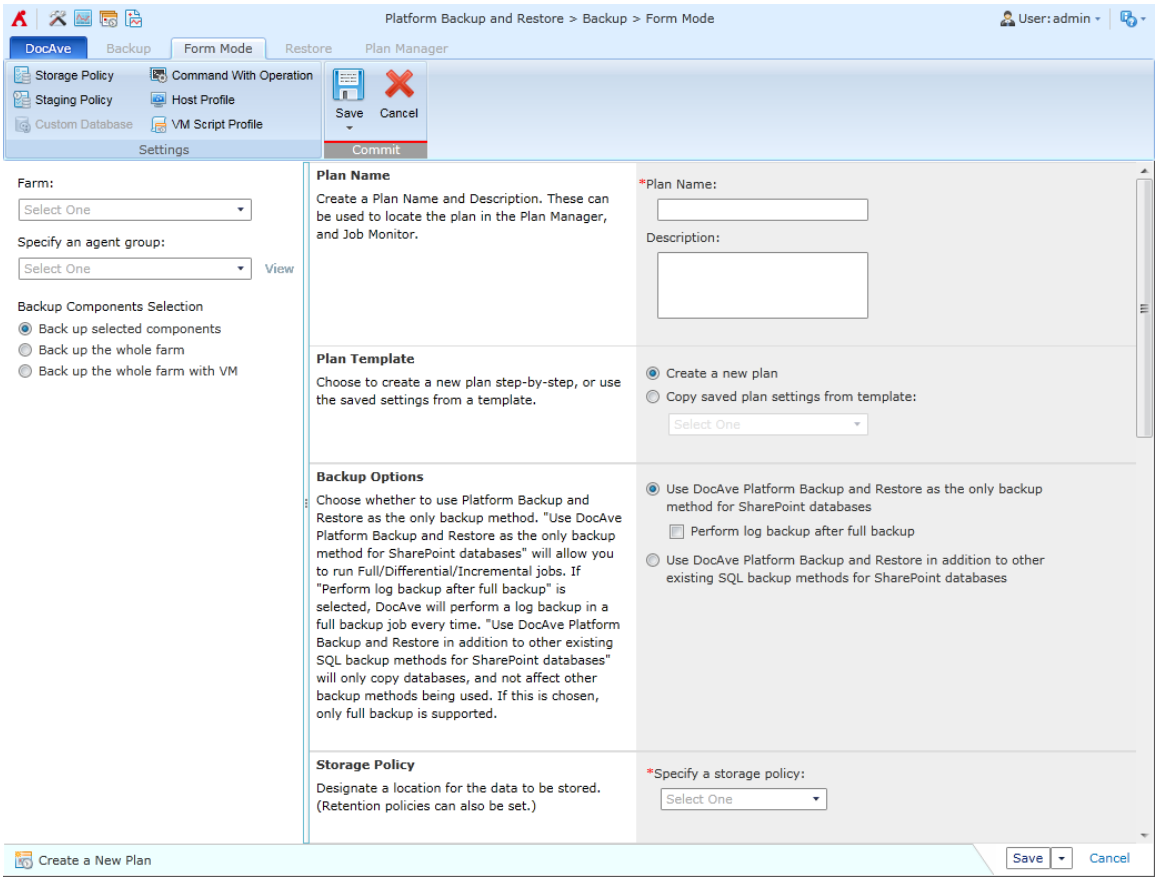


Figure 39: Create a new plan using the Form mode.

Performing the Out of Place Platform Restore

The out of place platform restore supports restoring one or more supported nodes to another farm. Refer to the detailed steps below to conduct an Out of Place Platform Restore:

1. Log into DocAve and navigate to **Data Protection** > **Platform Backup & Restore** > **Platform Restore**.
2. In the restore tab, click **Restore** on the ribbon to open the restore wizard.
3. In the **Job Filter** page, you can choose to filter the backup jobs according to the **Farm**, **Plan Name**, **Backup type**, **Restore granularity level** or **Time Range**, and then find the exact job that you want to restore data from.

   In this case, we use the default filters in the Job Filter page. Click **Next** on the ribbon to go to the Backup Jobs page.

   The backup jobs are listed in the Backup Jobs page according to the start time of the jobs. Click **Day**, **Week**, or **Month** to change the view to see all the available jobs during that time period. You can also click the page turn button (< >) on the top-left corner of the calendar to turn the page.

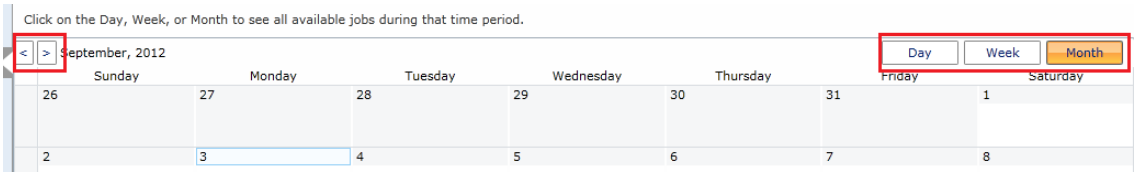


Figure 40: Change the view and turn the page.

In this case, select the backup job performed in the Backing up the Source Farm Using Platform Backup section and click the **Next** button at the bottom right corner to go to the Data Selection page.

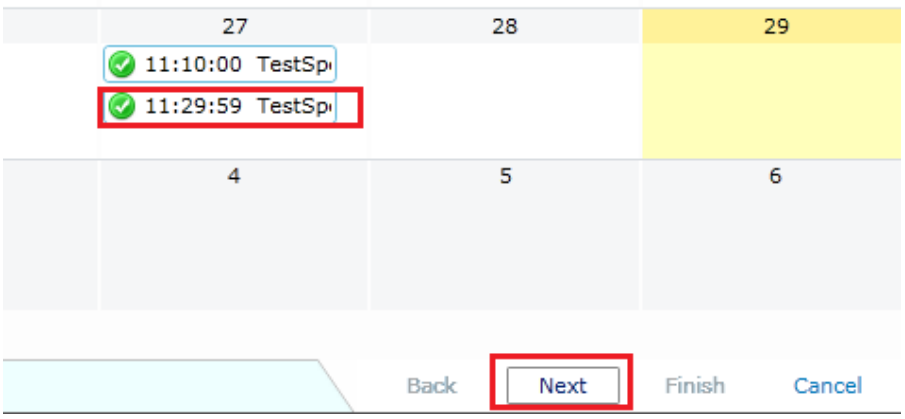


Figure 41: Select a backup job and click the Next button.

4. In the Data Selection page, click the farm node in the **Backup Data** area to load the tree and then select the content that you want to restore.

The following nodes cannot be restored using the out of place platform restore. For more details about the supported SharePoint 2010/2013 components of out of place platform restore, refer to Appendix D: SharePoint 2010 Components Supported in Platform Backup and Restore or Appendix E: SharePoint 2013 Components Supported in Platform Backup and Restore.

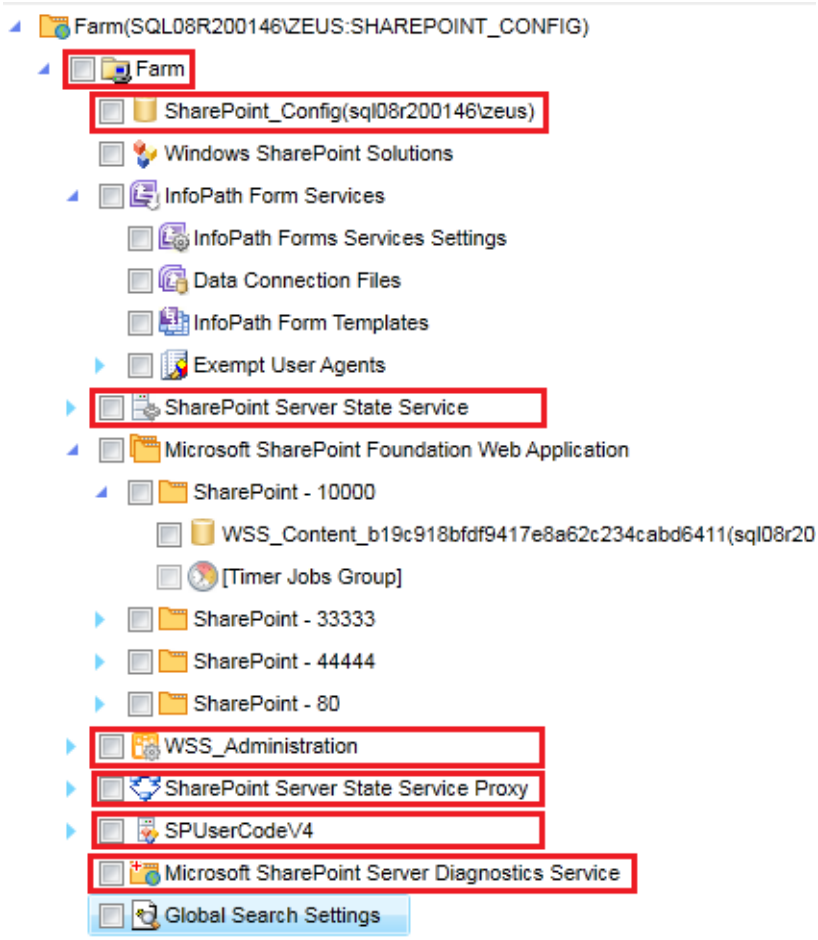


Figure 42: Nodes that cannot be restored using out of place platform restore.

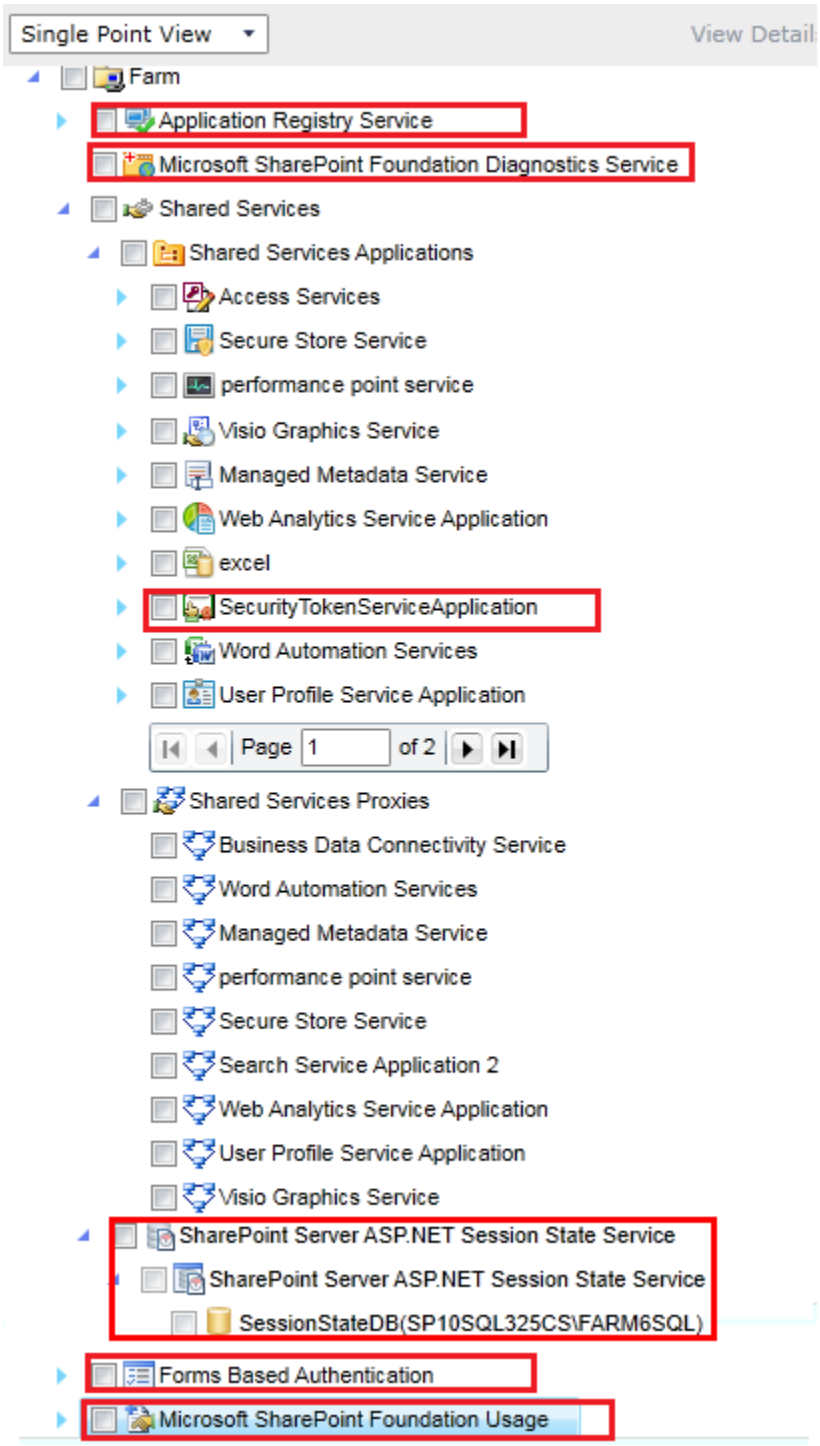


Figure 43: Nodes that cannot be restored using the out of place platform restore.

5. After selecting the content to be restored, refer to the corresponding sections below for the other configurations.

Restoring Solutions, InfoPath Form Services and Global Search Settings

1. In the Data Selection page, click the farm node in the **Backup Data** area to load the tree and then select **Solutions**, **InfoPath Form Services** and **Global Search Settings** nodes on the tree.

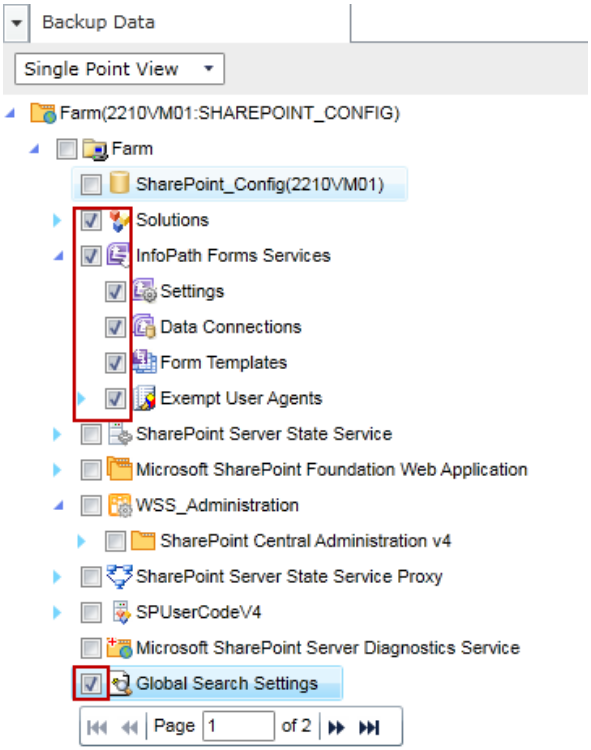


Figure 44: Selected nodes on the tree.

2. Click the **Next** button at the bottom right corner to go to the Restore Type page. Select **Out of place restore** in **Restore SharePoint farm components** and select a destination farm in the appeared **Destination Farm** drop-down list.

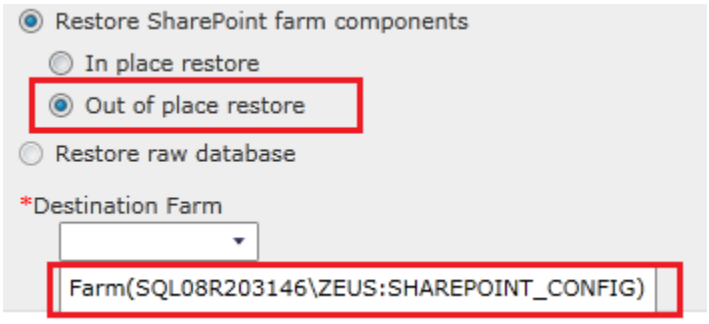


Figure 45: Configure the Restore Type field.

3. Click the **Next** button at the bottom right corner to go to the **Destination Component Options** page, and then configure the options according to your requirements. For the detailed explanation of each option, refer to the Building an Out of Place Restore Plan at Database Level in this user guide.

In this case, use the default settings in this page and 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 an Out of Place Restore Plan at Database Level in this user guide.

   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 specified **Start time** that you configure. For the detailed explanation of each option, refer to the Building an Out of Place Restore Plan at Database Level in this user guide.

   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 job.

Restoring Web Applications and Content Databases

Multiple Web applications and content databases can be selected when performing the restore. The following case shows the steps required to restore only one web application and one content database.

***Note**: If you use the Out of Place Platform restore to restore the same content database to the same destination farm more than once, there will be conflicts of the **Site ID**, even if you restore the same content database to Web application using different names.

***Note**: If performing an Out of Place Restore of a backed-up TDE-encrypted database, a master key must already exist in the destination regardless of the fact that whether or not the password of the master key is the same as the source one. On the destination server, use the following SQL statement to create a master key:

"USE master;

GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<YourPasswordHere>';

Go"

Then perform the out of place restore job to restore the TDE-encrypted database.

1. In the Data Selection page, click the farm node in the **Backup Data** area to load the tree and then select one web application and its database on the tree.

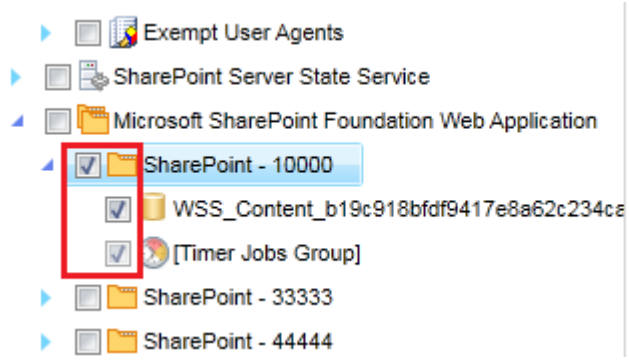


Figure 46: Select the web application and its database.

2. Click the **Next** button at the bottom right corner to go to the Restore Type page. Select **Out of place restore** in **Restore SharePoint farm components** and select a destination farm in the appeared **Destination Farm** drop-down list.

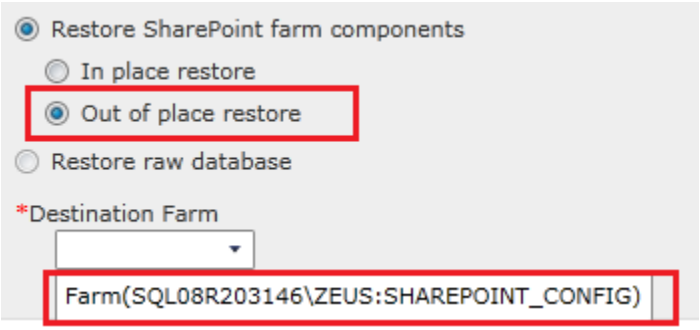


Figure 47: Configure the Restore Type field.

3. Click the **Next** button at the bottom right corner to go to the Destination Component Options page, and then configure the options according to your requirements.

   Click **Edit** in the **Details** column of the specified web application to edit the web application configuration. The options configured here are the same as those when creating a new web application. For example, when configuring the application pool you can choose to use an existing application pool or create a new one. The configuration and the permission requirements for creating a new application pool are the same as those when creating a new web application.

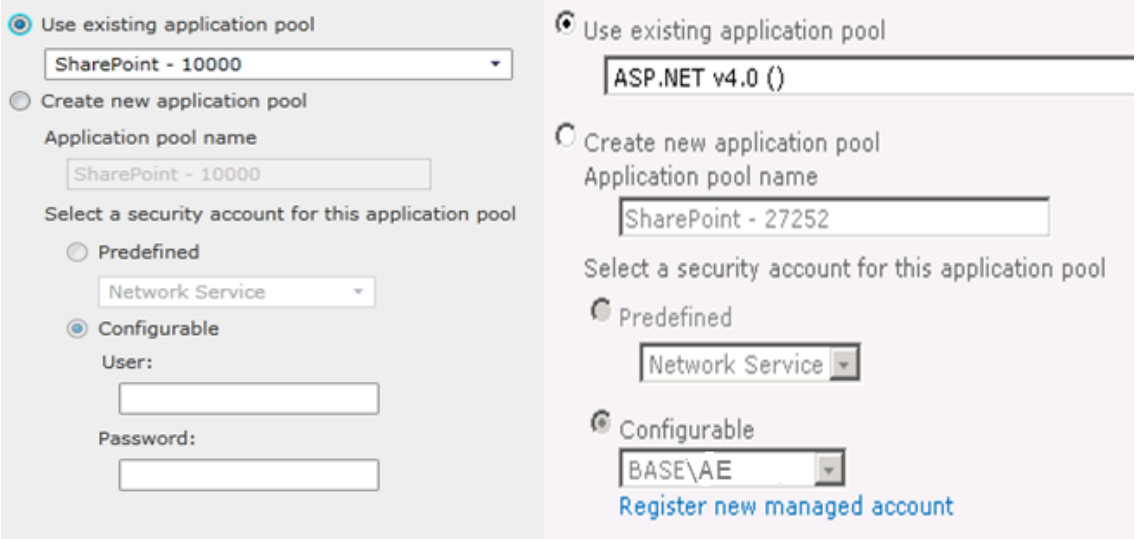


Figure 48: DocAve configuration (left) and the SharePoint configuration page (right).

After you finish the Web application configuration, click **OK** to save the configuration and then click **Edit** in the **Details** column of the specified content database to edit its configuration. The options configured here are the same as those when configuring the content database settings during creating a new web application. For the detailed explanation of each option, refer to Building an Out of Place Restore Plan at Database Level.

Component Name	Type	Details
SharePoint - 10000	Web Application	*Edit
WSS_Content_b19c918bfdf9417e8a62c234cabd6411	Content Database	Edit

Figure 49: Edit the content database configuration.

After you finish the content database configuration, click **OK** to save the configuration and 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. 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 specified **Start time** that you configure. For the detailed explanation of each option, refer to Building an Out of Place 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 job.

Helpful Notes When Restoring Special Kinds of Web Applications

Below are some helpful notes when restoring special kinds of Web applications:

- Restoring the HTTPS Web application.

  The displayed URL in the **Public URL** field will start with **https**.

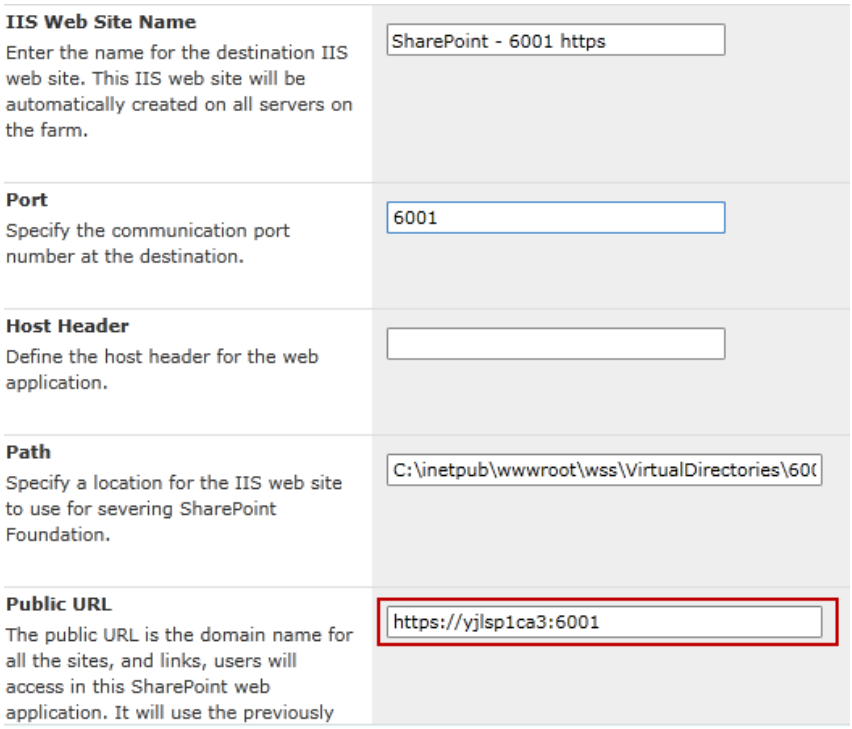


Figure 50: Public URL of the HTTPS web application.

- When restoring a Web application that has several zones in the Out Of Place Platform Restore, click **Show Other Zone Information** to configure the settings of other zones.

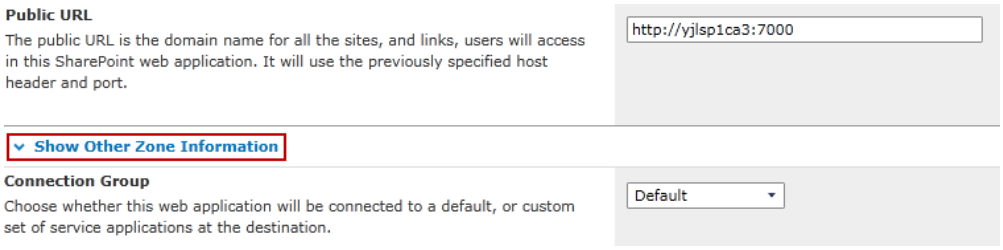


Figure 51: Show Other Zone Information link.

For example, the Intranet zone settings.

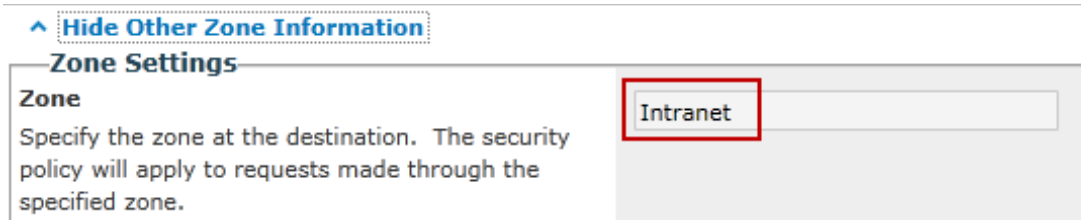


Figure 52: Settings of the Intranet zone.

- When restoring multiple content databases at one time, you must configure the detailed settings for each of the content database that will be restored.

