DocAve® 6 Platform Backup and Restore

User Guide

Service Pack 3 Cumulative Update 2

Revision J

Issued October 2013

Table of Contents

About DocAve Platform Backup and Restore 5

Complementary Products 5

Submitting Documentation Feedback to AvePoint 5

Before You Begin 6

Configuration 6

Agents 6

Required Permissions 7

Agent Account Configured on the SharePoint Agents Included in the Agent Group 7

Agent Account Configured on Other SharePoint Web Front-End Servers (Except for SQL Server and FAST Search Server) 8

Agent Account Configured on the FAST Search Server 8

Agent Account Configured on the SQL Server 9

SQL Server Service Account Configured on the SQL Server 10

Local System Permissions 10

Supported Hardware in DocAve 6 Platform Backup and Restore 10

Getting Started 11

Launching Platform Backup and Restore 11

User Interface Overview