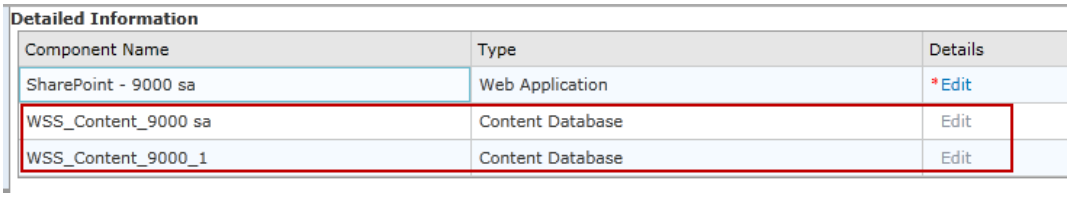


Figure 53: Configure the settings for each content database.

- If one content database has more than one **NDF** file, all its **NDF** files will be loaded when configuring the detailed settings for this content database.

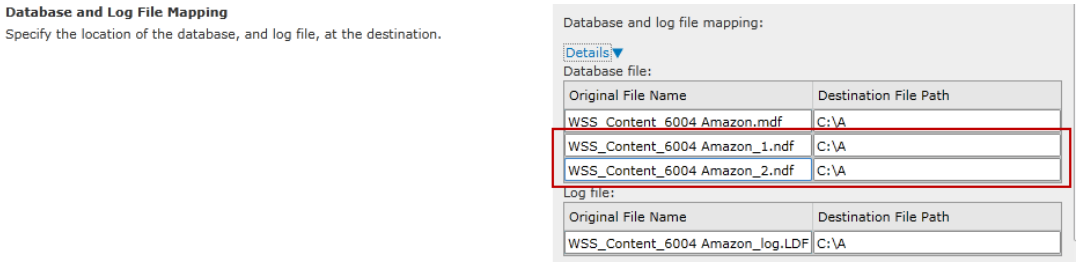


Figure 54: Detailed settings for one content database having multiple NDF files.

- If you select only one content database and perform the out of place restore, you can select the web application that you want to restore this content database to in the

Parent Web Application URL field when configuring the detailed settings for this content database.

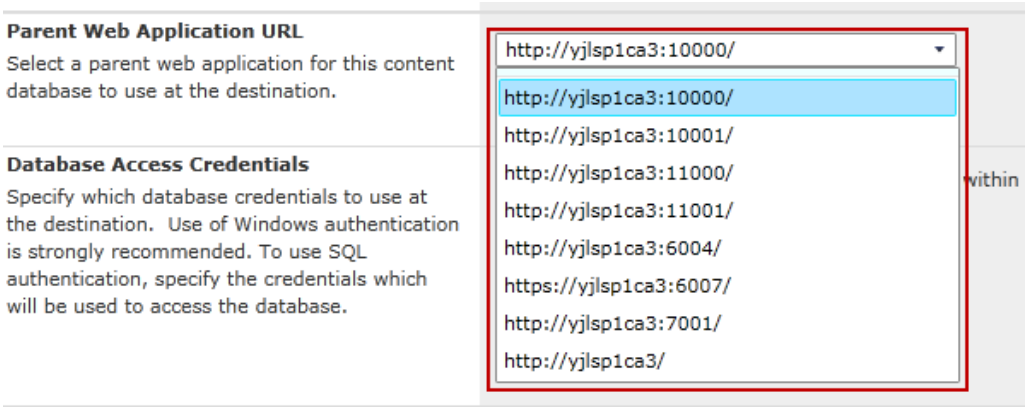


Figure 55: Configure the Parent Web Application URL field.

Restoring Service Applications

Multiple service applications can be selected when performing the restore. In the following case, we choose to restore all the service applications of SharePoint 2010/2013/2016 that are supported in the out of place platform restore.

1. In the Data Selection page, click the farm node in the **Backup Data** area to load the tree and then select all the service applications that are supported in the out of place platform restore on the tree.

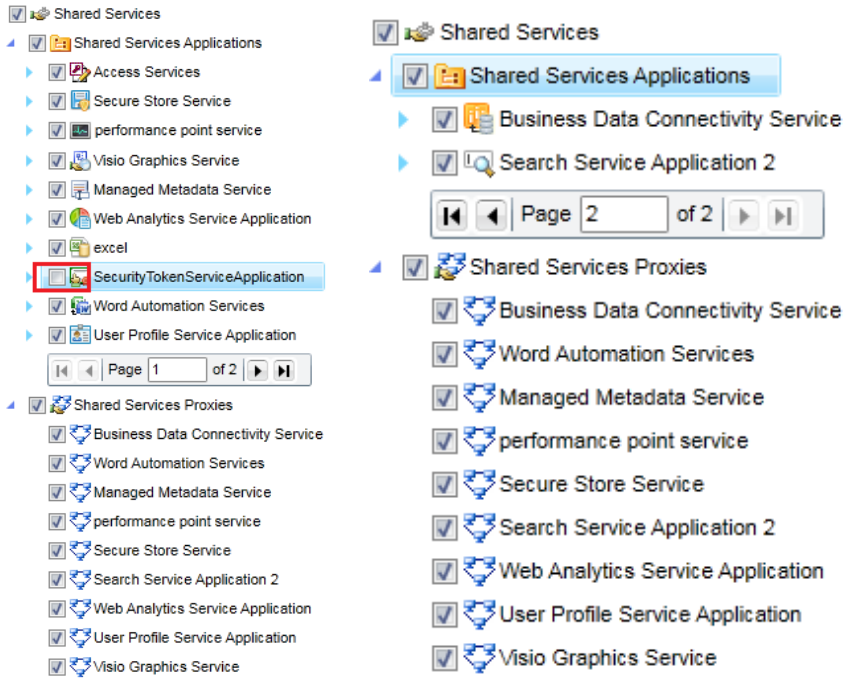


Figure 56: Select all the service applications of SharePoint 2010 that are supported in the out of place platform restore.

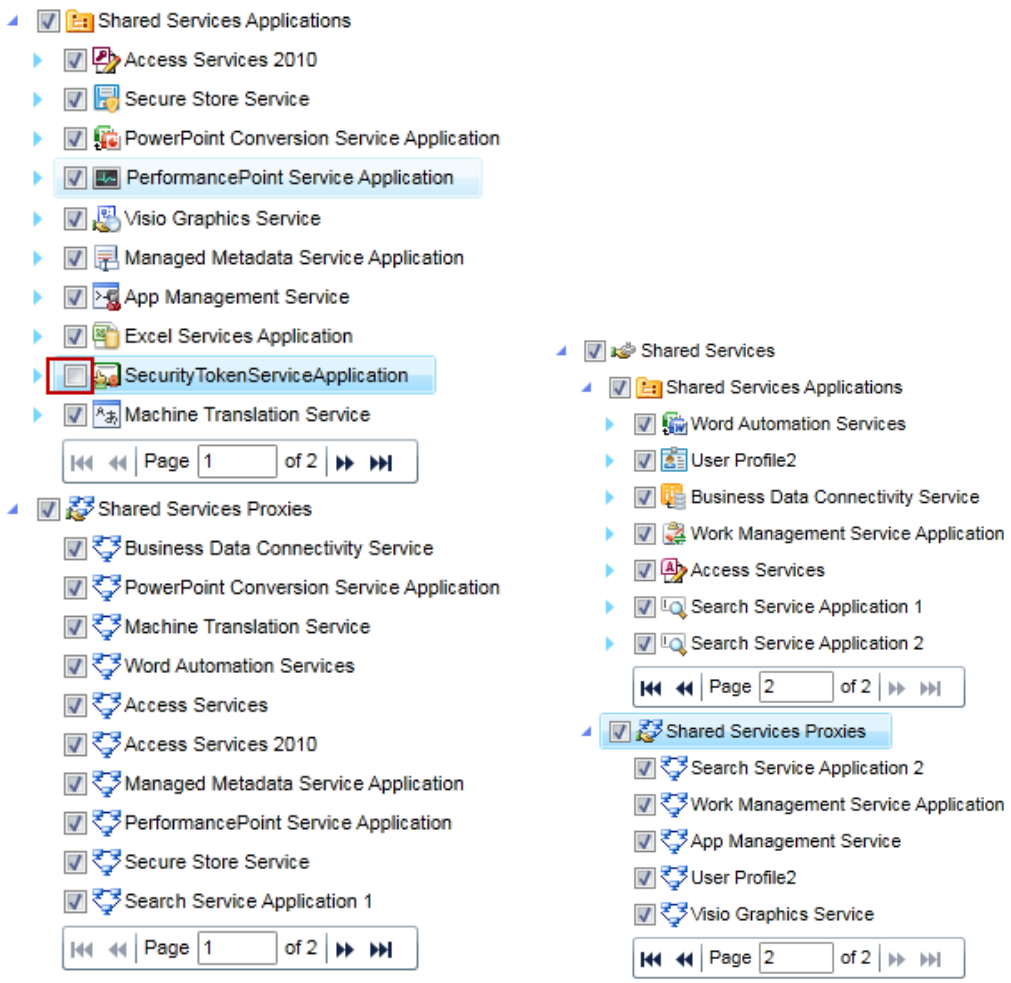


Figure 57: Select all the service applications of SharePoint 2013 that are supported in the out of place platform restore.

2. Click the **Next** button at the bottom right corner to go to the Restore Type page. Select **Out of place restore** in **Restore SharePoint farm components** and select a destination farm in the appeared **Destination Farm** drop-down list.

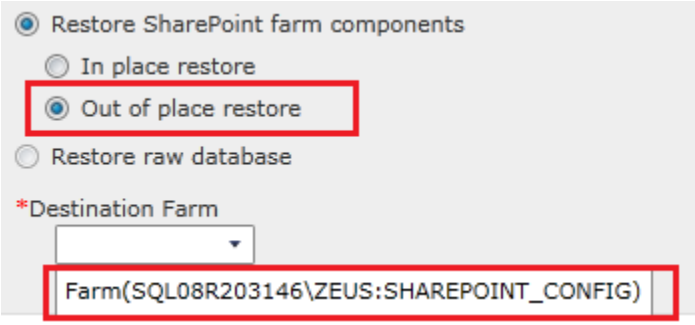
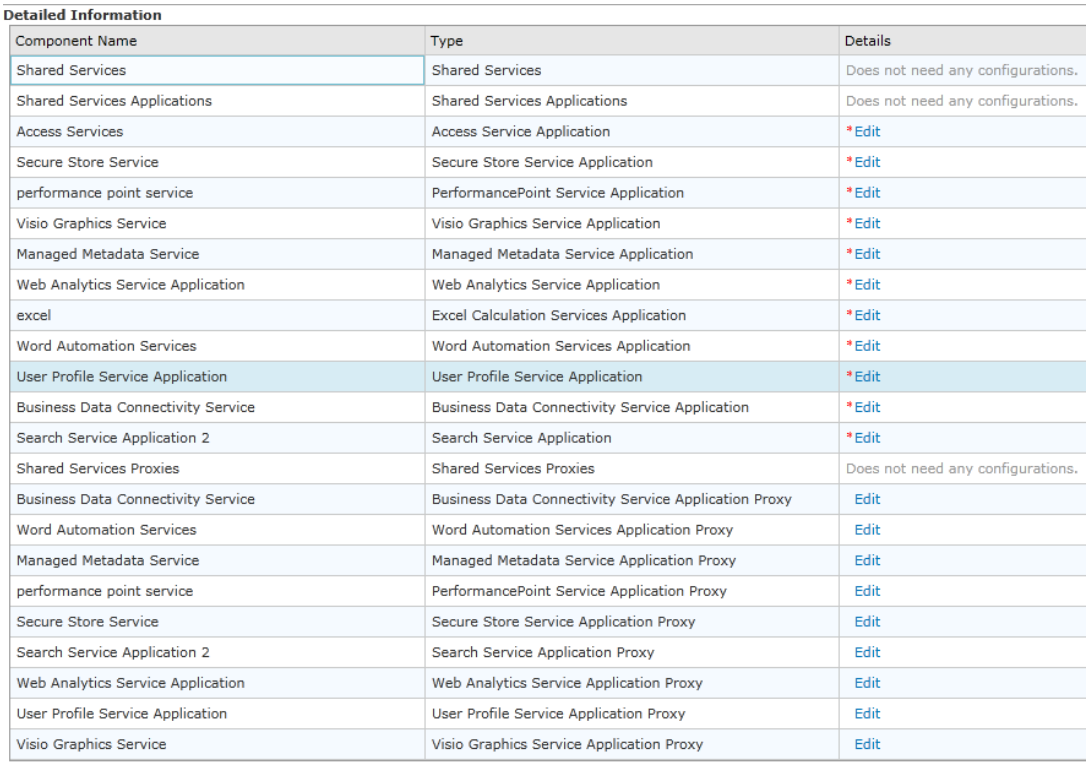


Figure 58: Configure the Restore Type field.

3. Click the **Next** button at the bottom right corner to go to the **Destination Component Options** page, and then configure the options according to your requirements.

Click **Edit** in the **Details** column of each service application to edit its configuration. The options configured here are the same as those when creating a new service application. For example, when configuring the application pool, you can choose to use an existing application pool or create a new one. The configuration and the permission requirements for creating a new application pool are the same as those when creating a new service application. To be



Detailed Information

Component Name	Type	Details
Shared Services	Shared Services	Does not need any configurations.
Shared Services Applications	Shared Services Applications	Does not need any configurations.
Access Services	Access Service Application	*Edit
Secure Store Service	Secure Store Service Application	*Edit
performance point service	PerformancePoint Service Application	*Edit
Visio Graphics Service	Visio Graphics Service Application	*Edit
Managed Metadata Service	Managed Metadata Service Application	*Edit
Web Analytics Service Application	Web Analytics Service Application	*Edit
excel	Excel Calculation Services Application	*Edit
Word Automation Services	Word Automation Services Application	*Edit
User Profile Service Application	User Profile Service Application	*Edit
Business Data Connectivity Service	Business Data Connectivity Service Application	*Edit
Search Service Application 2	Search Service Application	*Edit
Shared Services Proxies	Shared Services Proxies	Does not need any configurations.
Business Data Connectivity Service	Business Data Connectivity Service Application Proxy	Edit
Word Automation Services	Word Automation Services Application Proxy	Edit
Managed Metadata Service	Managed Metadata Service Application Proxy	Edit
performance point service	PerformancePoint Service Application Proxy	Edit
Secure Store Service	Secure Store Service Application Proxy	Edit
Search Service Application 2	Search Service Application Proxy	Edit
Web Analytics Service Application	Web Analytics Service Application Proxy	Edit
User Profile Service Application	User Profile Service Application Proxy	Edit
Visio Graphics Service	Visio Graphics Service Application Proxy	Edit

Figure 59: Configurations for the service applications.

- **Access Services 2010 Web Service Application** (SharePoint 2013)**/Access Service Web Service Application** (SharePoint 2010) — Configure the following settings for this service application.
    - **Service Name** — After the out of place platform restore, the restored Access Services Web Service Application will be named using the name entered here.
    - **Application Pool** — Choose the application pool that will be used by this service application. You can choose to use an existing application pool or create a new application pool.
    - **Default Proxy List** — Choose whether to add this service application's proxy to the default proxy list in the destination farm.

  Configure the settings for the same options of other service applications according to the detailed information above.

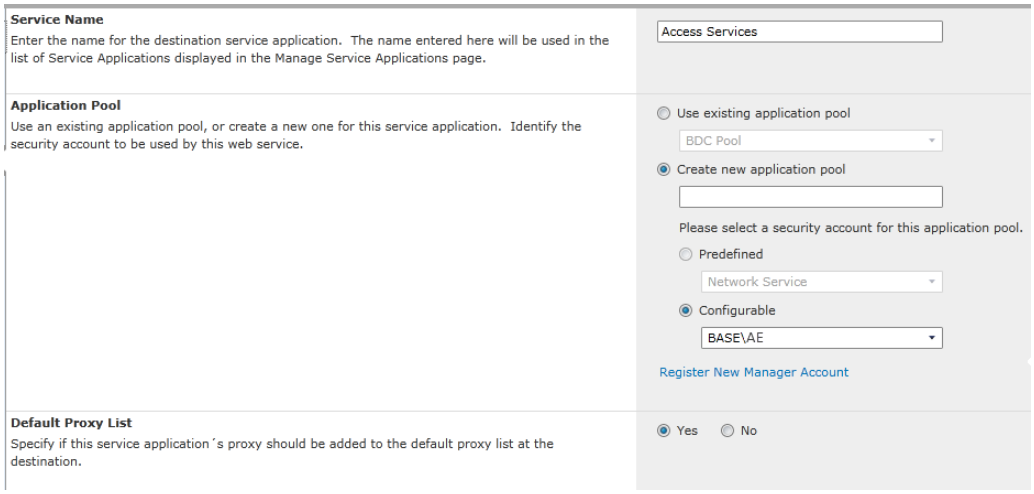


Figure 60: Access Services 2010 Web Service Application (SharePoint 2013)/Access Service Web Service Application (SharePoint 2010) settings.

- **Access Services Web Service Application** (SharePoint 2013) – Configure the following settings for the SharePoint 2013 Access Service Web Service Application:
    - **Database Server –** Enter the database server for this service application and configure the access credentials. We recommend you use Windows authentication. If you want to use the SQL authentication, enter the credential to access the database server.

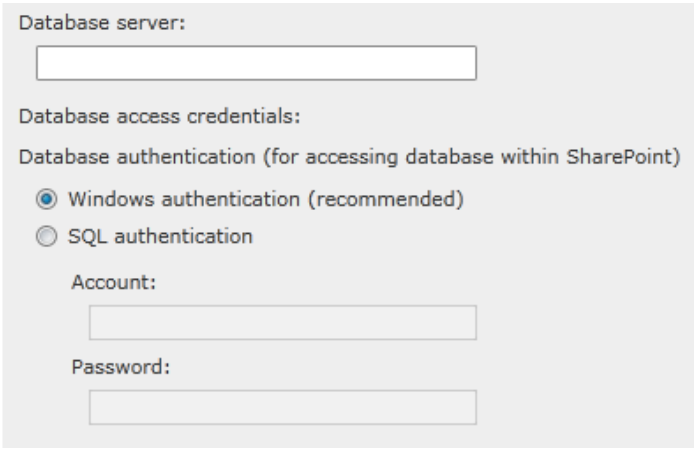


Figure 61: Access Services Web Service Application (SharePoint 2013) settings.

- **Secure Store Service** – Configure the following settings for this service application.
    - **Database** – Configure the settings of the database used by this service application. Click **Details** to view the detailed configuration.
    - **Failover Database Server** – Configure a failover database server for this service application. The failover SQL Server instance entered here must be an existing instance, and the destination Agent account must have access to this instance.

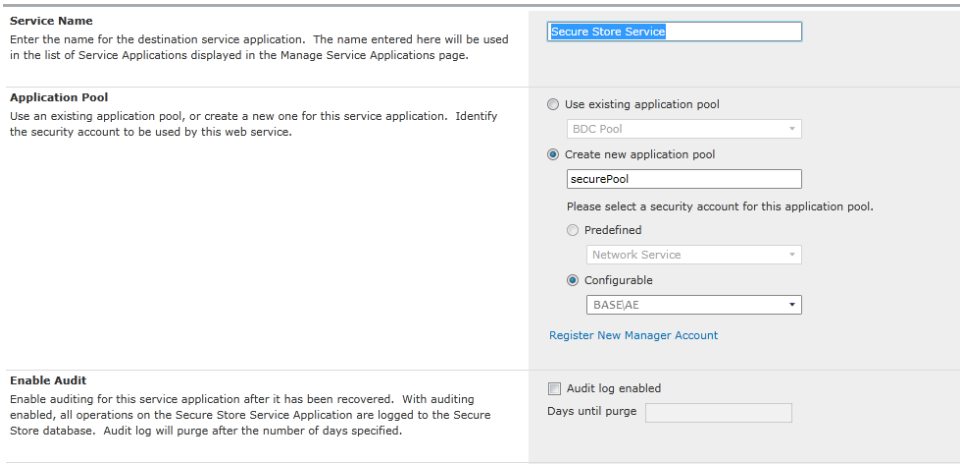


Figure 62: Secure Store Service Application settings.

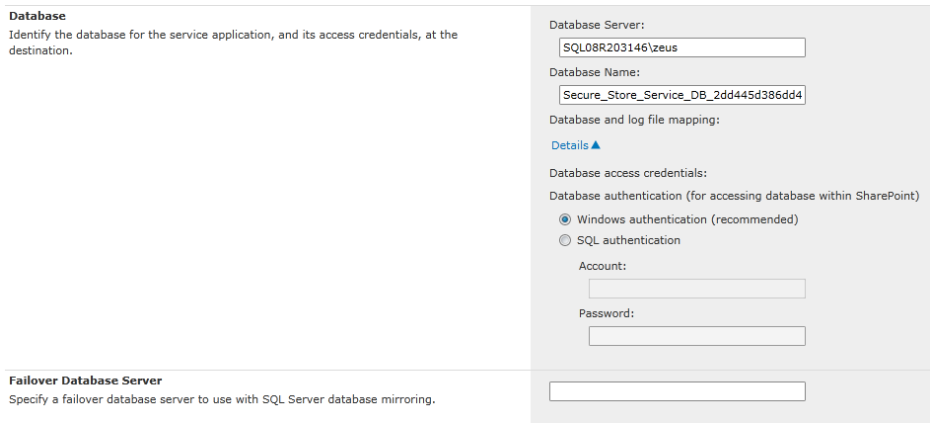


Figure 63: Secure Store Service Application settings.

Configure the same settings for other service applications according to the detailed information above.

- **PerformancePoint Service Application**

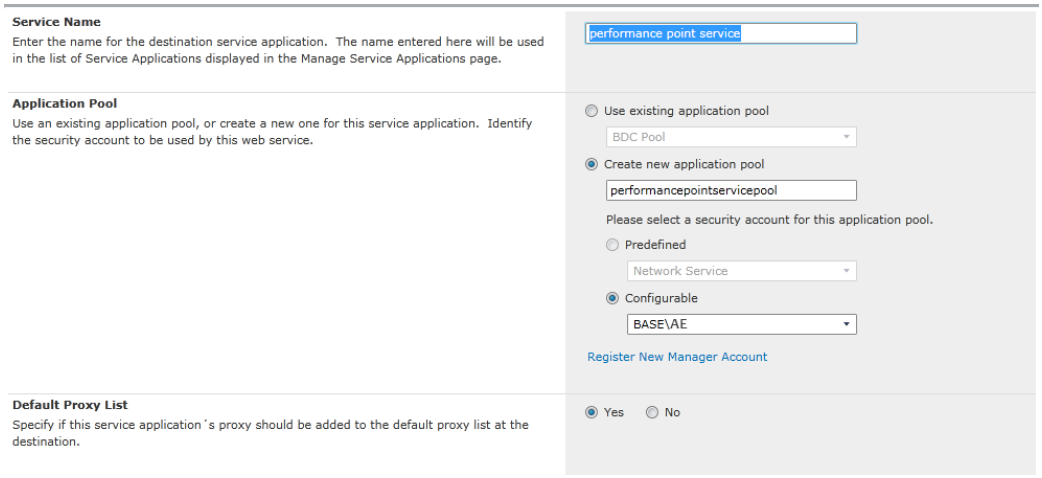


Figure 64: PerformancePoint Service Application settings.

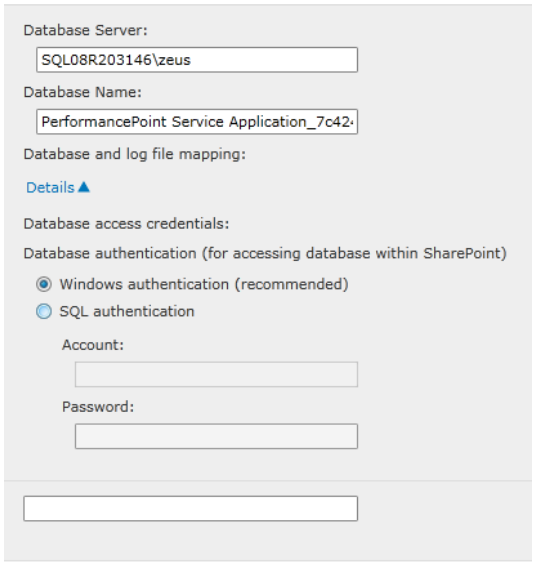


Figure 65: PerformancePoint Service Application settings.

- **Project Service Application** (SharePoint 2010) – To out of place restore the Project Service Application, make sure that the Project Server is properly configured and installed in the destination farm.

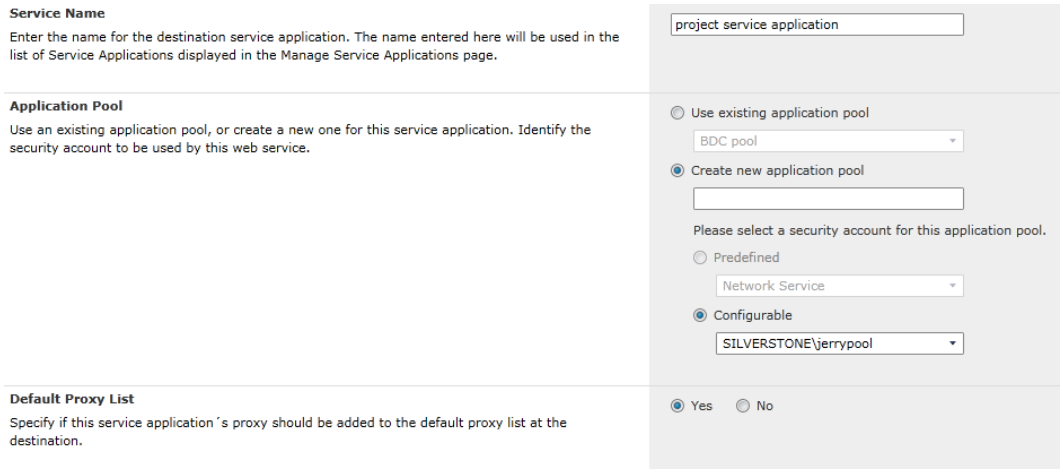


Figure 66: Project Service Application (SharePoint 2010) settings.

- **Project Service Application** (SharePoint 2013) – To out of place restore the Project Service Application, make sure that the Project Server is properly configured and installed in the destination farm.

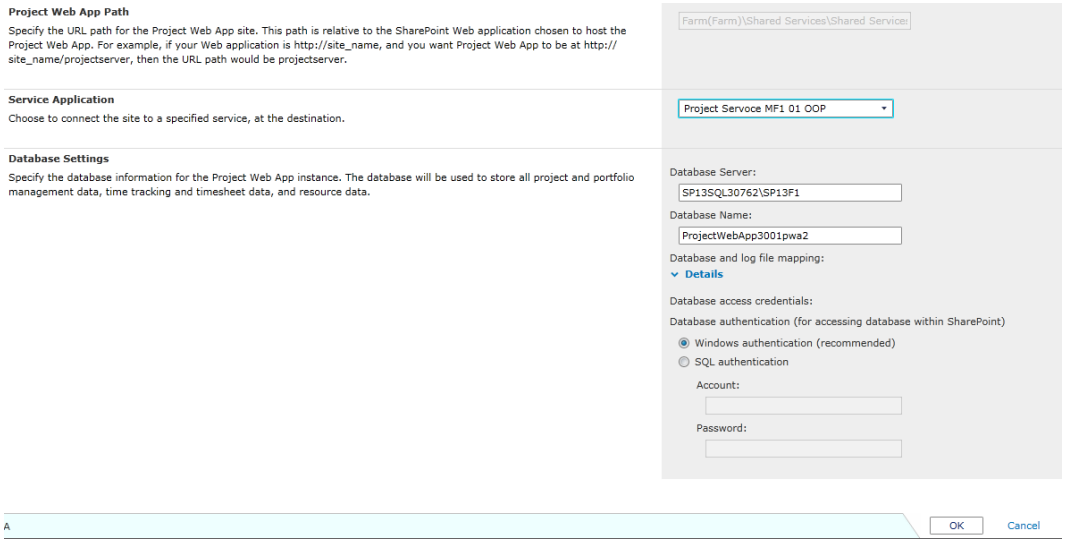


Figure 67: Project Service Application (SharePoint 2013) settings.

- **PowerPoint Service Application (Only in SharePoint 2010)**

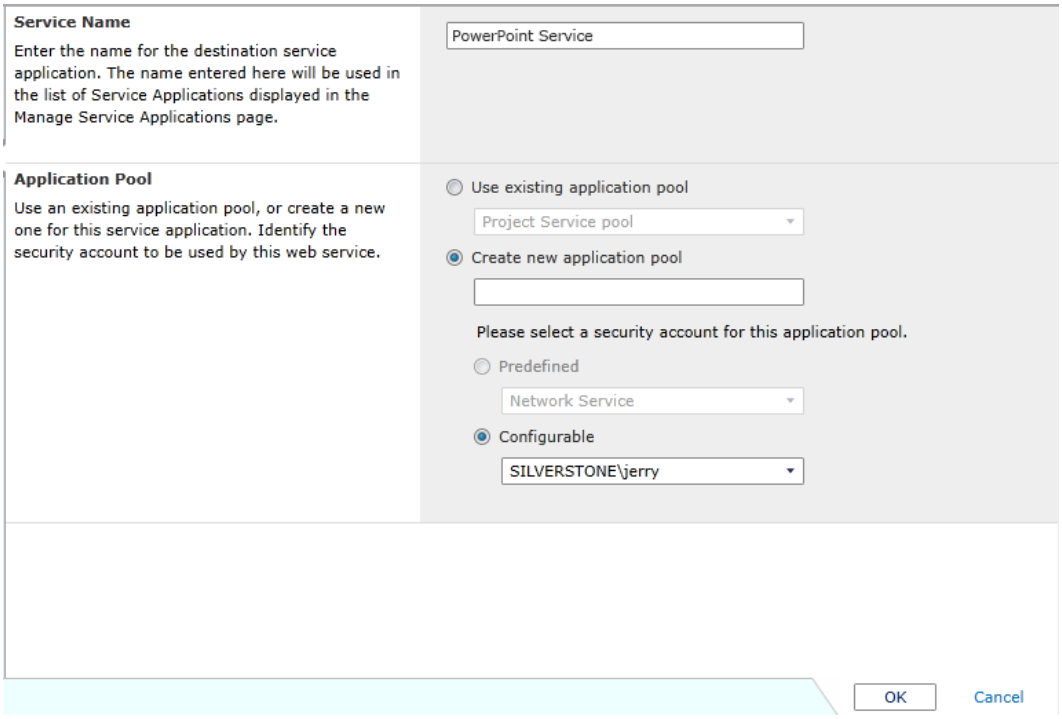


Figure 68: PowerPoint Service Application Settings.

- **Visio Graphics Service**

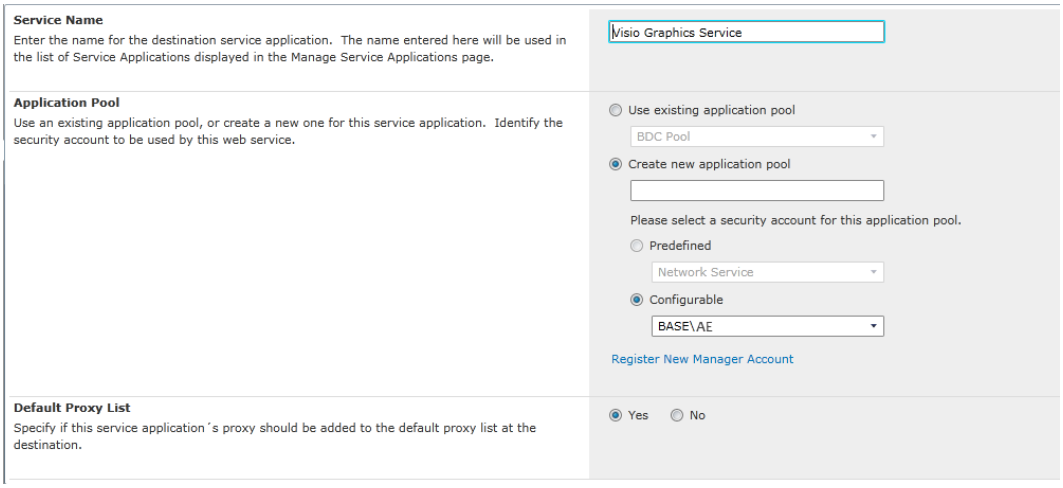


Figure 69: Visio Graphics Service Application settings.

- **Managed Metadata Service**

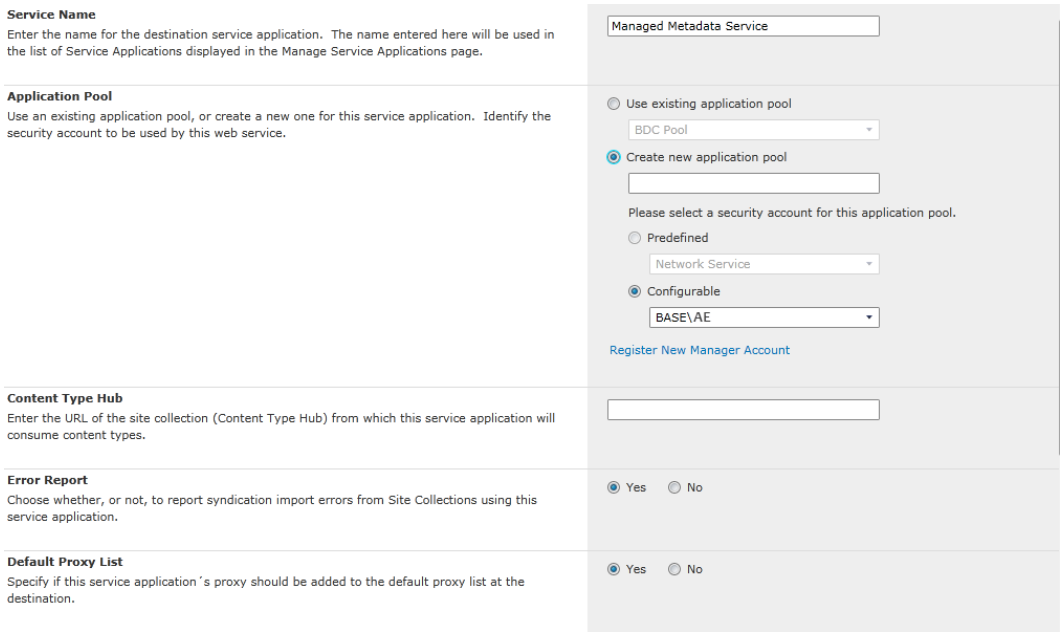


Figure 70: Managed Metadata Service Application settings.

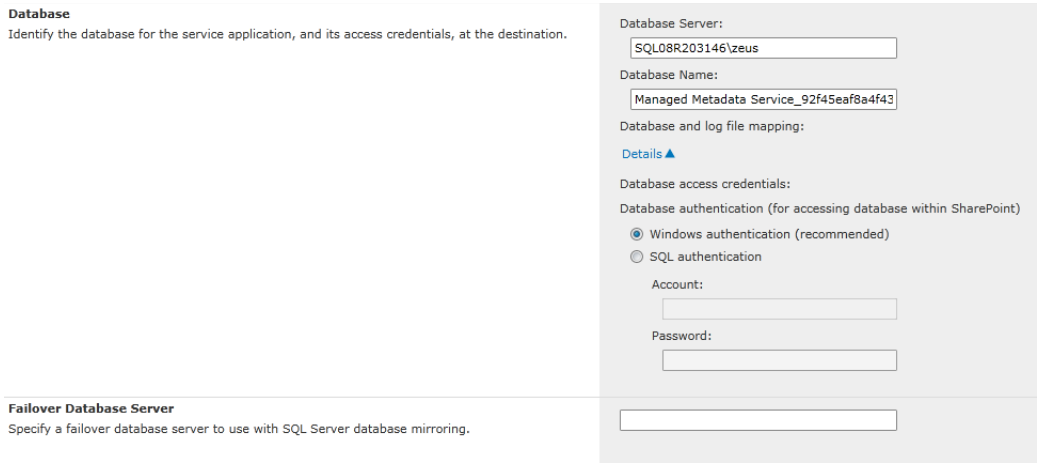


Figure 71: Managed Metadata Service Application settings.

- **Web Analytics Service Application**

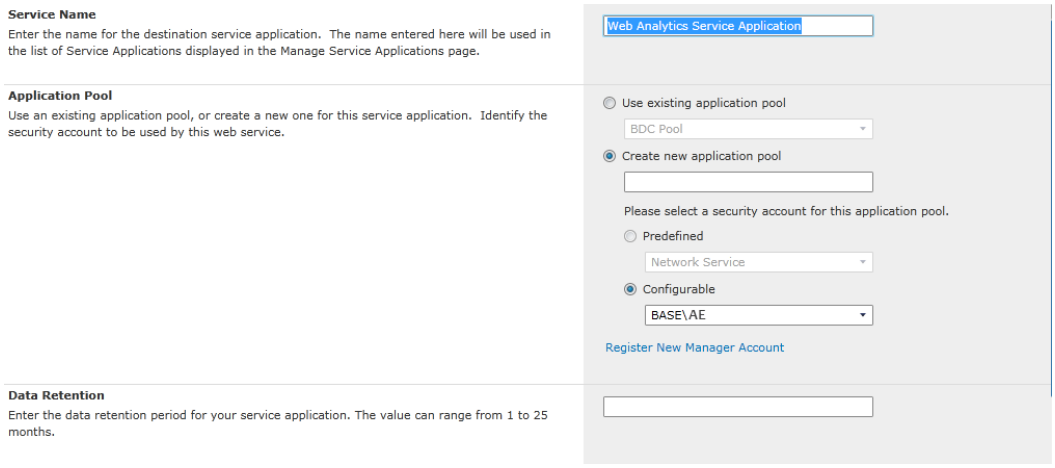


Figure 72: Web Analytics Service Application settings.

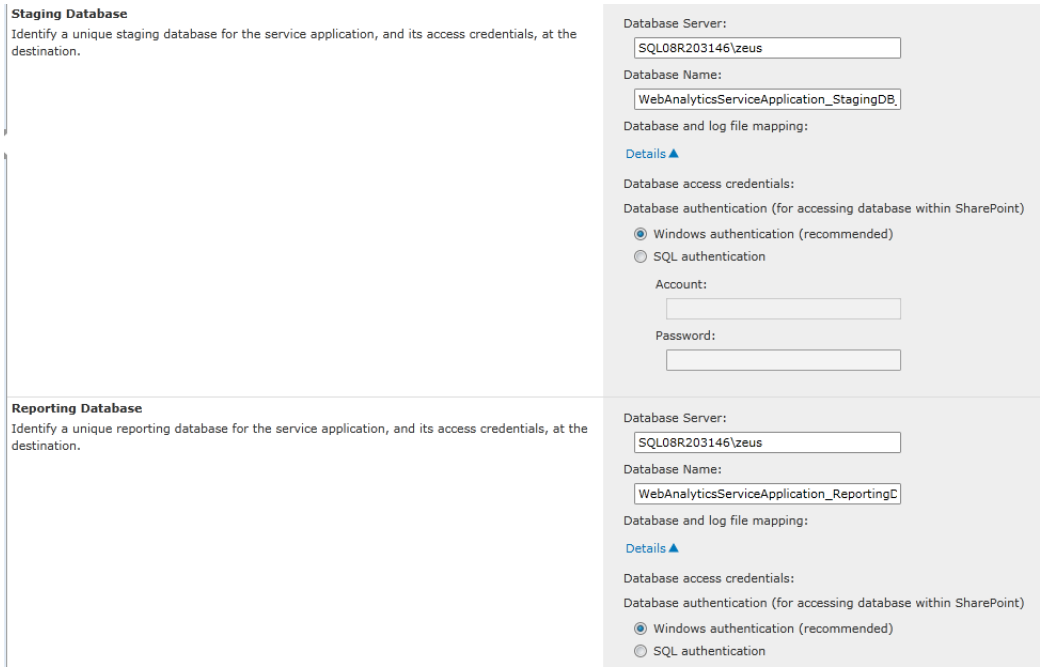


Figure 73: Web Analytics Service Application settings.

- **Excel Services Application**

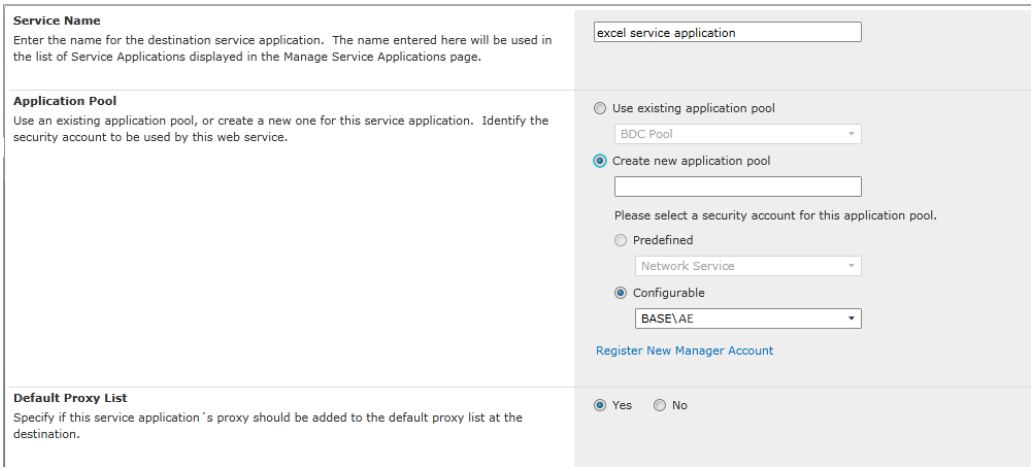


Figure 74: Excel Services Application settings.

- **Word Automation Services**

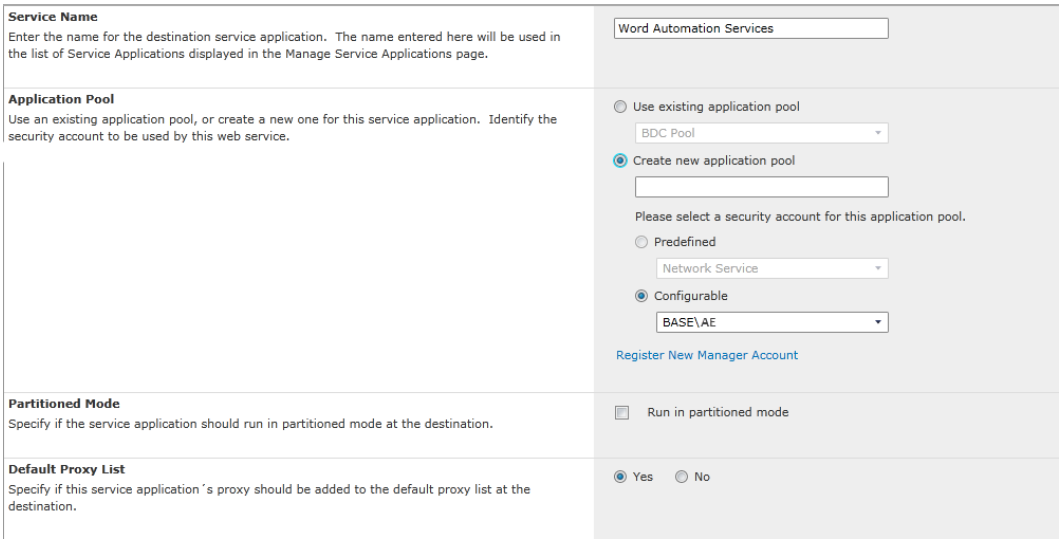


Figure 75: Word Automation Services settings.

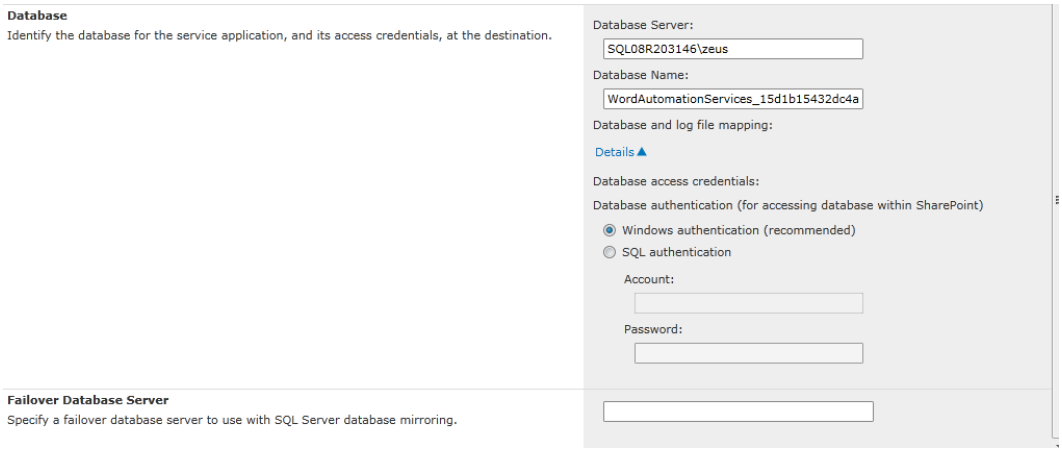


Figure 76: Word Automation Services settings.

- **App Management Service Application** (SharePoint 2013)

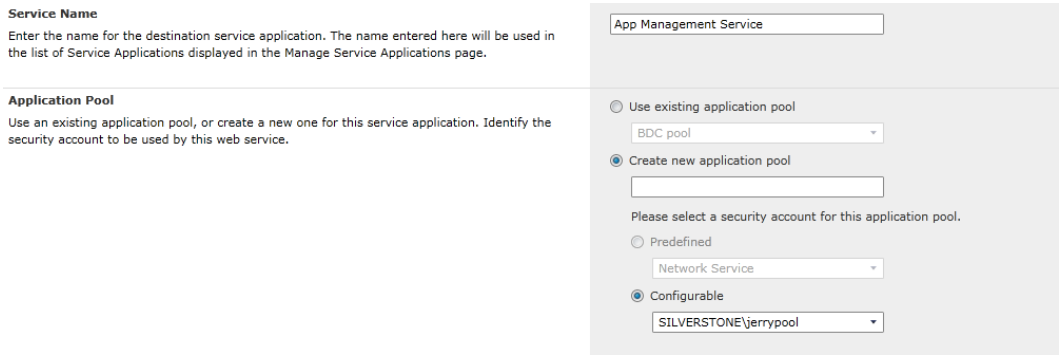


Figure 77: App Management Service Application settings.

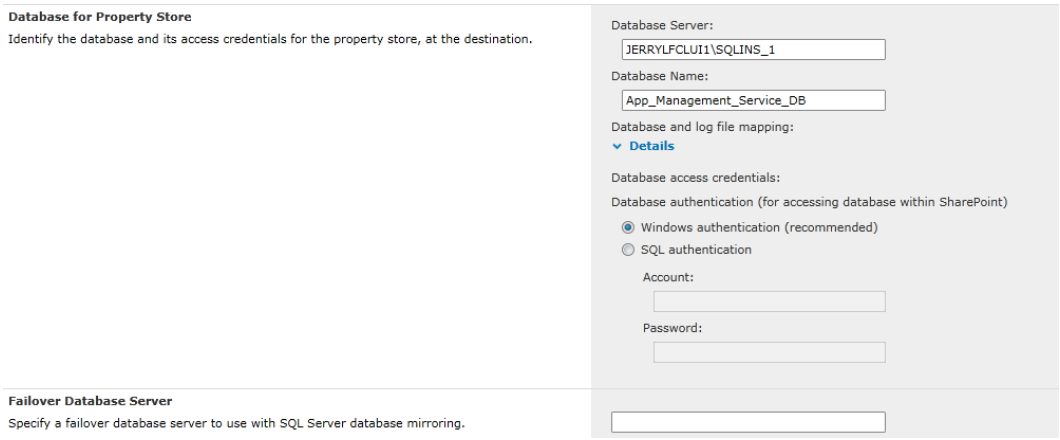


Figure 78: App Management Service Application settings.

- **User Profile Service Application** – Configure the following settings for this service application.
    - **Profile Synchronization Instance** – Select the machine in the destination farm where you wish to run the Profile Synchronization process. If the User Profile Synchronization Service is not started on the specified server, after the out of place platform restore, this service will remain not started on the specified server. If you do not enter a server in this field, by default, the destination Central Administration server will be used to run the Profile Synchronization process.
    - **My Site Host URL and My Site Managed Path** – You can choose to enter the desired configuration here or configure the corresponding settings in the destination SharePoint Central Administration after the out of place platform restore completes.

      ***Note**: Make sure you have configured the **My Site Host URL** and **My Site Managed Path** correctly before configuring the **Site Naming Format**, because the **Site Naming Format** can only be restored when the **My Site Host URL** and **My Site Managed Path** are properly configured.

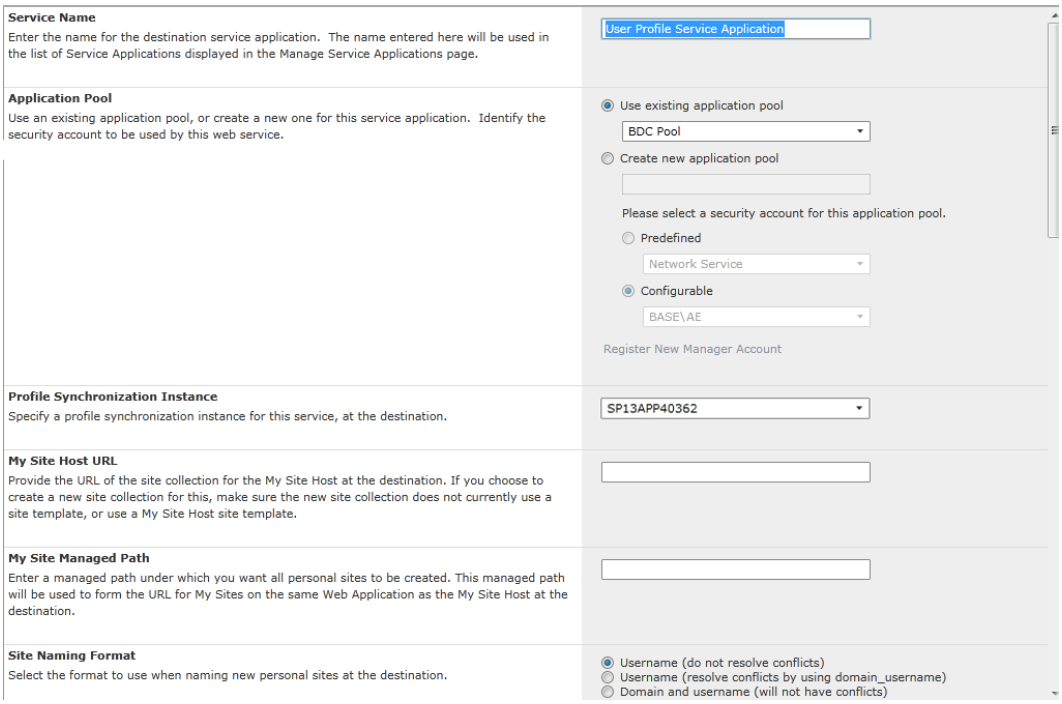


Figure 79: User Profile Service Application settings.

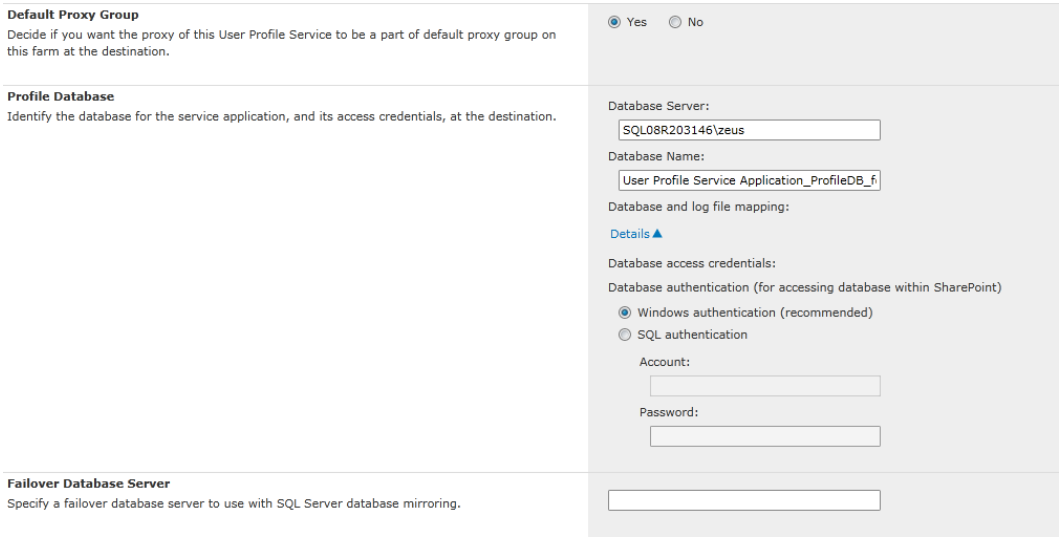


Figure 80: User Profile Service Application settings.

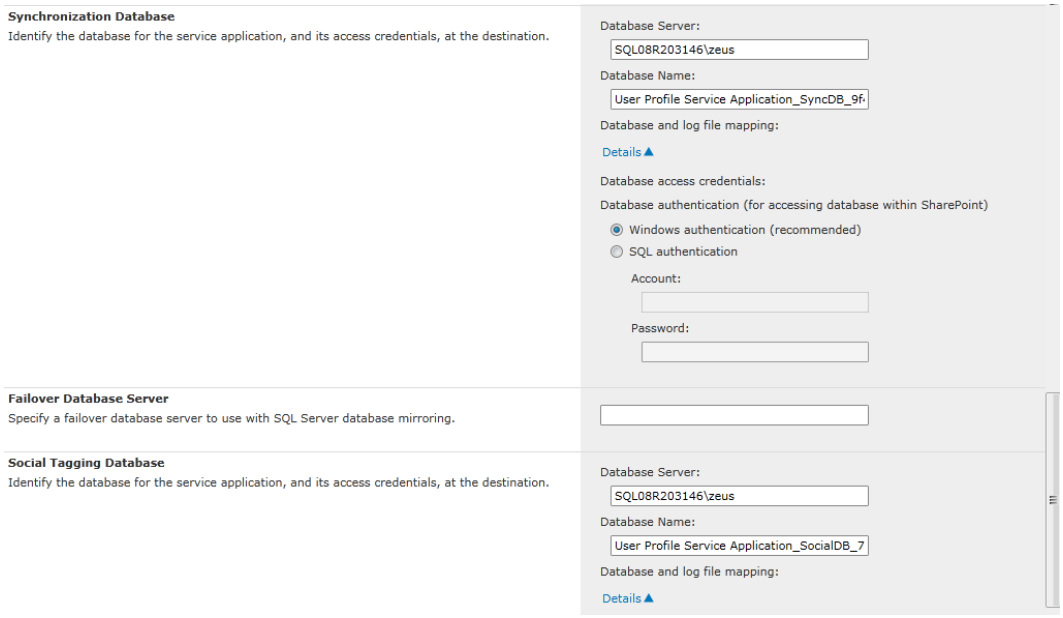


Figure 81: User Profile Service Application settings.

- **Business Data Connectivity Service**

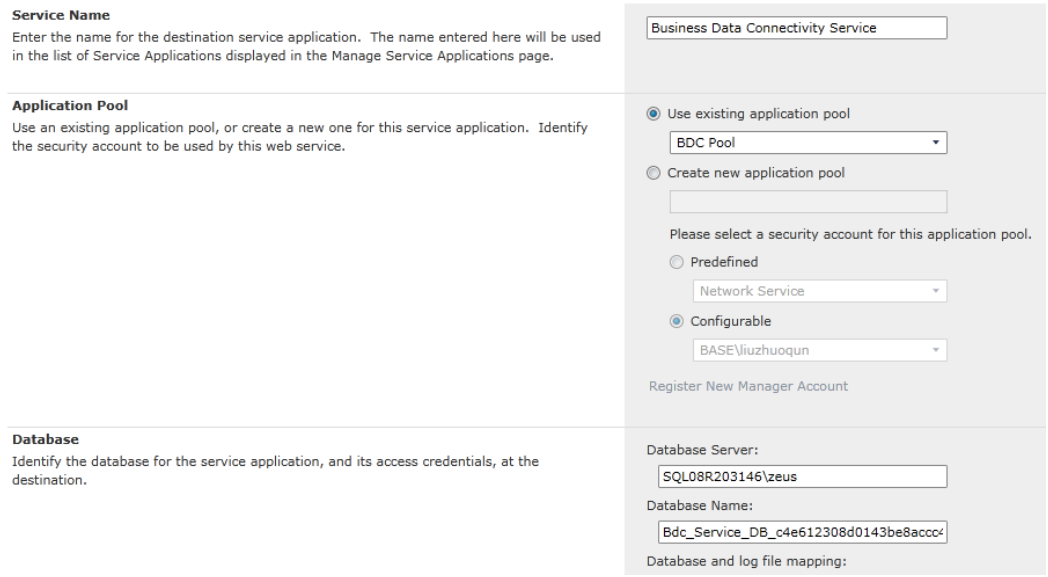


Figure 82: Business Data Connectivity Service settings.

- **Search Service Application** (SharePoint 2010) – Configure the following settings for this service application. You can configure the servers where you want to host the search admin component, crawl component and search query component in the corresponding **Server** drop-down list; all the SharePoint servers where the corresponding component can be hosted will be listed in the corresponding **Server** drop-down list. After the out of place platform restore, the **SharePoint Server Search** service will be enabled on the specified servers automatically.

***Note**: If you choose to create a new application pool, the application pool used for Search Admin Web Service and the application pool used for Search Query and Site Settings Web Service must be different.

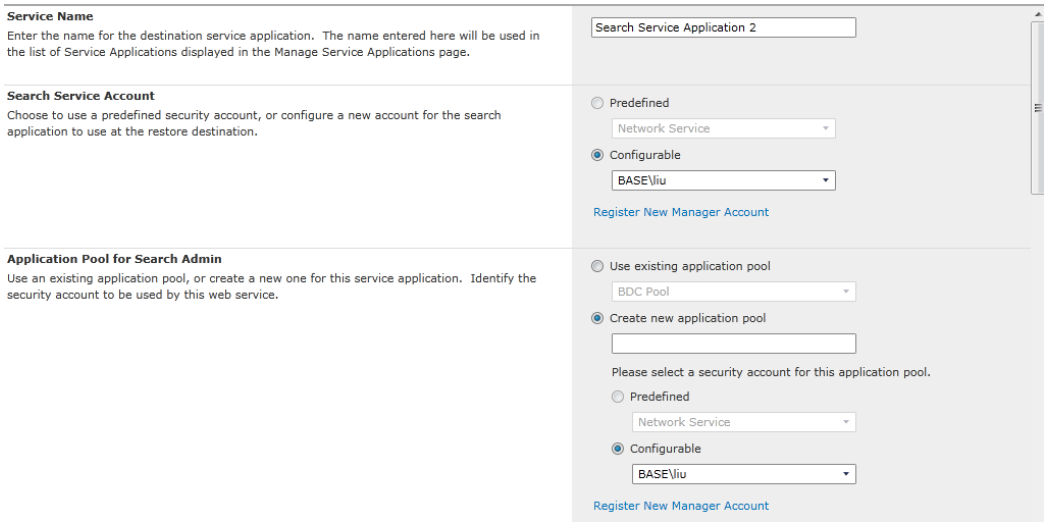


Figure 83: Search Service Application settings.

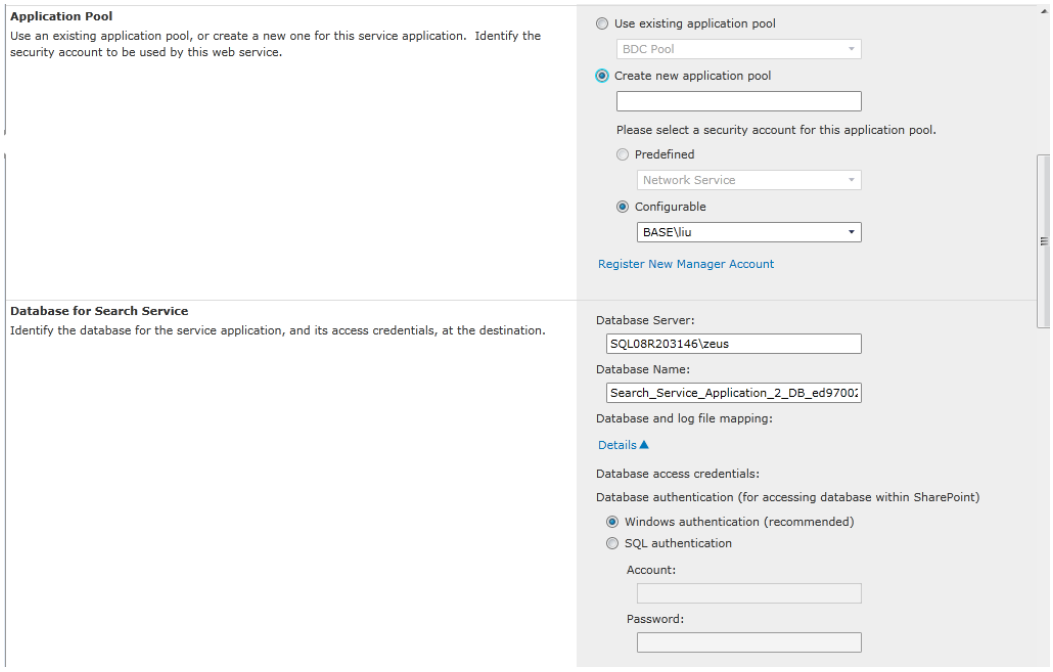


Figure 84: Search Service Application settings.

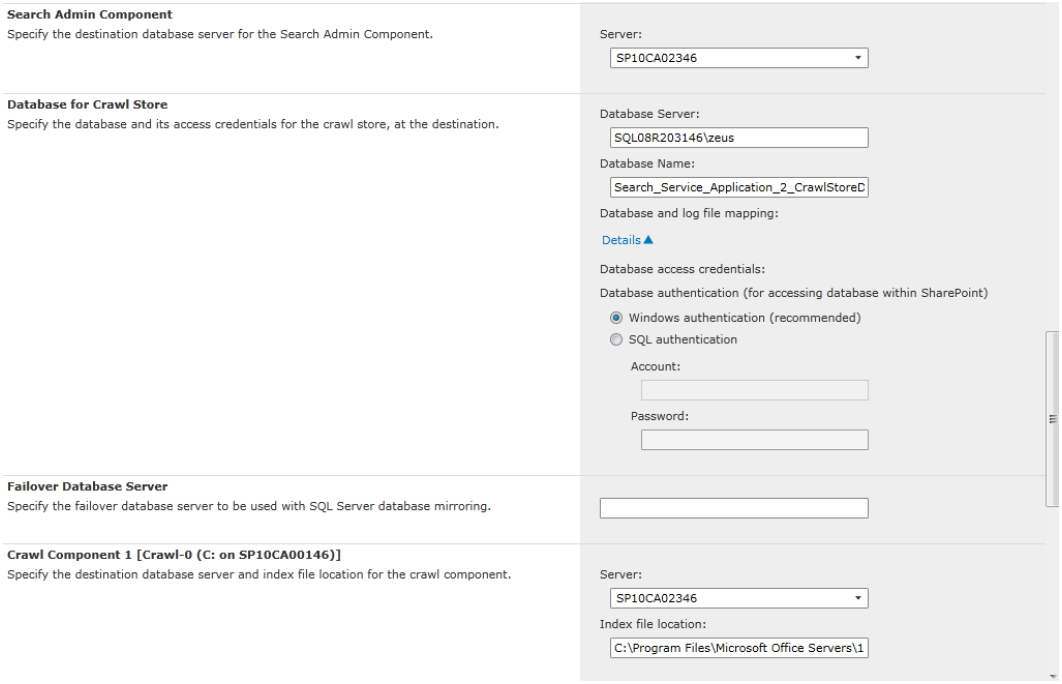


Figure 85: Search Service Application settings.

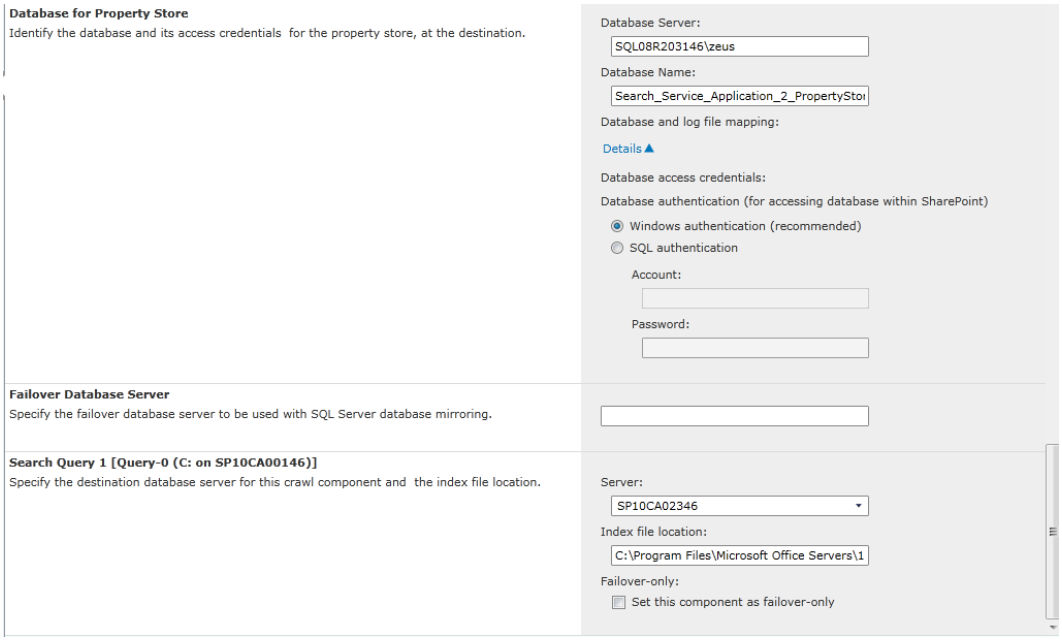


Figure 86: Search Service Application settings.

- **Search Service Application** (SharePoint 2013) – Configure the following settings for the SharePoint 2013 Search Service Application. After the out of place platform restore, the **SharePoint Server Search** service will be enabled on the specified servers automatically.

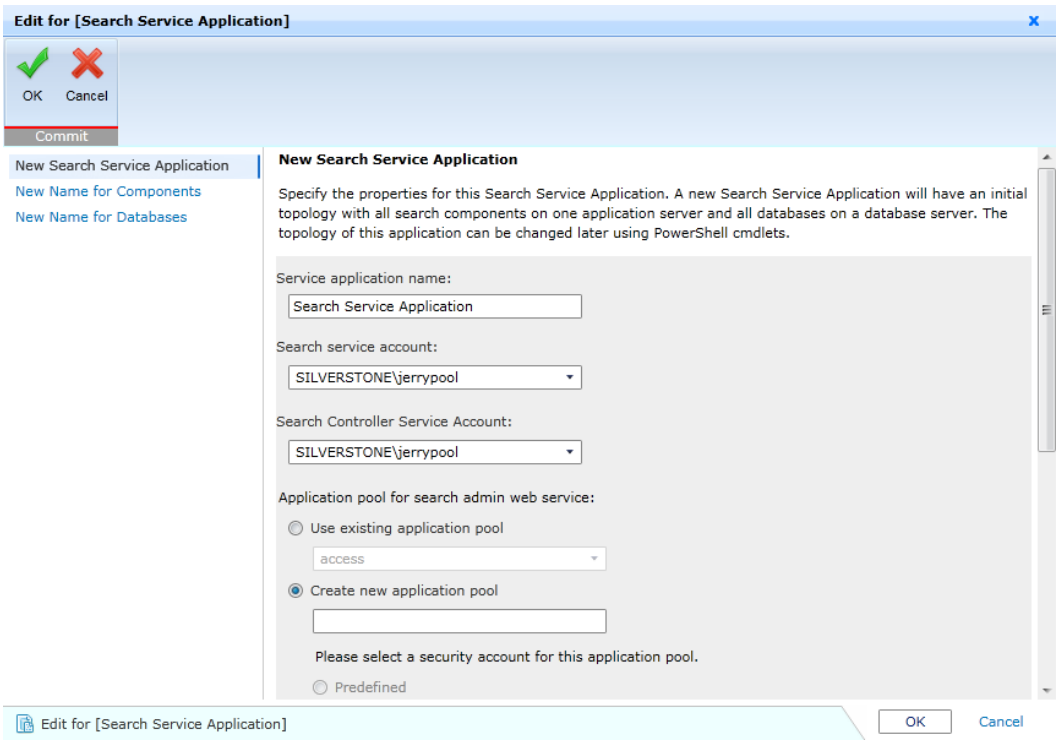


Figure 87: Search Service Application Settings.

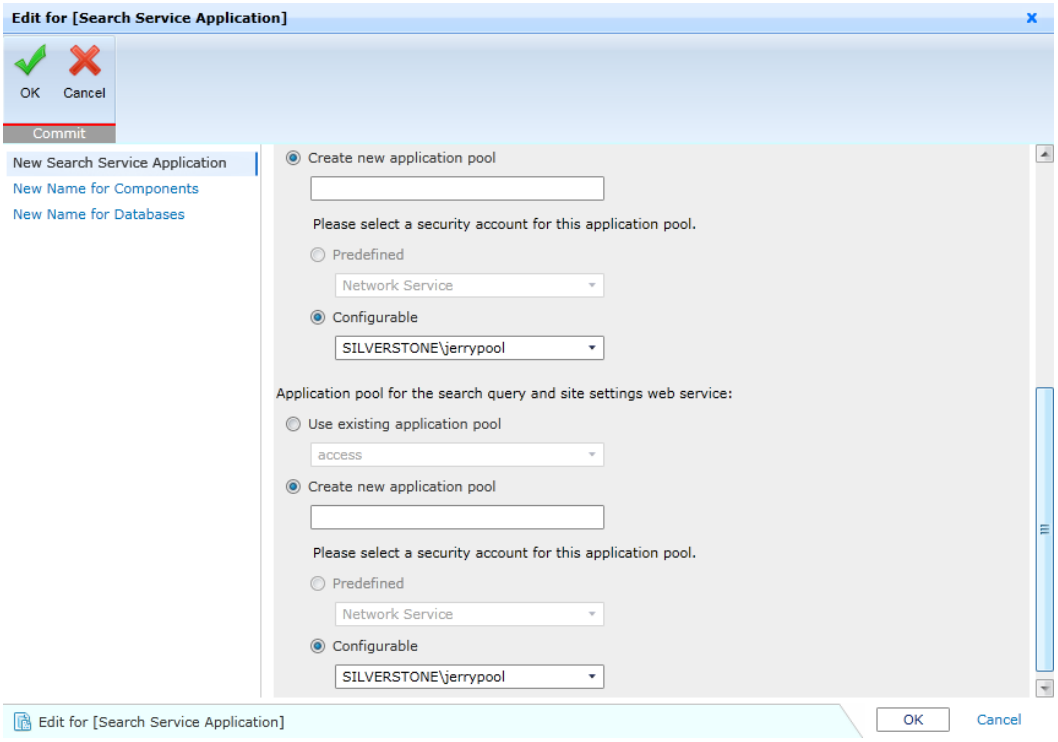


Figure 88: Search Service Application Settings.

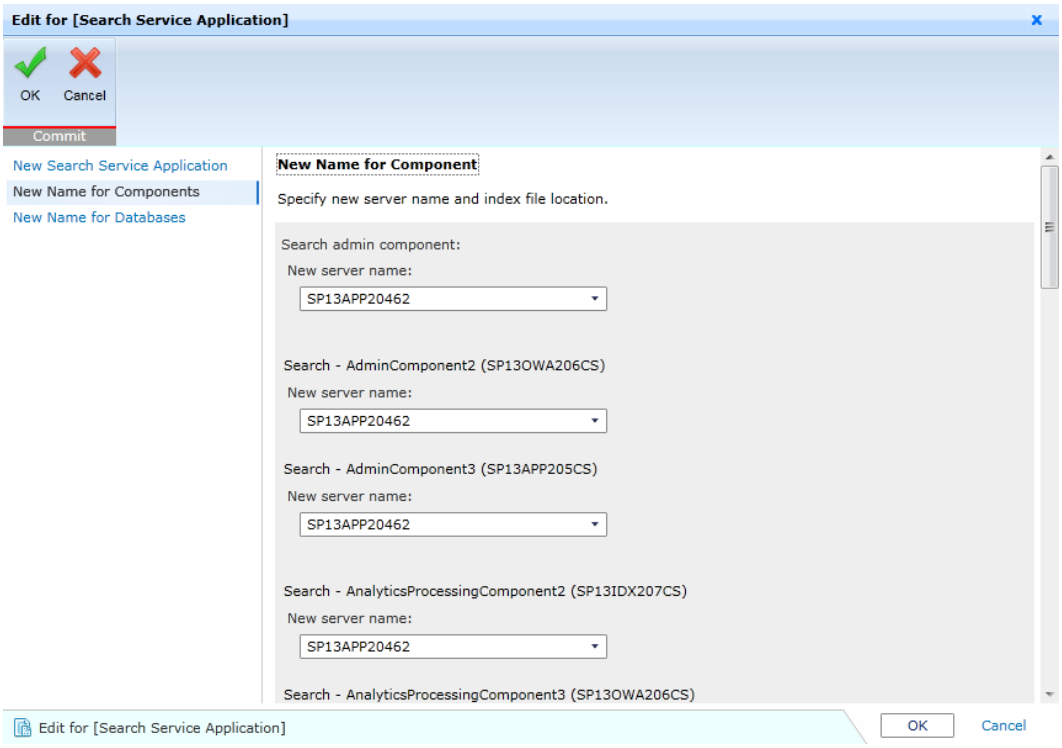


Figure 89: Search Service Application Settings.

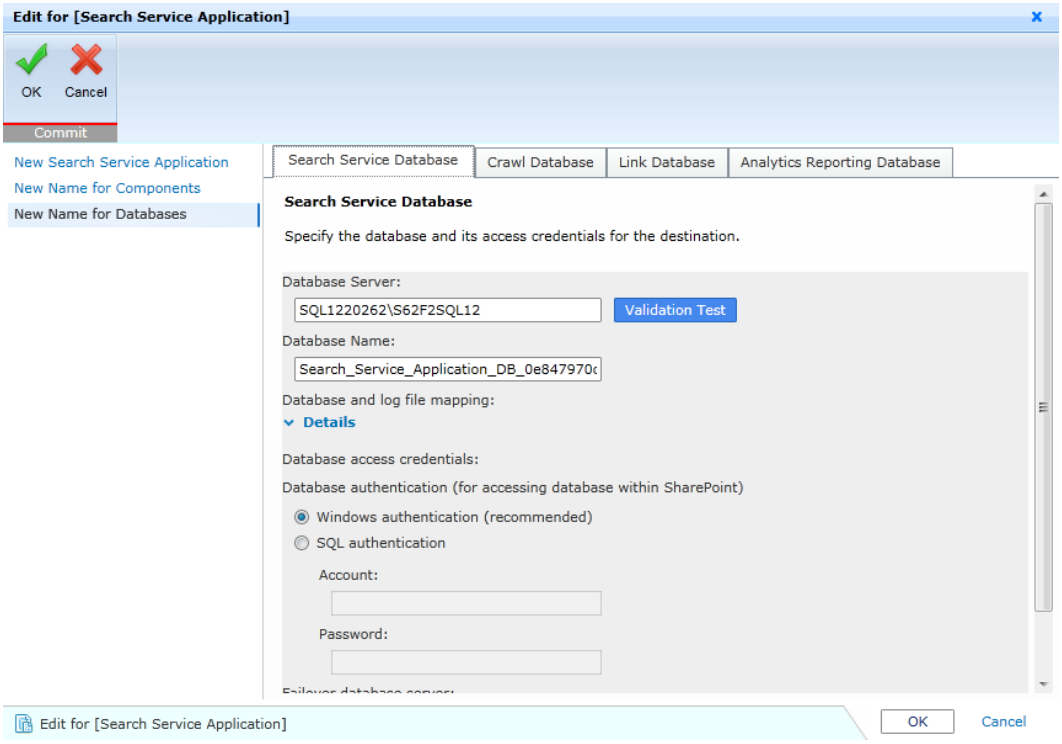


Figure 90: Search Service Application Settings.

- **Word Viewing Service Application**

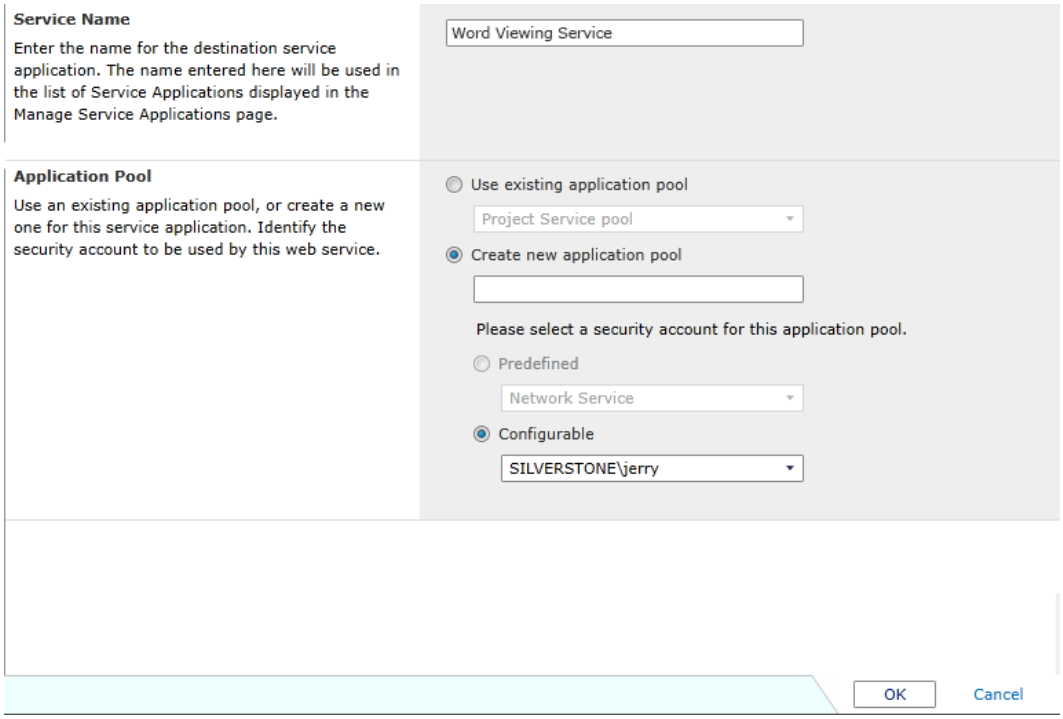


Figure 91: Word View Service Application Settings.

- **SQL Server Reporting Services (SSRS)** – Make sure the Reporting Service add-in has been installed on all of your Web front-end servers. Otherwise, you cannot load the backup data tree to restore the SQL Server Reporting Services. The restoration of SQL Server Reporting Services for SQL Server 2012 SP1 or later will fail if the Windows user profile of your Agent account is a temporary user profile. If you have registered your Agent account and its user profile is a temporary user profile, delete the user profile and then restore the SQL Server Reporting Services again. If you did not register your Agent

account, use the Agent account to log into the current server. The operating system will create a user profile for your Agent account automatically.

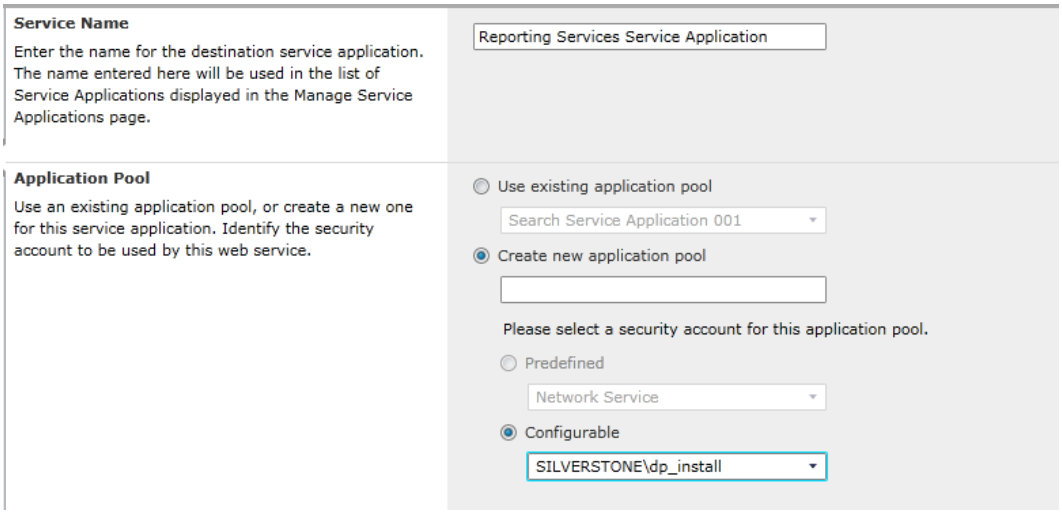


Figure 92: SQL Server Reporting Service settings.

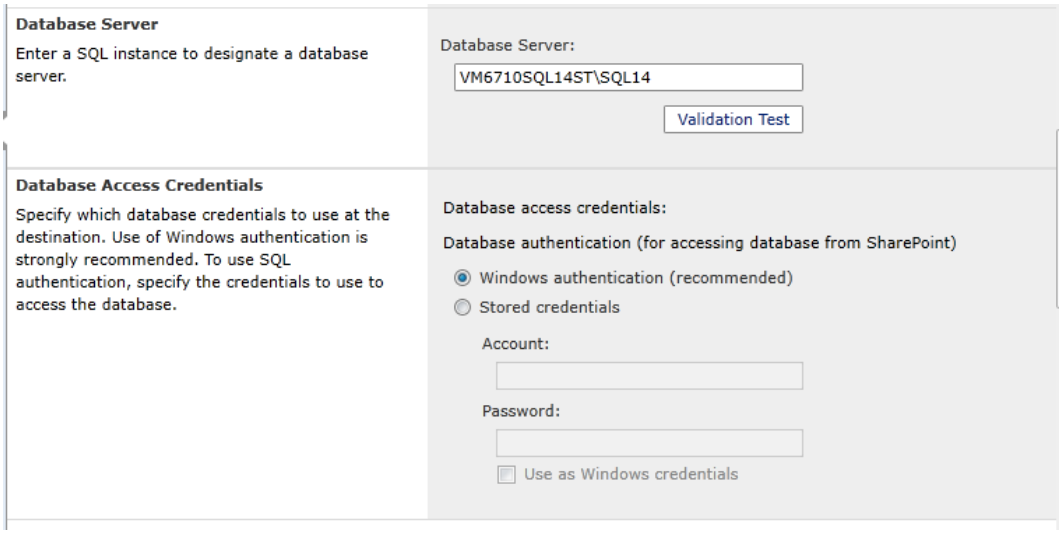


Figure 93: SQL Server Reporting Service settings.

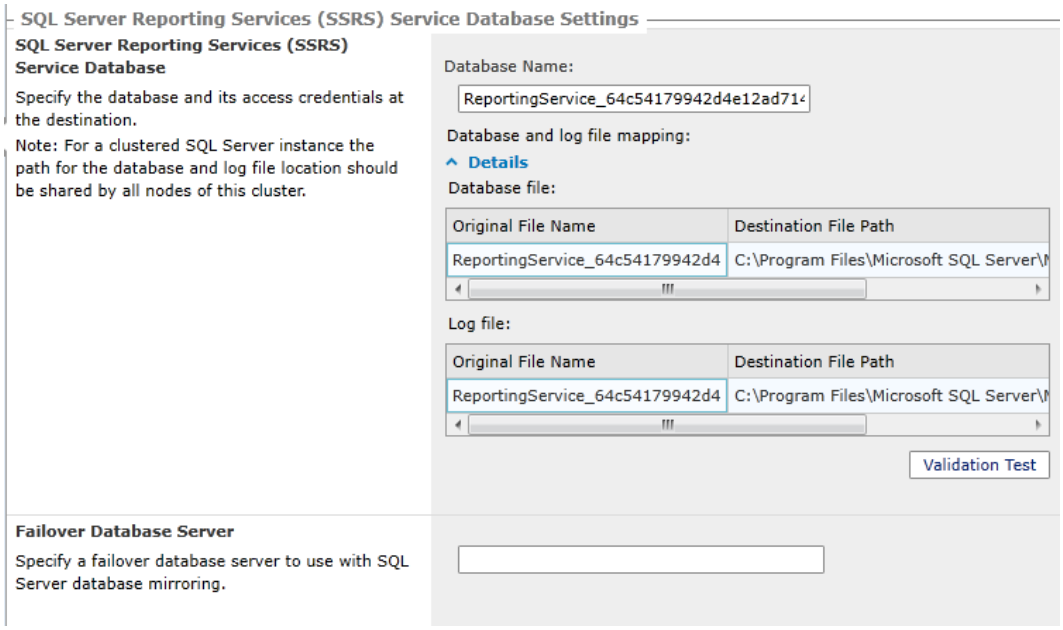


Figure 94: SQL Server Reporting Service settings.

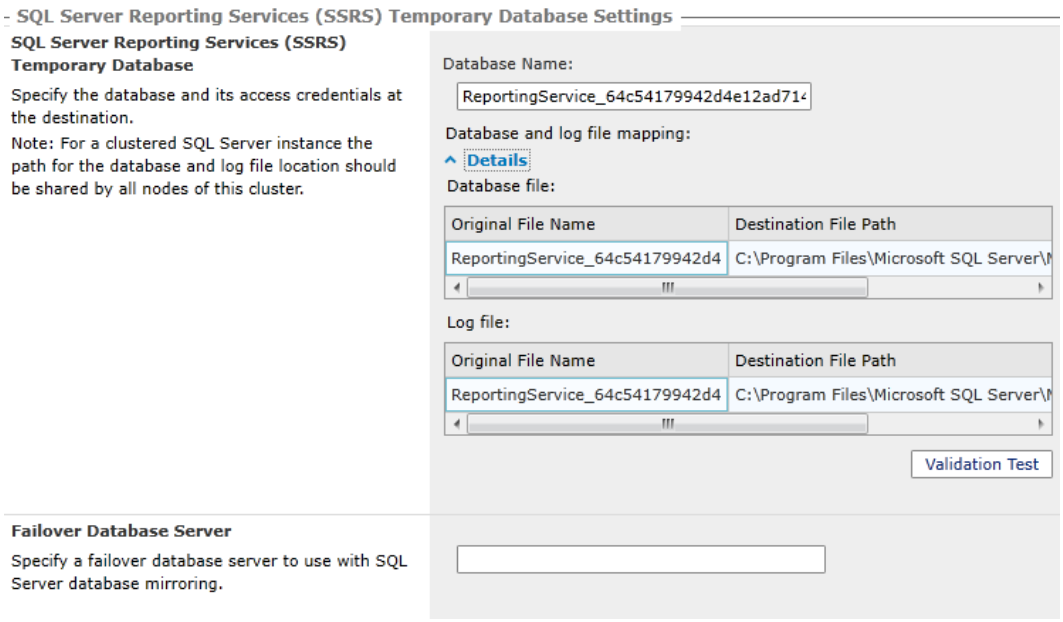


Figure 95: SQL Server Reporting Service settings.

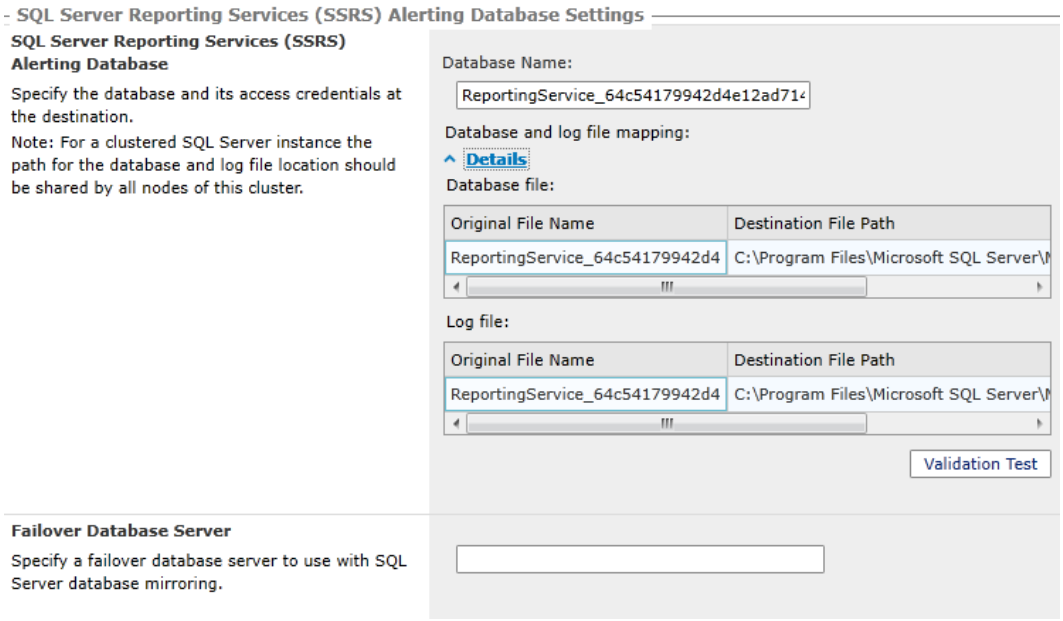


Figure 96: SQL Server Reporting Service settings.

- **SQL Server PowerPivot Service** (For SharePoint 2010 and SharePoint 2013) – To restore the SQL Server PowerPivot Service for SharePoint 2013, make sure that PowerPivot for SharePoint 2013 is installed on each server in the SharePoint 2013 farm.

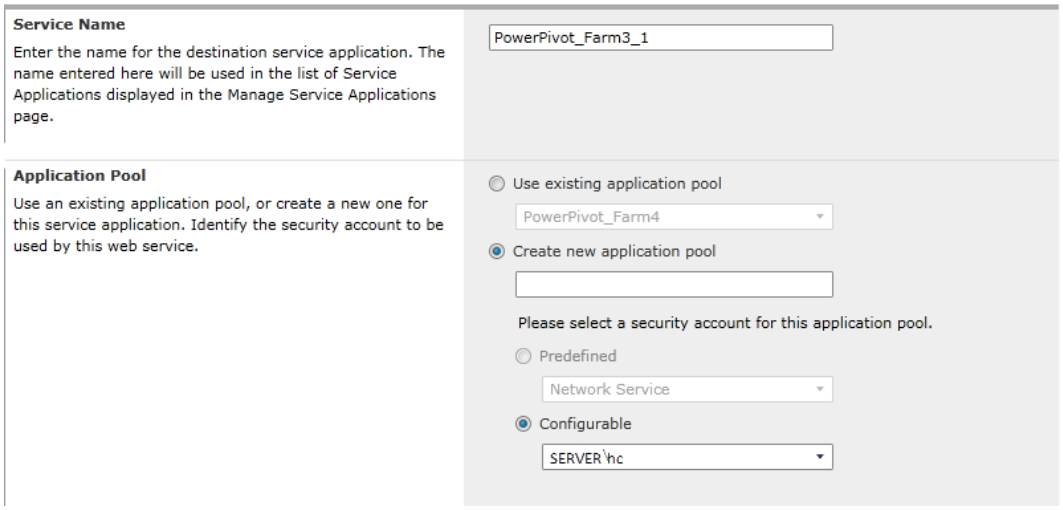


Figure 97: SQL Server PowerPivot Service settings.

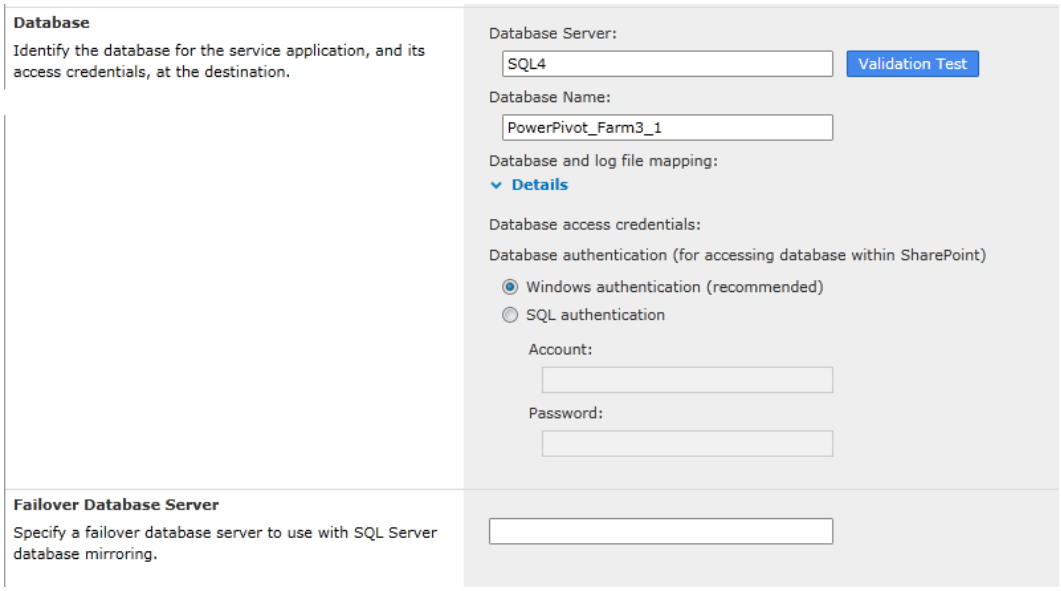


Figure 98: SQL Server PowerPivot Service settings.

After you finish the service application configuration, click **OK** to save the configuration and then 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 an Out of Place 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 specified **Start time** that you configure. For the detailed explanation of each option, refer to Building an Out of Place 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 job.

Helpful Notes When Restoring the Proxies of the Service Applications

- When restoring the service application proxies, configure the following settings:
  - **Proxy Name** — After the out of place platform restore, the restored proxy will be named using the name entered here.
  - **Service Application** — After the out of place platform restore, the restored proxy will be connected to the service application specified here.

- **Default Proxy List** — Choose whether to add this proxy to the default proxy list in the destination farm.

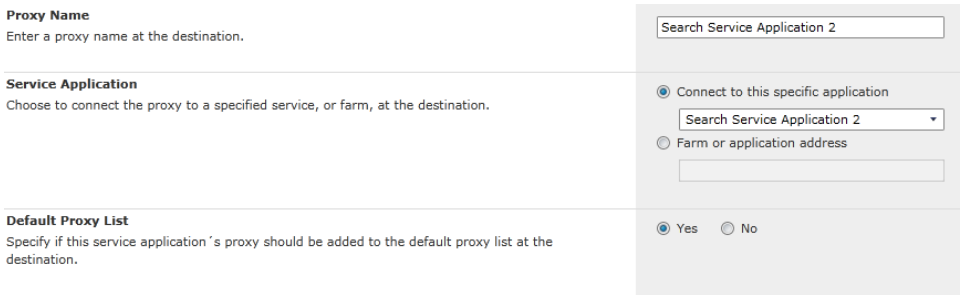


Figure 99: Proxy settings.

- If you want to restore **Business Data Connectivity Service/PerformancePoint Service Application** separately, make sure the **Secure Store Service** is restored to the destination farm first (using the original **Secure Store Service** name). This is because the **Business Data Connectivity Service** and **PerformancePoint Service Application** are associated with the **Secure Store Service**, and they need the original **Secure Store Service** name to find the restored **Secure Store Service** in the destination farm.

Restoring Backed up Web Front-End Servers Data

1. In the Data Selection page, click the farm node in the **Backup Data** area to load the tree. After the tree is loaded, find the **Web Front-End Servers** node on the tree, and then select the Web front-end servers' data you want to restore.

   ***Note**: DocAve does not recommend performing the Platform out of place restore job to restore the IIS site of SharePoint Central Administration.

   ***Note:** When selecting multiple nodes in the red box displayed in the following screenshot, only **In place restore** can be performed

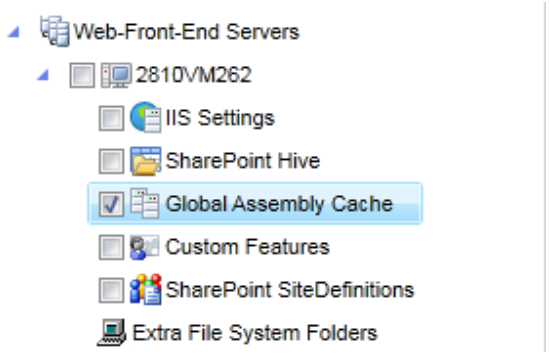


Figure 100: Selected nodes on the tree.

2. Click the **Next** button at the bottom right corner to go to the Restore Type page. Select **Out of place restore** as the restore type and select one destination Agent from the appeared **Destination Agent** drop-down list. Then click the displayed destination Agent node to load the location where you want to restore the data selected in the previous step.

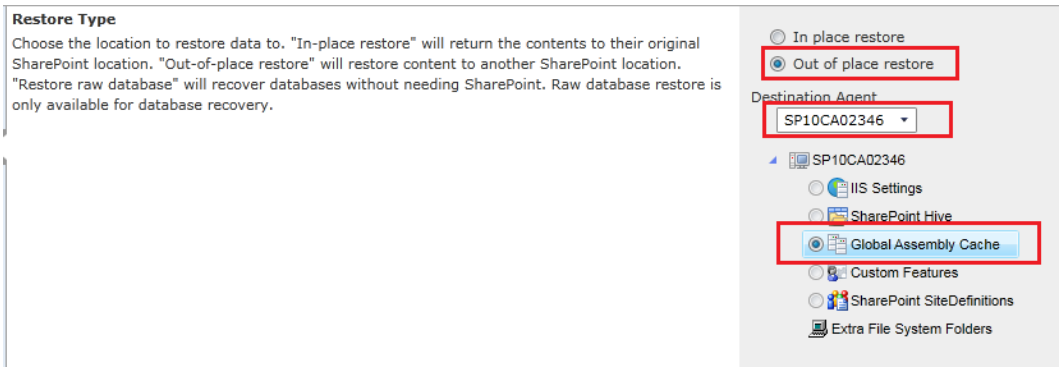


Figure 101: Configure the Restore Type field.

3. Click the **Next** button at the bottom right corner to go to the Restore Settings page.

   In the Restore Settings page, configure the options according to your requirements. For the detailed explanation of each option, refer to the Building an Out of Place 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.

4. 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 specified **Start time** that you configure. For the detailed explanation of each option, refer Building an Out of Place 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.

5. 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 job.

***Note**: When restoring the backed up extra file system folders, you can choose to create a new folder in the destination and then restore the backup data to the created folder.

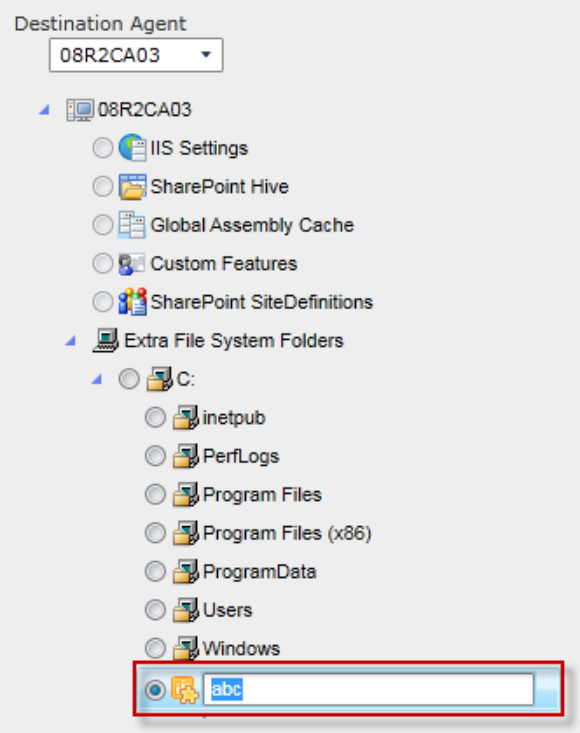


Figure 102: Restore to a manually inputted file system folder.

DocAve 6 Platform Backup and Restore Use Case

Core content is the most significant asset within a SharePoint deployment, as it represents intellectual property critical to an organization's operations. Equally important, however, is the underlying infrastructure of the SharePoint deployment, which consists of many platform-level components coupled tightly together to create a working environment. Since there are so many critical components in a SharePoint platform, a failure of any one component could adversely affect the entire environment.

The SharePoint administrator, Mackenzie, is facing a situation in which his organization's SharePoint deployment incurs a catastrophic failure. Mackenzie is now faced with the task of restoring his organization's entire SharePoint environment.

Backing up the Entire SharePoint Farm

Prior to the SharePoint farm going down, Mackenzie had created and run scheduled Incremental backup jobs:

- Mackenzie selected the entire farm to back up and selected the **Include New** checkbox to ensure that newly created objects are backed up.
- Mackenzie chose to Use DocAve Platform Backup and Restore as the only backup method for SharePoint databases, and selected Perform log backup after full backup to ensure that the log file is truncated after the Incremental backup.
- Since the scheduled Incremental jobs were run during off-business hours, Mackenzie chose not to **Create Persistent Snapshots**.

Restoring the Platform

As a result of the catastrophic SharePoint farm failure, Mackenzie must now recover the entire farm using a platform-level backup. In order to do so, there are some notable prerequisites:

- Windows Server 2008 or Windows Server 2008 with Service Pack 2
- IIS with ASP.NET enabled
- NET Framework 3.0
- Microsoft SharePoint Server 2010 installed but not configured (if an existing farm already has Web front-end servers deployed, they should all be disconnected through the SharePoint Products and Technologies Configuration Wizard)
- SharePoint patch level should remain the same
- Server names and topology should remain the same
- SQL Server disk layout should remain the same
- The same Domain account for SharePoint administration should be used.

With these prerequisites satisfied, Mackenzie can now recover the farm by simply loading the appropriate platform backup through the DocAve Restore interface. Due to dependencies between various elements of the SharePoint farm, this restoration process is usually a multi-step procedure. Before any Web front-end servers can be attached, Mackenzie must first restore the configuration database and the Central Administration databases.

After completing this, Mackenzie can bring the Web front-end servers online and connect them to the restored configuration database using the SharePoint configuration wizard. It is important to keep in mind that one of these Web front-end servers should host the central administration Web application.

After the Web front-end servers are online, Mackenzie can restore additional farm-level components. These include any IIS (for example, SSL or forms-based authentication, web.config) customizations, custom solutions, or Shared Services Applications for 2010, etc.

Note that any restored Web front-end related components (for example, IIS settings, SharePoint site definitions, and custom features), should be restored on all of the Web front-end servers of the SharePoint farm.

End-User Platform Restore

The End-User Platform Restore feature is used in SharePoint and allows end users to restore the backed up SharePoint contents at list/library, folder, and item/document levels using in-place-restore type. End users can search desired objects, for which they have required permissions, by specifying search conditions in SharePoint, and restore them. Administrator can configure search scope, maximum limit of search results, and required permissions on DocAve Manager for end users. The conflict resolution of restore can be specified by administrator, or by end users. A detailed job report for all items is available.

***Note**: End-User Platform Restore supports restoring the granular data from the backed up BLOB data, which has been backed up by Platform Backup job.

Supported and Unsupported Web Browsers

Before you begin to use the End-User Platform Restore feature, refer to the table below for the supported and unsupported Web browsers:

SharePoint Version	Web Browser	Support Status
SharePoint 2010	Internet Explorer 11	Supported
	Internet Explorer 10	Supported
	Internet Explorer 9	Supported
	Internet Explorer 8	Supported
	Internet Explorer 7	Unsupported
	Internet Explorer 6	Unsupported
	Google Chrome	Supported
	Mozilla Firefox	Supported
	Apple Safari	Supported with limitations
SharePoint 2013 and SharePoint 2016	Internet Explorer 11	Supported
	Internet Explorer 10	Supported
	Internet Explorer 9	Supported
	Internet Explorer 8	Supported
	Internet Explorer 7	Unsupported
	Internet Explorer 6	Unsupported
	Google Chrome	Supported
	Mozilla Firefox	Supported
	Apple Safari	Supported

Installing the End-User Platform Restore Solution

To use the End-User Platform Restore feature, complete the following steps to deploy the **SP2010EndUserPlatformRestore.wsp/SP2013EndUserPlatformRestore.wsp/ SP2016EndUserPlatformRestore.wsp** solution to at least one Web application in the farm. The **SP2010EndUserPlatformRestore.wsp** is used for SharePoint 2010 and the SharePoint 2010 mode site

collections within SharePoint 2013. The **SP2013EndUserPlatformRestore.wsp** solution is used for SharePoint 2013. The **SP2016EndUserPlatformRestore.wsp** solution is used for SharePoint 2016.

1. Navigate to **Control Panel** > **Solution Manager**.
2. Select the farm where you want to deploy the solution from the **Farm** drop-down list.
3. Select the **SP2010EndUserPlatformRestore.wsp**/**SP2013EndUserPlatformRestore.wsp**/ **SP2016EndUserPlatformRestore.wsp** according to the farm you selected.
4. Click **Install** in the **Actions** group to install this solution.
5. After the solution is installed, click **Deploy** in the **Actions** group to deploy the solution to the selected SharePoint farm.

For more information of managing solutions, refer to the DocAve 6 Control Panel Reference Guide.

Activating the End-User Platform Restore Feature

To use the End-User Platform Restore feature, complete the following steps to activate the feature in the desired site collections in both DocAve Manager and SharePoint after the solution is deployed to the desired farms.

1. In DocAve Manager, navigate to **Platform Backup and Restore** > **Restore** > **End-User Platform Restore**.
2. Expand the tree to the site collection level. Select the site collections that you want to activate the End-User Platform Restore feature. You can also select the farm node or the Web application node to select all included site collections.
3. Click **Activate** on the ribbon to activate the feature in the selected site collections. You can also click **Activate** next to each site collection to activate the feature one by one.

   The site collection status of activating the End-User Platform Restore feature is displayed in the **Status** column.
4. Access the site collection in SharePoint that the End-User Platform Restore feature is activated in DocAve.

Manage the site collections features according to your SharePoint version.

- When using SharePoint 2010, navigate to **Site Actions** > **Site Settings** > **Site Collection Administration** > **Site collection features**.
- When using SharePoint 2013 or SharePoint 2016, click the settings ( ) button on the upper-right corner and navigate to **Site settings** > **Site Collection Administration** > **Site collection features**.

Activate the **End-User Platform Restore for SharePoint 2010**/**End-User Platform Restore for SharePoint 2013**/**End-User Platform Restore for SharePoint 2016** feature. After the activation, you can find the **Restore from Platform Backup** link under the **Site Actions** drop-down list (in

SharePoint 2010) or under the drop-down list after clicking the settings ( ) button (in SharePoint 2013 or SharePoint 2016).

Configuring the End-User Platform Restore Settings

Before end user proceeds with an End-User Platform Restore, DocAve administrator can complete the following steps to configure the settings.

1. Select the site collections, which you want to configure the advanced settings for, by selecting the checkboxes next to the relative URL.
2. Click **Advanced Settings** on the ribbon to configure the settings for the selected site collections. You can also click **Advanced Settings** next to each site collection to configure the settings one by one.
    a. **Select a Plan** – Select a plan to specify a searching scope of backup data for restore.
    b. **Permission Level** – Specify the required minimum permission level for the end-user restore: **Full Control**, **Design**, or **Contribute**. Only if the end user has the specified permission level or higher to the desired SharePoint content, he/she can search out the content from the backup data. If the end user does not have the required permission level to the desired SharePoint content, he/she cannot search out the content or perform the restore job.

    If a site collection has **Read-only (blocks additions, updates, and deletions)** selected in the **Lock status for this site** settings (**SharePoint Central Administration** > **Site Collection Quotas and Locks** > **Site Lock Information**), the end-user can only view the site content and does not have **Full Control**, **Design**, or **Contribute** permission level. Therefore, the end-user cannot perform a search or restore operations at the specified site collection.

    c. **Conflict Resolution** – Define the conflict resolution behavior. When restoring, if the SharePoint object name in the source node is the same as an existing object in the destination node, it is considered as a conflict.

    Selecting **Let end user decide** will leave the decision of conflict resolution to end user on SharePoint when they are performing a restore.

    DocAve administrator can define the conflict resolution for end user by selecting **Specify conflict resolution**, and choosing the behavior for resolving the conflict during a restore.

    - **Container level conflict resolution** – Set the conflict resolution on the list, library, and folder level.
        - **Skip** – Ignores the source container that has the same name as the destination one.
        - **Merge** – Combines the configuration of the source and destination container. If there is a conflict, the source configuration overwrites the destination one.

- **Replace** – Deletes the destination container and then restores the source container to the destination.

***Note:** A discussion board item is considered a folder, so it is restored as a container.

- **Content level conflict resolution** – Set the conflict resolution on the item, document, and attachment level.
  - **Skip** – Ignores the source item/document/attachment that has the same item ID/document name/attachment name as the destination item/document/attachment.
  - **Overwrite** – Copies the source item/document/attachment to the destination by overwriting the destination item/document/attachment with same item ID/document name/attachment name.
  - **Overwrite by Last Modified Time** – Keeps the conflict item/document/attachment which has the latest modified time and overwrites the older one.
  - **Append an Item/Document Name with a Suffix** – Adds the conflict source item/document/attachment to the destination and adds a suffix to the end of the item title/document name/attachment name. The conflict destination item/document/attachment is not deleted.
  - **Append a New Version** – Adds the conflict source item/document to the destination as a new version of the conflict destination item/document.

d. **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** 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 original SharePoint farm, then the selected content in the backup is not restored.

***Note**: Selecting **Let end user decide** will leave the decision to end user on SharePoint when they are performing a restore.

e. **Use InstaMount** – Choose whether or not to use InstaMount when performing the restore. Selecting **Yes** will generate an InstaMount temporary database, and recover single items directly. Selecting **No** will generate an ordinary temporary database used for recovering the entire database. For more information about InstaMount, refer to About InstaMount.

f. **Staging Policy** – Select an existing staging policy. A staging policy allows you to execute InstaMount when necessary. It also includes a temporary database to store data. For information about staging policy, refer to About the Staging Policy.

g. **Verify GUID** – Define how to resolve a conflict when the name of the selected object for restore matches with the name of an existing object in the destination. Selecting **Verify object GUID in backup data** will compare the object GUID from the backup data with the object GUID in the destination. If the GUIDs are not the same, the object will not be restored. Deselecting this option will not compare the GUIDs and the object will be restored.

h. **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.

i. **Item Dependent Columns and Content Types** – Choose whether or not to restore item-dependent columns and content types.

   - **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 or library. The item still uses the dependent column and content type. Proceed to select a conflict resolution from the **Conflict resolution for dependent items** list.
   - **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.

j. **Maximum Search Job Allowed** – Set a maximum limit of backup job search scope to let end users search the backup data of desired objects and restore them.

k. **Maximum Search Results to Display** – Set a maximum amount of search results to be displayed in the **Search Result** pane of SharePoint > Restore from Platform Backup interface.

l. **Notification** –Select a created e-mail notification profile, or create a new one that contains the report settings and the report recipients. You can view the detailed information of the selected profile by clicking **View**. For more information on working with notification policies, refer to the DocAve 6 Control Panel Reference Guide.

***Note**: There are two notification settings both in DocAve advanced settings and SharePoint restore settings. This is required in DocAve Manager, otherwise the e-mail cannot be sent.

3. Click **OK** to save the advanced settings.

Using the End-User Platform Restore Feature

To perform an End-User Platform Restore, an end user need to complete the following steps:

1. Access the site collection with the required permission.
2. Launch End-User Platform Restore according to your SharePoint version.
    - When using SharePoint 2010, navigate to **Site Actions** > **Restore from Platform Backup**. The **Restore from Platform Backup** page appears.
    - When using SharePoint 2013 or SharePoint 2016, click the settings ( ) button on the top right corner and click **Restore from Platform Backup**. The **Restore from Platform Backup** page appears.
3. Configure the search conditions:
    - **Restore Object Level** – Specify the level of the objects that you want to restore.
    - **Backup Time Range** – Search the contents within the specified time range:
        - **This Week** – Search the contents backed up within this week.
        - **This Month** –Search the contents backed up within this month.
        - **Custom** – Search the contents backed up within the customized time range. Click the calendar to select the specified date and time.
    - **Keyword** – Search the desired contents by the keywords. The objects with a name or title containing the keyword will be returned.

      Note:** The search function is not case sensitive. Wildcards **?** and ** are supported. View the table below for details of what to search when entering the keyword.

Object Level	What to Search
List	List name
Library	Library name
Folder	Folder name
Item	Item title
Document	Document name and/or the extension

    ***Note**: If the search results of backup jobs in this time range exceed the maximum amount set in DocAve Manager. A pop-up message will appear to remind users to narrow down the time range, or click **Select Backup Time** button to select no more than the maximum limit of backup jobs.
4. Click **Search** to start searching the contents that match the search conditions. You can also click **Reset** to reset the search conditions.
5. On the **Search Result** pane, view the following information:
    - **Object Name** – The name of the objects that matches the search conditions.

- **Backup Time** – The time when the objects are backed up. You can click **View Backup History** to view and select the version that you want to restore.
- **Path** – The URL of the objects in the source.

***Note**: When the number of search results exceeds the maximum limit set in DocAve Manager, a pop-up message appears to remind users to search again with more specific conditions if their desired objects are not included in the search results.

- **View Backup History** – you can click **View Backup History** to view and select the version that you want to restore.

6. After you select the version of the object to restore, click **Restore** and configure restore settings in the pop-up window.
7. **Restore Settings** – Configure the following restore settings:
   - **Conflict Resolution** – Define the conflict resolution behavior. When restoring, if the SharePoint object name in the source node is the same as an existing object in the destination node, it is considered as a conflict.

     ***Note**: End users can make decisions about the conflict resolution. When the end user selects a content level to restore, the **Container level conflict resolution** setting will be hidden in restore settings pop-up window.

   - **Consider the existing data in destination Recycle Bin** – Choose whether or not to compare the data in the backup with the data in the original SharePoint farm's recycle bin.

   ***Note**: The two settings above only appears when administrator select **Let end user decide** for the same settings on DocAve Manager.

   - **Notification** – Specify an e-mail notification. The specified users will receive e-mail notifications about the restore job results. Use a semicolon (;) to separate multiple e-mail addresses.
8. Click **OK** when you are finished. A pop-up window appears indicating that the restore job is running.
9. The restore job result is displayed in the pop-up window after the job completes. Click **OK** to close the pop-up window. You can also close the pop-up window during the restore process, which does not affect the restore job.

***Note:** Click **Powered by AvePoint DocAve** on the **End-User Platform Restore** page. It will link to the AvePoint homepage in a new Web window.

Appendix A: About Find Site Collection

Find Site Collection feature provides you a quick method to find your desired site collection from your backup data by entering the URL or with the wildcards being used.

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

1. On the **Time-based Restore** tab within the **Data Selection** step of the **Restore Wizard**, click any node on the Backup Data tree to enable the Find Site Collection feature 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 enter 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 enter 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 to locate specific objects or data within each granular level (from site collection level down to item level) to restore. You can use Advanced Search in the Time-based Restore at the granular level to search for the granular content to restore.

Additionally, you can use the Advanced Search feature to search for a destination node from the destination farm tree for the granular contents you are about to restore, especially when the destination farm contains a very large amount of content and nodes.

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, and then select the **Restore Granular Content** option on the **Restore Granular Level** field.
3. Click **OK** to proceed to restore the granular data, and then select 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	Searches for the site collection whose last modified time is between 2013-12-12 16:41:00 (UTC+08:00) Beijing,

Level	Rule	Condition	Value	Result
			16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Chongqing, Hong Kong, Urumqi) and 2013-12-27 16:41:00 (UTC+08:00) Beijing, 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)

Level	Rule	Condition	Value	Result
		After	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the list 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 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**.
	Modified Time	Before	2013-12-27 16:41:00 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi)	Searches for the app 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 app 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 app 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)
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,	Searches for the folder whose last modified time is earlier

Level	Rule	Condition	Value	Result
			Chongqing, Hong Kong, Urumqi)	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**.
	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)	Searches for the item/document whose last modified time is between 2013-12-12 16:41:00 (UTC+08:00) Beijing,

Level	Rule	Condition	Value	Result
			Beijing, Chongqing, Hong Kong, Urumqi)	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: Accessing Hot Key Mode

In order to work faster and improve your productivity, DocAve supports hot key mode for you to perform corresponding actions quickly by only using your keyboard. To access hot key mode from the Platform Backup and Restore interface, press the key combination of **Ctrl** +**Alt** + **Z** on your keyboard.

The following table provides a list of hot keys for the Home page of the Platform Backup and Restore interface. Each time you want to go back to the Home page, press **Ctrl** + **Alt** + **Z** on your keyboard. For example, continue pressing **B** to go back to the **Backup** tab of Platform Backup and Restore.

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	SP				
				Staging Policy	A				
				Custom Database	U				
				Command With Operation	ZO				
				Host Profile	HP				
				VM Script Profile	VS				
				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				
				Host Profile	HP				
				VM Script Profile	VS				
				Save	SV	Save	S		
						Save and Run Now	R		
						Save and Test Run	T		
				Cancel	C				
Storage Policy	SP								
Staging Policy	A	Create	N	Save	O				
				Cancel	C				
		Edit	E	Save	O				
				Cancel	C				
		Delete	D						
		Close	C						
Command With Operation	ZO	Command Profile	CM	Create	CR	Save	O		
						Cancel	C		
				Edit	E				
				Delete	D				
		Script Profile	S	Create	CR	Save	O		

Functionality Name and Hot Key							
						Cancel	C
				Edit	E		
				Delete	D		
		Close	CL				
Host Profile	HP						
VM Script Profile	VS	Create	CR		Save		O
					Cancel		C
		Edit	E		Save		O
					Cancel		C
		Delete	D				
		Close	CL				
Migrate Database	MD	Back	B				
		Next	N				
		Start	F				
		Cancel	C				
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	FN				
		Cancel	CX				
Farm Repair	FP	Repair	FP				
		Close	C				
Staging Policy	SP	Create	N		Save		O
					Cancel		C
		Edit	E		Save		O
					Cancel		C
		Delete	D				
		Close	C				
Command with Operation	CO	Command Profile	CM	Create	CR	Save	O
						Cancel	C

Functionality Name and Hot Key							
				Edit	E	Save	O
						Cancel	C
				Delete	D		
		Script Profile	S	Create	CR	Save	O
						Cancel	C
				Edit	E	Save	O
						Cancel	C
				Delete	D		
		Close	CL				
VM Script Profile	VS	Create	CR	Save		O	
				Cancel		C	
		Edit	E	Save		O	
				Cancel		C	
		Delete	D				
		Close	CL				
End-User Restore	E	Advanced Settings	S	Save		O	
				Cancel		C	
		Activate	A				
		Deactivate	D				
		Close	C				
Job Monitor	J						

Time-Based Restore

Functionality Name and Hot Key					
Time-based Restore	T	Create Container	T	OK	O
				Cancel	C
		Destination Physical Device	DP		
		Advanced Search	AS	Search	S
				Cancel	C
		Find Site Collection	Q		
		Staging 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
		Database and Log File Mapping	SD	Save	S
				Cancel	C
		SharePoint Server Mapping	SP	Save	S
				Cancel	C
		Index Location	I	Save	S
				Cancel	C
		Destination Physical Device	P	Save	O
				Cancel	C
		Back	B		
		Next	N		
		Start	ST		
		Cancel	CX		
Farm Clone with VM	FV	SQL Server Mapping	SM	Save	S
				Cancel	C
		Database and Log File Mapping	SD	Save	S
				Cancel	C
		SharePoint Server Mapping	SP	Save	S
				Cancel	C
		Index Location	I	Save	S
				Cancel	C
		Destination Physical Device	P	Save	O
				Cancel	C
		Back	B		
		Next	N		
		Start	ST		
		Cancel	CX		
Job Monitor	J				

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			
				Staging Policy	ZC			
				Custom Database	ZD			
				Command With Operation	ZO			
				Host Profile	HP			
				VM Script Profile	VS			
				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					
		Staging Policy	ZC					
		Custom Database	ZD					
		Command with Operation	ZO					
		Host Profile	HP					
		VM Script Profile	VS					
		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					

Appendix D: SharePoint 2010 Components Supported in Platform Backup and Restore

Refer to the section below for the details on the SharePoint 2010 Web parts, service applications, and component supported in Platform Backup and Restore.

Supported Web Parts

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.

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.

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

Web Part		Supported Status
	Query String(URL) Filter	Supported
	SharePoint List Filter	Supported
	Text Filter	Supported
Forms	HTML Form Web Part	Supported
	InfoPath Form Web Part	Supported
Media and Content	Content Editor	Supported
	Image Viewer	Supported
	Media Web Part	Supported
	Page Viewer	Supported
	Picture Library Slideshow Web Part	Supported
Outlook Web App	My Calendar	Supported
	My contacts	Supported
	My Inbox	Supported
	My Mail Folder	Supported
	My Tasks	Supported
Search	Advanced Search Box	Supported
	Dual Chinese Search	Supported
	Federated Results	Supported
	People Refinement Panel	Supported
	People Search Box	Supported
	People Search Core Results	Supported
	Refinement Panel	Supported
	Related Queries	Supported
	Search Action Links	Supported
	Search Box	Supported
	Search Core Results	Supported
	Search Paging	Supported
	Search Statistics	Supported
	Search Summary	Supported
	Top Federated Results	Supported
Social Collaboration	Contact Details ***Note**: The user related properties of this Web part will be backed up and restored together with the Web part.	Supported
	Note Board	Supported
	Organization Browser	Supported
	Site Users	Supported
	Tag Cloud	Supported
	User Tasks	Supported

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 Status for In-place Restore	Supported Status for Out-of-place Restore
Access Services	This Service Application does not have a database	Supported	Supported
Application Registry Service	application registry service database	Supported	Unsupported
Business Data Connectivity Service	Bdc_Service_DB(Business Data Connectivity Database)	Supported	Supported
Excel Services Application	This Service Application does not have a database	Supported	Supported
Managed Metadata Service	Managed Metadata Service_Database(Service Application Database)	Supported	Supported
PerformancePoint Service Application	PerformancePoint Service Application_Database(Microsoft.PerformancePoint.Scorecards.BIMonitoringServiceDatabase)	Supported	Supported
Search Service Application	Search_Service_Application_DB(Administration Database) Search_Service_Application_CrawlStoreDB(Crawl Database) Search_Service_Application_PropertyStoreDB(Property Database)	Supported	Partially Supported ***Note**: Search Service Application (Native) is supported and Search Service Application (FAST) is not supported.
Secure Store Service	Secure_Store_Service_DB(Secure Store Service Database)	Supported	Supported
Security Token Service Application	This Service Application does not have a database	Supported	Unsupported
State Service	StateService_Database(State Service Database Settings)	Supported	Unsupported

Service Application	Databases of the Service Application	Supported Status for In-place Restore	Supported Status for Out-of-place Restore
Session State Service	SessionStateService_Database	Supported	Unsupported
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)	Supported	Supported
Visio Graphics Service	This Service Application does not have a database	Supported	Supported
Web Analytics Service Application	WebAnalyticsServiceApplication_StagingDB (Web Analytics Staging Database) WebAnalyticsServiceApplication_ReportingDB(Web Analytics Warehouse Database)	Supported	Supported
Word Automation Services(Word Conversion Service)	WordAutomationServices_Database(Microsoft.Office.Word.Server.Service.QueueDatabase)	Supported	Supported
Lotus Notes Connector	–	Unsupported	Unsupported
Usage and Health data collection	WSS_Logging	Supported	Unsupported
Word Viewing Service	–	Supported	Supported ***Note**: The destination farm must have OWA installed.
PowerPoint Service Application	–	Supported	Supported ***Note**: The destination farm must have OWA installed.

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

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	Supported in Out-of-place Restore	Notes
Configuration Database	Supported (Restore Database Only must be used)	Unsupported	
Central Admin Web Application	Supported (Restore Database Only must be used)	Unsupported	
Admin Content Database	Supported	Unsupported	
Web Application	Partially Supported	Partially Supported	VSS does not support backing up the database whose database files are stored in Net Share.
Content Database	Supported	Supported	
Global Search Settings	Supported	Supported	Farm-level search settings and Crawler impact rules are supported.
SharePoint Help Search	Supported	Unsupported	
InfoPath Form Services	Supported	Supported	InfoPath Forms Services Settings and InfoPath Forms Services Form templates are supported.
FBA Databases	Supported	Unsupported	The FBA Database and some configurations in the Web.config under WebApp IIS Setting (such as MemberShipProvider) are supported.

Features	Supported in In-place Restore	Supported in Out-of-place Restore	Notes
Solutions	Supported	Supported	• For in place restore, restoring the uploaded solution and its status in the Solution Management is supported. • For out of place restore, restoring the uploaded solution in the Solution Management is supported. Restoring the solution's status in the Solution Management is not supported.
FAST Search Server 2010 for SharePoint	Supported	Unsupported	DocAve Platform Backup and Restore backs up FAST components, configuration files, index data, etc. 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	Partially Supported	Unsupported	
BLOB	Supported	Supported	Only Storage Manager BLOB data supports out of place restore.
NewsGator	Supported	Unsupported	Social Sites (NewsGator) 1.2 and 2.5 are supported in DocAve 6 Service Pack 1 and later.
Nintex Workflow	Supported	Unsupported	Nintex workflows can be restored to their original location where they were backed up. However, they cannot be restored to another farm using the out of place Platform restore.
Farm Level Backup and Item Level Restore	Supported	Supported	• If you want to do Platform granular Restore, the Platform granular Restore index must be generated. • InstaMount function is supported.

Features	Supported in In-place Restore	Supported in Out-of-place Restore	Notes
Web Front-End Server	Supported	Supported	• IIS Settings (such as Form Authentication, SSL certification, etc.) 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 Platform Backup and Restore can also backup and restore the files in the file system of the Web front-end server.

Appendix E: SharePoint 2013 Components Supported in Platform Backup and Restore

Refer to the section below for the details on the SharePoint 2013 Web parts, service applications, and component supported in Platform Backup and Restore.

Supported Web Parts

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.

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.

Web Part		Supported Status
Business Data	Business Data Actions	Supported
	Business Data Connectivity Filter	Supported
	Business Data Item	Supported
	Business Data List	Supported
	Business Data Related List	Supported
	Chart Web Part	Supported
	Excel Web Access	Supported
	Indicator Details	Supported
	Status List	Supported
	Visio Web Access	Supported
Content Rollup	Categories	Supported
	Content Search	Supported
	Relevant Documents	Supported
	RSS Viewer	Supported
	Site Aggregator	Supported
	Sites in Category	Supported
	WSRP Viewer	Supported
	XML Viewer	Supported
Filters	Apply Filters Button	Supported
	Choice Filter	Supported
	Current User Filter	Supported
	Date Filter	Supported
	Page Field Filter	Supported
	Query String(URL) Filter	Supported
	SharePoint List Filter	Supported
	Text Filter	Supported

Web Part		Supported Status
Forms	HTML Form Web Part	Supported
	InfoPath Form Web Part	Supported
Media and Content	Content Editor	Supported
	Image Viewer	Supported
	Media Web Part	Supported
	Page Viewer	Supported
	Picture Library Slideshow Web Part	Supported
Search	Search Box	Supported
	Search Results	Supported
	Refinement	Supported
Social Collaboration	Contact Details ***Note**: The user related properties of this Web part will be backed up and restored together with the Web part.	Supported
	Note Board	Supported
	Organization Browser	Supported
	Site Users	Supported
	Tag Cloud	Supported
	User Tasks	Supported

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	Supported in Out-of-place Restore
Access Services	This Service Application does not have a database	Supported	Supported
Access Services 2010	This Service Application does not have a database	Supported	Supported
App Management Service	AppMng_Service_DB (App Management Database)	Supported	Supported
Business Data Connectivity Service	Bdc_Service_DB(Business Data Connectivity Database)	Supported	Supported
Excel Services Application	This Service Application does not have a database	Supported	Supported
Lotus Notes Connector	–	Unsupported	Unsupported
Managed Metadata Service	Managed Metadata Service_Database(Service Application Database)	Supported	Supported

Service Application	Databases of the Service Application	Supported in In-place Restore	Supported in Out-of-place Restore
Machine Translation Service Application	Machine Translation Service Database	Supported	Unsupported
PerformancePoint Service Application	PerformancePoint Service Application_Database(Microsoft.PerformancePoint.Scorecards.BIMonitoringServiceDatabase)	Supported	Supported
PowerPoint Conversion Service Application	This Service Application does not have a database	Supported	Supported
Project Service Application	This Service Application does not have a database. Platform Backup and Restore backs up and restores the databases of Project 2013 PWA site: ProjectWebApp	Supported	Supported
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)	Supported	Supported
Secure Store Service	Secure_Store_Service_DB(Secure Store Service Database)	Supported	Supported
Security Token Service Application	This Service Application does not have a database	Supported	Unsupported
Session State Service	SessionStateService_Database	Supported	Unsupported
State Service	StateService_Database(State Service Database Settings)	Supported	Unsupported
Subscription Settings Service Application	Subscription Settings Database	Supported	Supported
SQL Server Reporting Service	Reporting Service Database Reporting Service Alerting Database Reporting Service Temp Database	Supported	Supported
SQL Server Powerpivot Service Application	PowerpivotServiceApplication	Supported	Supported ***Note**: The PowerPivot for SharePoint must be installed in the destination farm.
Usage and Health data collection	WSS_Logging	Supported	Unsupported

Service Application	Databases of the Service Application	Supported in In-place Restore	Supported in Out-of-place Restore
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)	Supported	Supported
Visio Graphics Service	This Service Application does not have a database	Supported	Supported
Word Automation Services(Word Conversion Service)	WordAutomationServices_Database (Microsoft.Office.Word.Server.Service.QueueDatabase)	Supported	Supported
Workflow Services Proxy(Workflow Service Application Proxy)	–	Supported	Unsupported
Work Management Service	This Service Application does not have a database	Supported	Unsupported

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	Supported in Out-of-place Restore	Notes
Web Application	Partially Supported	Partially Supported	VSS does not support backing up the database whose database files are stored in Net Share.
Configuration Database	Supported (Restore Database Only must be used)	Unsupported	
Central Admin Web Application	Supported (Restore Database Only must be used)	Unsupported	
Solutions	Supported	Supported	For in place restore, restoring the uploaded solution and its status in the Solution Management is supported.
InfoPath Form Services	Supported	Supported	InfoPath Forms Services Settings and InfoPath Forms Services Form templates are supported.
Global Site Template	Supported	Supported	
Custom DB	Supported	Unsupported	
Web Front-End Server	Supported	Supported	
Item Level Restore	Supported	Supported	• If you want to do Platform granular Restore, the Platform granular Restore index must be generated. • InstaMount function is supported.
FBA Databases	Supported	Unsupported	The FBA Database and some configurations in the Web.config under WebApp IIS Setting (such as MemberShipProvider) are supported.
BLOB	Supported	Supported	Only Storage Manager BLOB data supports out of place restore.
NewsGator	Supported	Unsupported	Social Sites (NewsGator) 4.0 for SharePoint 2013 is supported in DocAve 6 Service Pack 4 and later. Social Sites (NewsGator) 5.0 for SharePoint 2013 is supported in DocAve 6 Service Pack 6 and later.

Features	Supported in In-place Restore	Supported in Out-of-place Restore	Notes
Nintex Workflow	Supported	Unsupported	Nintex workflows can be restored to their original location where they were backed up. However, they cannot be restored to another farm using the out of place Platform restore.

Appendix F: SharePoint 2013 Social Features Supported in Platform Backup and Restore

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

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	
Community Portal		Supported	Supported	

Appendix G: SharePoint 2016 Components Supported in Platform Backup and Restore

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

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

Appendix H: SharePoint Object Security and Property

Refer to the table below for the detailed information of 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 I: Advanced Settings in Configuration Files

AgentCommonWrapperConfig.config

Edit the **AgentCommonWrapperConfig.config** file to configure whether to restore custom properties in SharePoint property bag.

Go to the machines with DocAve Agent installed and open the *…\AvePoint\DocAve6\Agent\bin* directory to find the **AgentCommonWrapperConfig.config** file.

Restoring Specified Web Properties

Open the **AgentCommonWrapperConfig.config** file and find the **WrapperCommon** node. Within this node, find the **<RestoredAllWebProperties>False</RestoredAllWebProperties>** node and the **<SpecialWebPropertyNames></SpecialWebPropertyNames>** node. These two nodes are added to the configuration file automatically when you first run a Platform Backup and Restore job at the item level.

- If you do not want to restore custom properties in property bag, use the default **False** value. When using the **False** value, you can also add the specific custom properties in the **SpecialWebPropertyNames** node, and the custom properties you specified will be restored. Use the semicolon sign to separate the custom properties, for example, **<SpecialWebPropertyNames>property1; property 2; property3</SpecialWebPropertyNames>**. Note that the built-in properties in property bag are all restored.
- If you want to restore all the properties, including the custom and built-in properties, change **False** to **True**. When using the **True** value, you can add the specific properties in the **SpecialWebPropertyNames** node and the properties you specified will not be restored.

SP2010PlatformConfiguration.xml

Edit the **SP2010Configuration.xml** file to trigger some further functions.

Go to the machines with DocAve Agent installed and open the *…\AvePoint\DocAve6\Agent\data\SP2010\Platform* directory to find the **SP2010Configuration.xml** file.

Controlling Agents Backing Up in Parallel

By default, all of the Agents on SharePoint servers execute backup in parallel, and this method will improve the backup performance. If you want the Agents to execute backup in serial, modify the **SP2010Configuration.xml** file on all of the SharePoint server Agents:

Open the **SP2010Configuration.xml** file, and find the <**BackupConfig**> node. Within this node, find the **IsAgentConcurrent="true"** attribute. Change the default value **true** to **false** to disable Agents backing up in parallel.

Configuring Maximum Amount of Concurrent Threads on Agents

By default, an Agent can execute a maximum of five concurrent threads. The maximum amount of concurrent threads on Agents can be modified in the **SP2010Configuration.xml** file:

Open the **SP2010Configuration.xml** file in the Agents that are installed on SQL Server or Index Server, and find the <**BackupConfig**> node. Within this node, find the **MaxConcurrentThreadsCount="5"** attribute. AvePoint recommends you setting the value of the **MaxConcurrentThreadsCount** between three and five.

Configuring Connecting Media Settings

Open the **SP2010Configuration.xml** file and find the **FarmLevel** node. Within this node find the **networkTimeOut** and the **mediaRetryTimes** attributes.

- **networkTimeOut** – This attribute defines the session timeout of connecting to the Media Service server. The unit of this attribute value is in seconds.
- **mediaRetryTimes** – This attribute defines the time for reconnecting to the Media Service server.

Configuring Maximum Number of Files and Folders to Be Backed up

Open the **SP2010Configuration.xml** file, and find the **<WFEConfig></WFEConfig>** child node under the **FarmLevel** node. The **BackupBufferSize** attribute within this node defines the maximum number of files and folders that can be backed up at a time. The default value is 10000. If the number of files and folders is greater than this value, they will be backed up in batches.

Configuring Index Generation Option

Open the **SP2010Configuration.xml** file, and find the **<VDBSupportGenerateIndexConfig></VDBSupportGenerateIndexConfig>** child node under the **FarmLevel** node. Refer to the information below to configure the **supportGenerateIndex** attribute:

- **True** – The default value of the **supportGenerateIndex** attribute is **true**, which means the index will be generated on the virtual databases.
- **False** – Setting the value of the **supportGenerateIndex** attribute to **false** means that the index will be generated on the database when performing a Platform Backup job, and the index will be generated on the temporary databases when performing a maintenance job.

Shrinking Transaction Log

Open the **SP2010Configuration.xml** file and find the **FarmLevel** node. Within this node find the **ShrinkLogAfterBackup** and **ShrinkLogThreshold** attributes. Configure the attributes:

- **ShrinkLogAfterBackup** – If you want to truncate transaction log after finishing Incremental backup, change **False** to **True**.
- **ShrinkLogThreshold** – The value of this attribute decides when to trigger the truncating function according to how much space can be released. For example:

  The value is 0.8, the truncating function will be triggered out when there are 80% of the storage space can be released.

PlatformRecoveryConfig.Config

You can create the **PlatformRecoveryConfig.Config** file in the …*AvePoint**DocAve6**Manager**Control**Config*\ *PlatformRecoveryConfig* directory to change the later Incremental Backup jobs to Full Backup jobs.

Changing Incremental Backup Job to Full Backup Job

Complete the steps below to create the **PlatformRecoveryConfig.Config** file:

1. Open the Notepad, and enter the following configuration information:

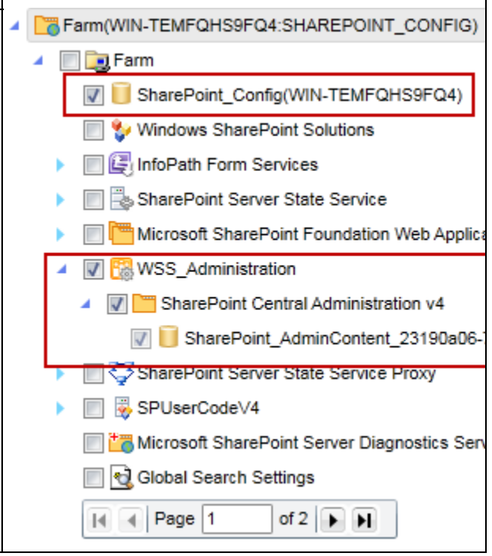
   ```
   <?xml version="1.0" encoding="utf-8" ?>
   <Configurations>
   <Configuration name="ForceFullEnable" support ="true"/>
   </Configurations>
   ```

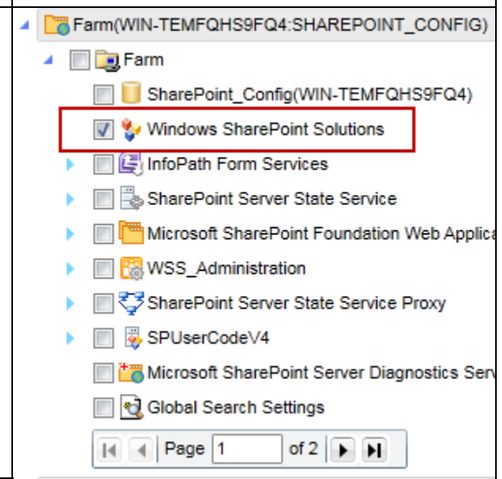
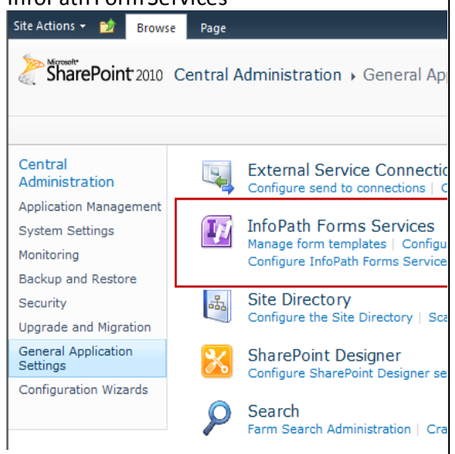
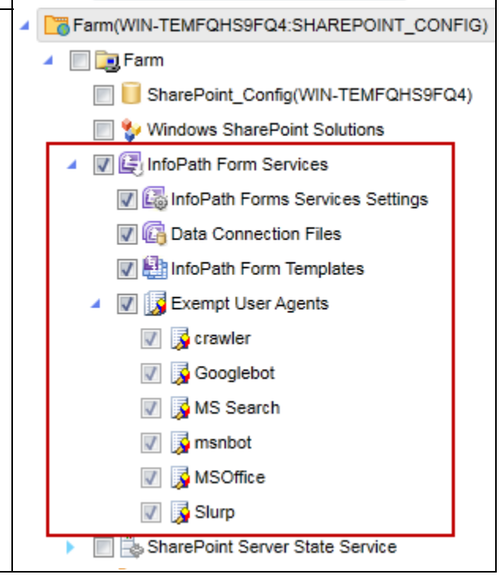
2. Save the file as the **PlatformRecoveryConfig.Config** file under the …*AvePoint**DocAve6**Manager**Control**Config*\ *PlatformRecoveryConfig* directory.

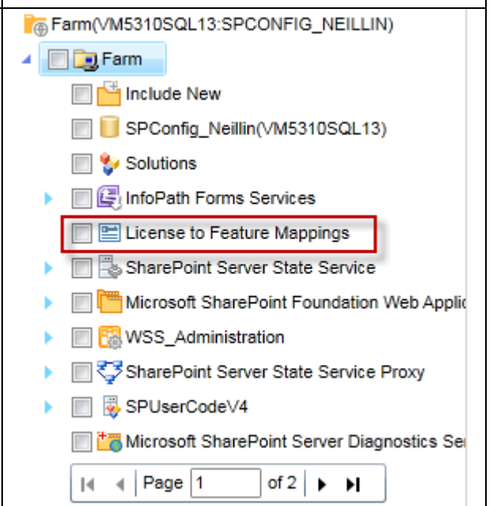
Appendix J: Customization Support Table

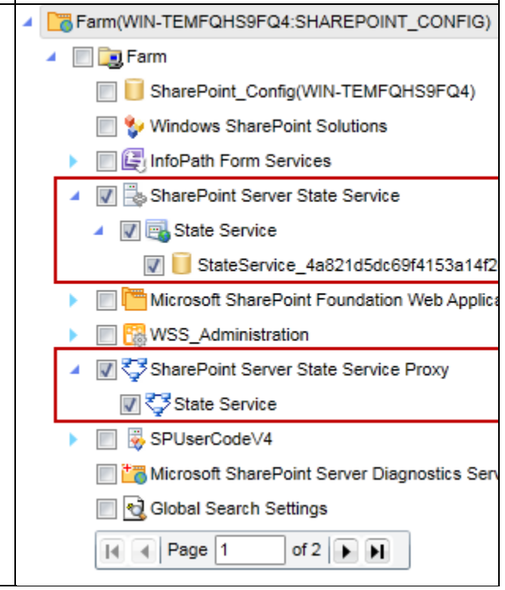
***Note**: Before you restore any content at the specified Restore Granularity, make sure the related higher level SharePoint objects are restored at the farm level or database level. For example, if you want to use the customized feature correctly, you must restore the backed up features in the **Custom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

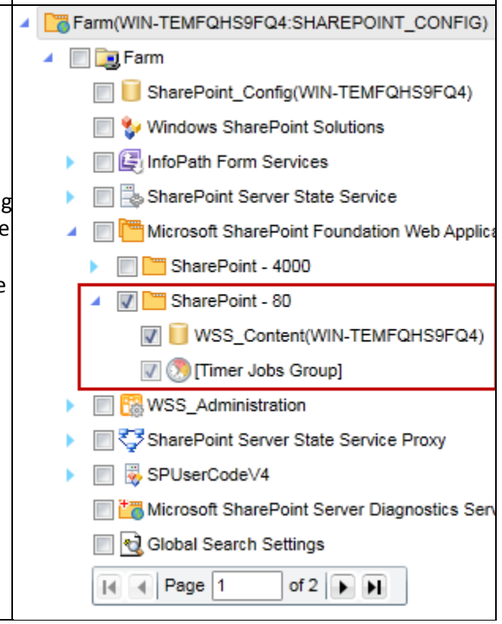
√ means the restore is **Supported** at this level and a blank area means the restore is **Not Supported** at this level.

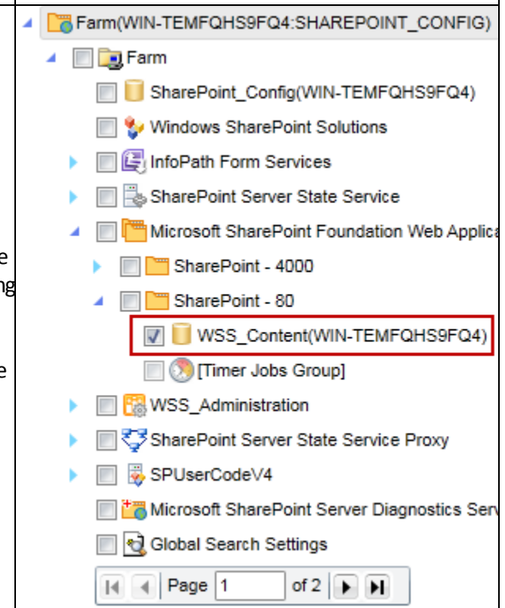
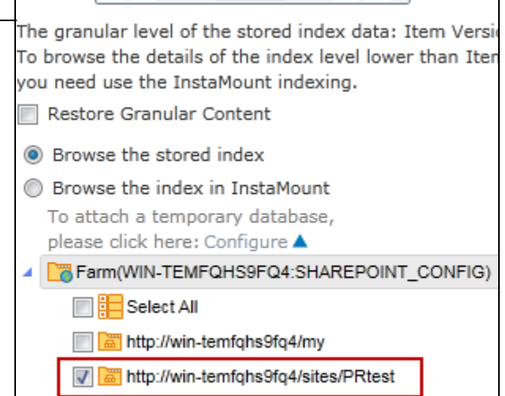
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Central Administration and SharePoint Configuration Database	√	√						The SharePoint Central Administration content database will be automatically selected if the SharePoint Configuration database is selected, and they can only be restored using **In place** restore with the **Restore Database Only** option enabled or using the **Restore Raw Database** method. These nodes will be skipped in the restore job even you have selected to restore them if you do not select the **Restore Database Only** option.	

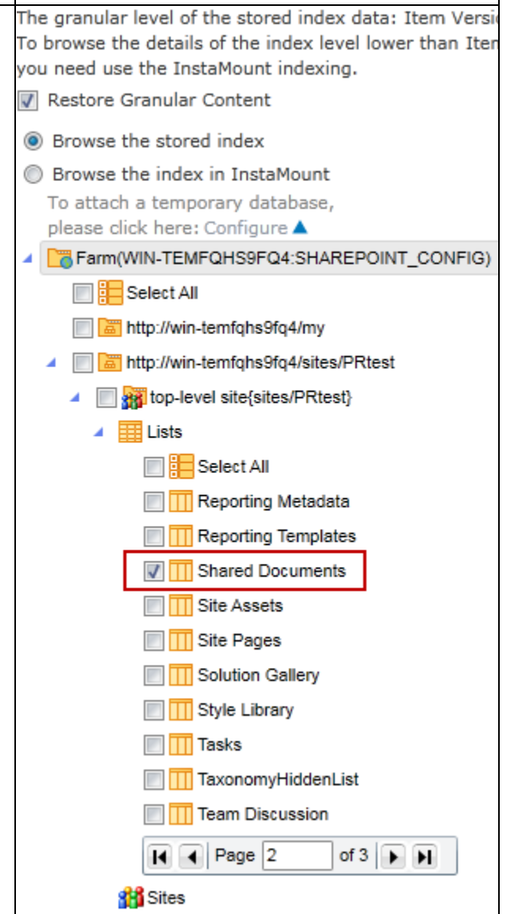
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Solutions	√	√							
InfoPath Form Services 	√	√							

What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			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.	

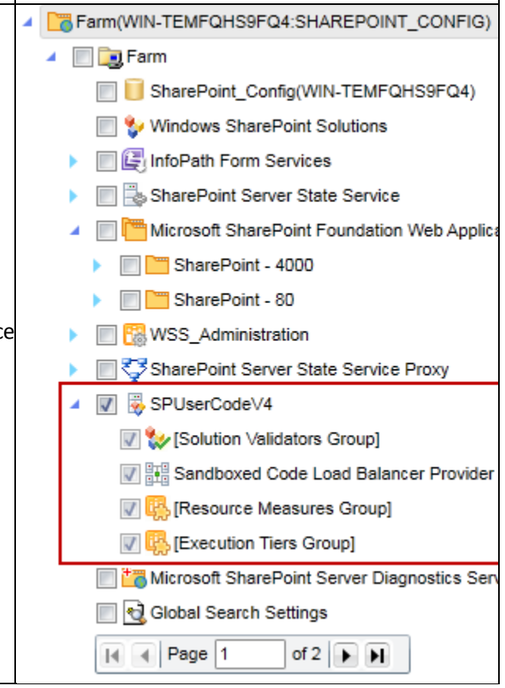
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Server State Service	√	√							

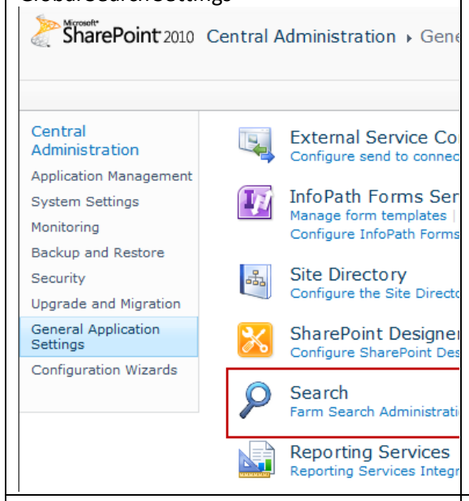
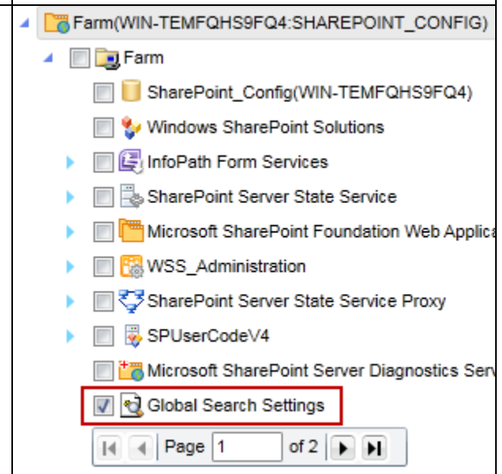
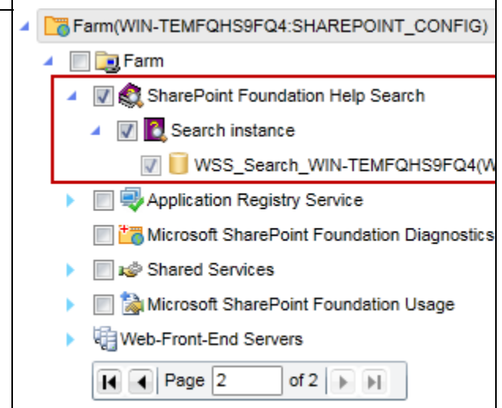
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Web Application	√	√						1. In an **In Place** restore, if you choose to overwrite an existing target web application using the backed up one that has the same name, 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. 2. For web applications with extended zones, you can configure the extended zones after clicking **Show Other Zone** Information.	

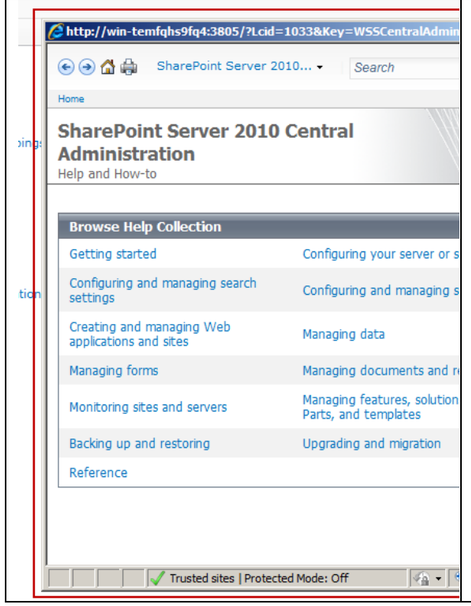
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Content Database	√	√	√	√	√	√	√	Features can be restored at Farm Level, Database Level, Site Collection Level, and Site Level; however, when restoring at Site Collection Level and Site Level, DocAve only restores the existing status and using status of this feature. It will not restore the physical files, which are in …*Common Files**Microsoft Shared**Web Server Extensions**14**TEMPLATE**FEATURES*, of the features.	
Sites with Content types	√	√	√	√				The content types in the site/site collection will be restored together with the site/site collection.	

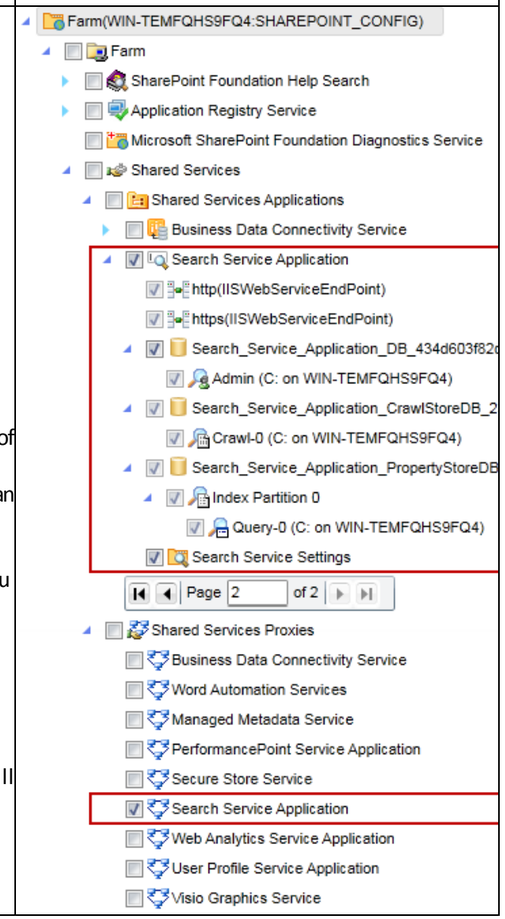
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Lists with Content Types	√	√	√	√	√			The content types in the list will be restored together with the list.	

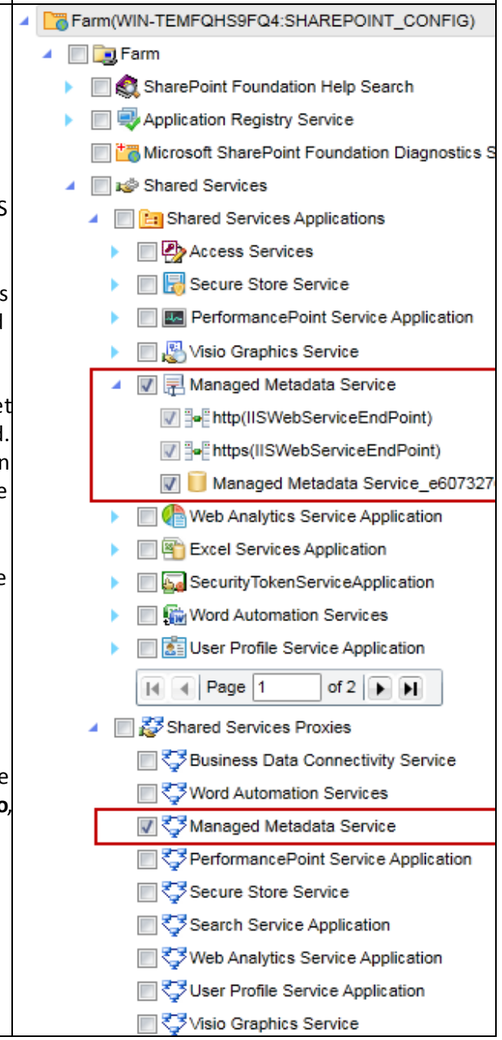
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Built-in Workflow	√	√	√	√	√	√	√	1. If you want to restore the Workflow, you must select the SharePoint object that is associated with the workflow on the tree, and check the check box 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 not such options). For more information, see Notes for Appendix.	**Workflow** Decide how SharePoint workflows are recovered. Selecting ´Include workflow definition´ will restore the definition of the source workflows to the SharePoint container. Selecting ´Include workflow instance´ will recover the state, history, and tasks for each item.
SharePoint Designer Customizations	√	√	√	√	√	√	√	The SharePoint Designer customizations can be restored together with the selected content in the content database. ***Note**: Custom actions are stored in the content databases. If you want to restore the custom actions of a SharePoint Designer workflow, restore the related content databases via Platform Restore at database level.	N/A
Web Part	√	√	√	√	√	√	√	1. 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. 2. The content you selected on the tree can be down to Page and Page Version level.	N/A
Lists and items with Managed Metadata	√	√	√	√	√	√	√	If you want to restore an item that uses the managed metadata term sets, make sure the related managed metadata service is successfully restored at 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. If the custom template is written by the customer, it may not be usable after a Platform Restore job. Because the development varies from each other and the template is specially designed to realize the customers’ requirements.	N/A

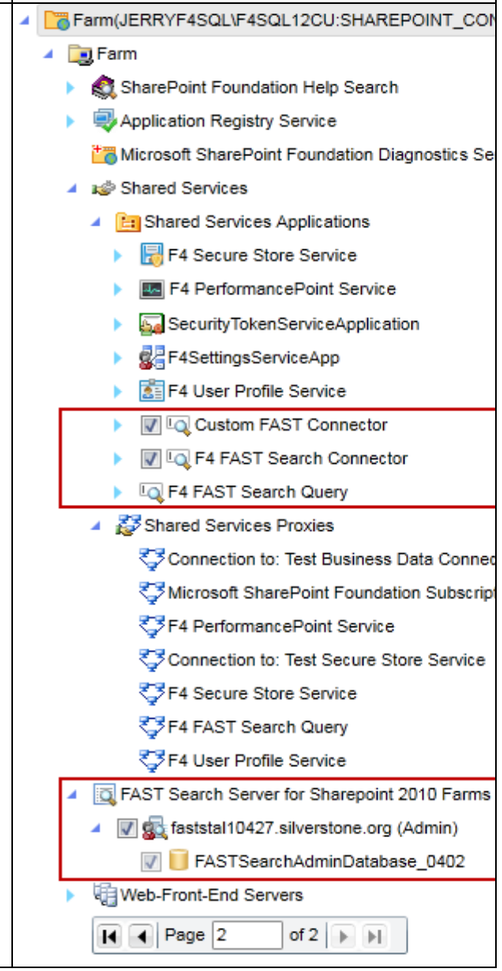
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SPUserCode V4	√	√						Type: Microsoft SharePoint Foundation Sandboxed Code Service Description: Settings for the Sandboxed Code Service.	

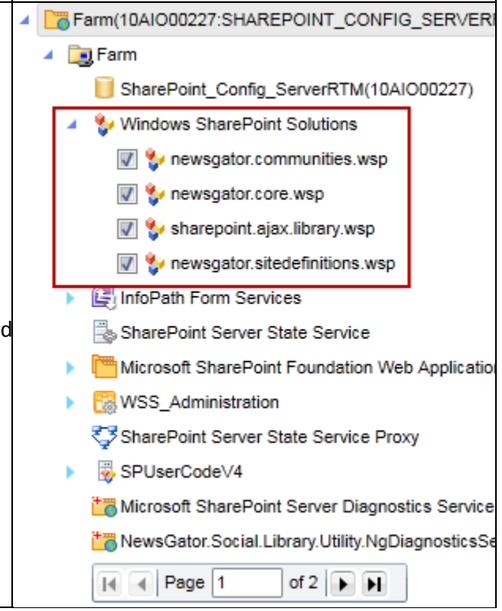
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Global Search Settings 	√	√							
SharePoint Foundation Help Search	√	√						Type: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

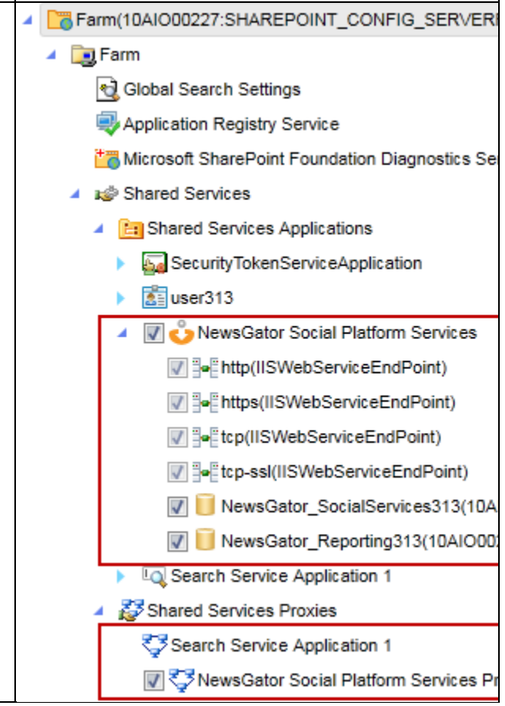
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
									

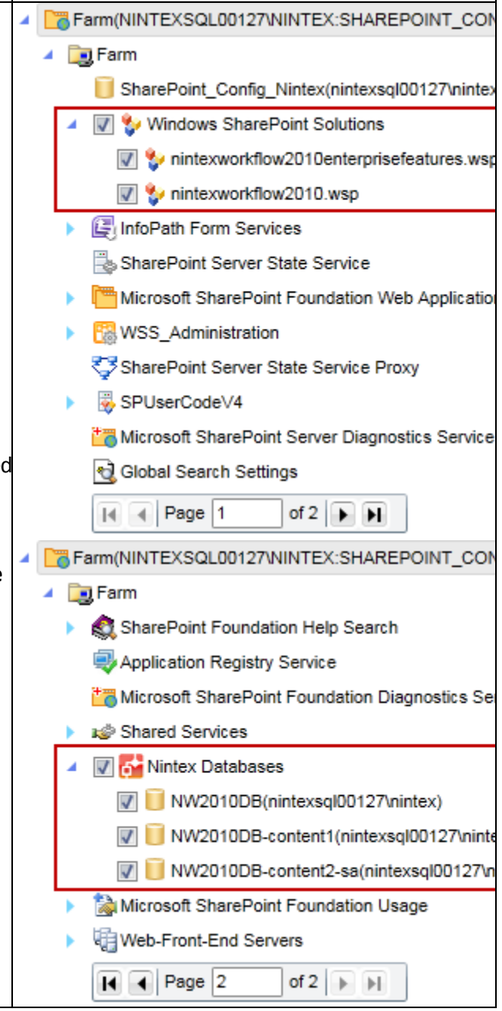
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Search Service Application	√	√						1. Search Service Settings: It is a virtual node that does not exist in SharePoint and it contains the following components: • Content Source • Crawl Rules • File Types • Crawl Impact Rules • Authentication Pages • Federated Locations • Metadata Properties • Scopes 2. 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. 3. 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. 4. Index Partition and Query Component: Under the **Server** drop-down list, all the SharePoint servers that can run the **Search Service Instance** will be displayed. No matter whether the service is enabled or not, the service can be restored normally. After the restore, the **Search Service** will be started on the specified SharePoint server.	

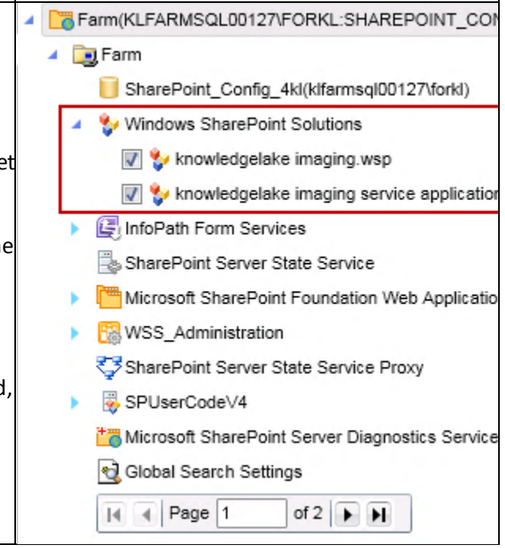
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Managed Metadata Service Application	√	√						1. **http (IISWebServiceEndPoint)** and **https (IISWebServiceEndPoint)** are the EndPoint groups of the IIS Web Service. They are also called **Service Application Endpoint Group** in SharePoint. 2. Service Applications that have no database or proxy: Access Services Service Application, Excel Services Application and Visio Graphics Service Application. 3. When restoring the service application proxy, a new proxy having the same name and type will be created in the target farm, and all the SharePoint will be restored and preserved. In an **Out of Place** restore, the service application proxy can be restored together with its service application or it can be restored alone. • In the **Connect to this specific application** drop-down list, all the destination service applications of the same type will be displayed and you can select one service application to restore to. • When entering the **Farm or application address**, you must enter the URL of the shared service application published by another farm. • In the **Default Proxy List** area, if you select **Yes**, after the out of place restore, this proxy will be added to the default proxy group at the destination. If you select **No**, it will not be added to the default proxy group at the destination.	

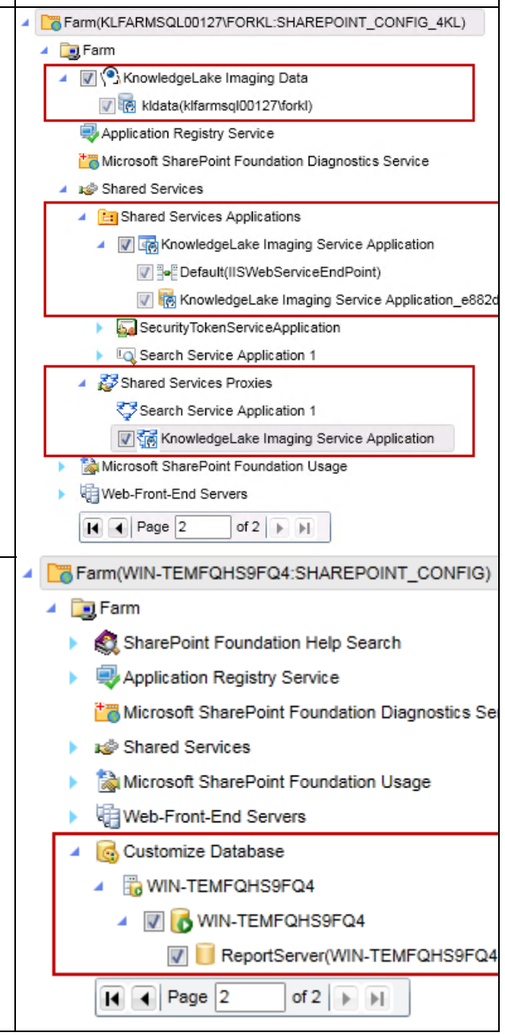
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
FAST Search Server for SharePoint 2010 Farms	√	√						This feature is specific to SharePoint 2010.	

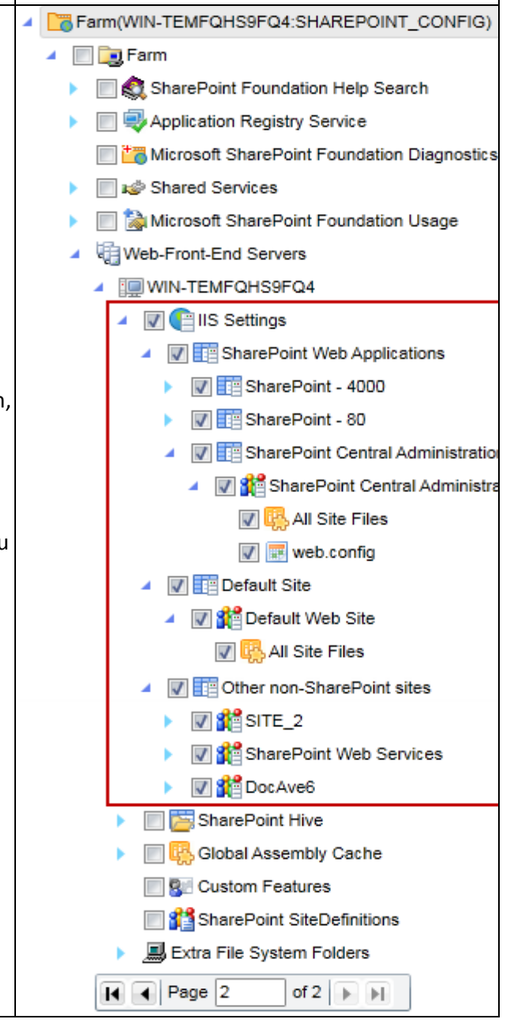
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
NewsGator Social Site 2010	√	√						Platform Backup and Restore supports NewsGator 1.2 and 2.5 for SharePoint 2010, and supports NewsGator 4.0 and 5.0 for SharePoint 2013. NewsGator Social Site must be installed in the target farm first. If you have uninstalled the NewsGator Social Site and want to restore it, make sure all the nodes are selected. Only **In Place** and **Restore Raw Database** restore type is enabled when restoring NewsGator Social Site. 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.	

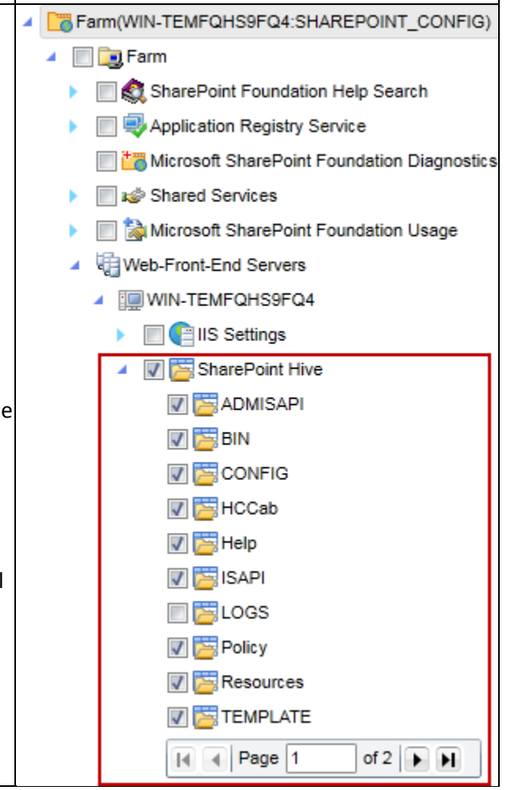
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
									

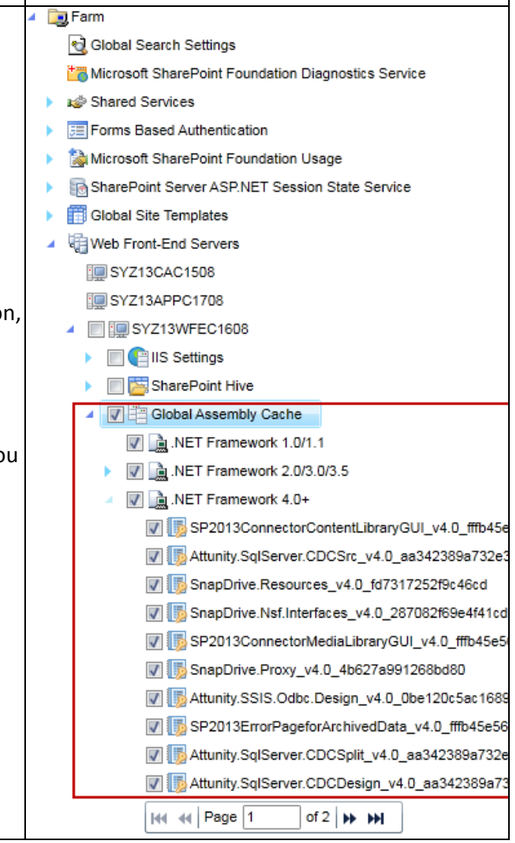
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Nintex Workflow 2010	√	√						Nintex Workflow 2010 or Nintex Workflow 2013 must be installed in the target farm first. Only **In Place** and **Restore Raw Database** restore type is enabled when restoring Nintex Workflow. 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.	

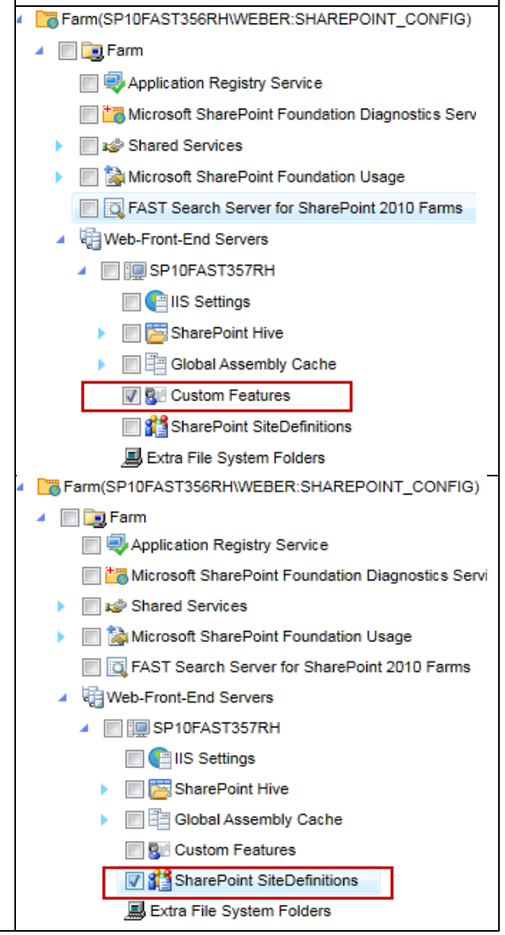
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
KnowledgeLake Imaging 2010	√	√						This feature is specific to SharePoint 2010. 1. 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. 2. Only **In Place** and **Restore Raw Database** restore type is enabled when restoring KnowledgeLake Imaging 2010. 3. 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.	

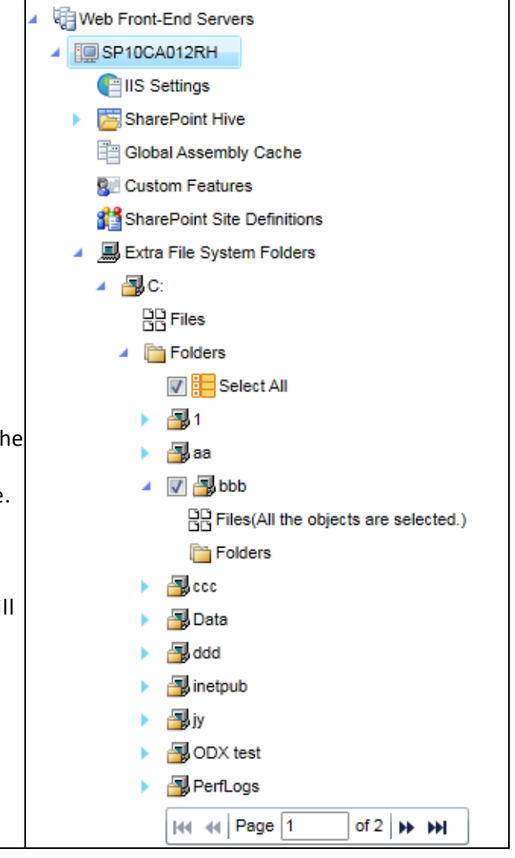
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
									
Custom Database	√	√						You cannot select detailed content inside the database to restore. You can only restore the whole database.	

What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
IIS Settings	√	√						If the data you want to restore does not exist in the destination, the data will be restored to the destination no matter you choose **Overwrite** or **Skip** option. 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.	

What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Hive	√	√						1. After performing the full backup, add some data and perform the incremental or differential backup. If you do not delete the added data and perform the **Overwrite** restore of the full backup data, the newly added data will not be deleted by DocAve. 2. After performing the full backup, modify some data and perform the incremental or differential backup. If you do not delete the modified data and perform the **Overwrite** restore of the full/differential/incremental backup data, the data backed up before the modification will be restored back and the modified data will not be deleted by DocAve. 3. After performing the full backup, delete some data and perform the incremental or differential backup. If you perform the **Overwrite** restore of the differential/incremental backup data, the deleted data will be restored by DocAve.	

What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity: Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level	Note	What to Select When Restoring
Global Assembly Cache	√	√						If the data you want to restore does not exist in the destination, the data will be restored to the destination no matter you choose **Overwrite** or **Skip** option. 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.	

What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Custom Features	√	√							
SharePoint Site Definitions	√	√							

What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Extra File System Folders	√	√						1. After performing the full backup, add some data and perform the incremental or differential backup. If you do not delete the added data and perform the **Overwrite** restore of the full backup data, the newly added data will not be deleted by DocAve. 2. After performing the full backup, modify some data and perform the incremental or differential backup. If you do not delete the modified data and perform the **Overwrite** restore of the full/differential/incremental backup data, the data backed up before the modification will be restored back and the modified data will not be deleted by DocAve. 3. After performing the full backup, delete some data and perform the incremental or differential backup. If you perform the **Overwrite** restore of the differential/incremental backup data, the deleted data will be restored by DocAve.	

Notes for Appendix J

Below are the detailed notes that are referenced in Appendix J: Customization Support Table.

Workflow Definition and Instance

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

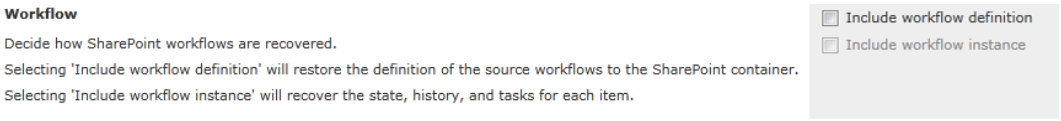


Figure 103: Workflow restore options.

1. 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.
2. **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 with an **In Progress** status at backup 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 where the workflow instance is based on skips being restored to the destination, the workflow instance will not be restored. If the content is restored to the destination and there is an existing destination workflow definition having the same name as the 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.

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:

1. Login to DocAve and navigate to **Data Protection** > **Platform Backup & Restore** > **Platform Backup**.
2. On the **Backup** tab, load the SharePoint farm tree in the **Scope** area to display the **FAST Search Server for SharePoint 2010 Farms** node. Then expand the node.
3. 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.
4. Click **Plan Builder** on the ribbon and choose **Wizard Mode** or **Form Mode** to create the plan and run it. You can view the job status in Job Monitor by clicking the corresponding button on the ribbon.

***Note**: Only Full backup is supported for the FAST Search Server farm. The Differential and Incremental backups are also Full backups with different Job IDs. FAST Content SSA and FAST Query SSA databases use simple model, so only Full backup and Differential backup are supported.

***Note**: In step 3, 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.

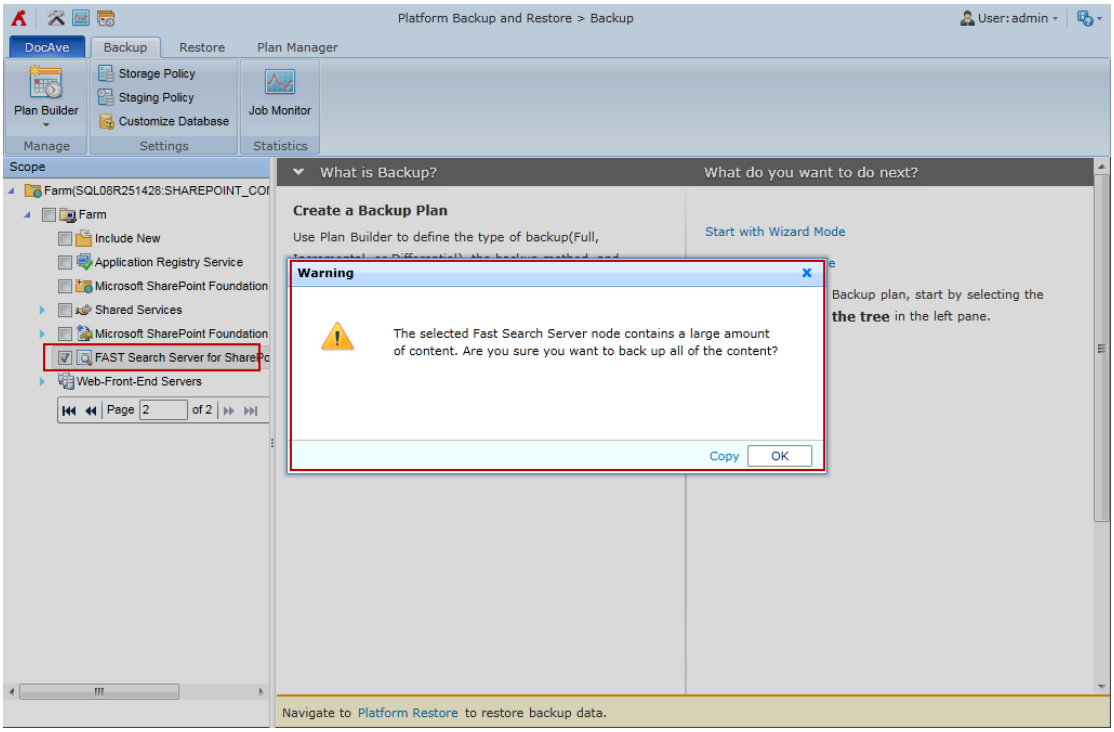


Figure 104: Warning message after selecting the content to back up.

Restoring the FAST Search Server

Follow the steps below to restore the FAST Search Server:

1. Login to DocAve and navigate to **Data Protection** > **Platform Backup & Restore** > **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.

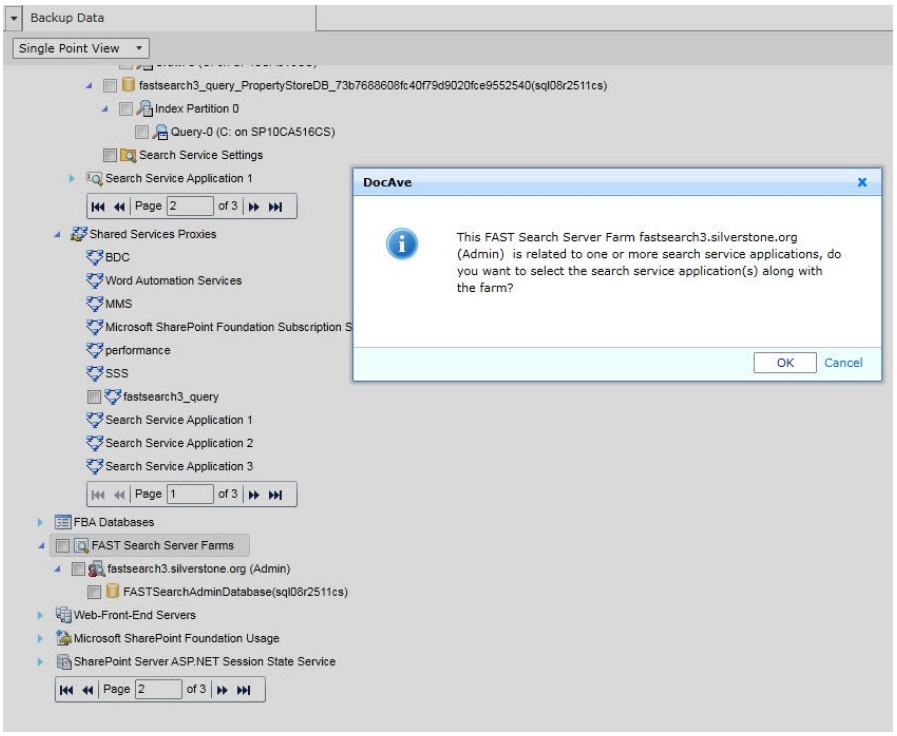


Figure 105: Prompt window after selecting the content to restore.

4. Only **In Place** restore type and **Overwrite/Skip** conflict resolutions are supported.

   In the **Advanced** field:

   a. If no checkboxes are selected, only the backed-up files on the backed-up FAST Search Server will be restored.

   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.

5. 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.

***Note:** If you selected **FAST Search Server for SharePoint 2010 Farms** node and perform the restore using the **Restore Raw Database** option, only the FAST Search Admin database is restored to the specified SQL instance. However, the FAST Search Servers backup data is not restored.

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)/(data_index)	On Stand-alone FAST server	Supported
	On FAST primary non-admin server	Supported
	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

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 © 2012-2017 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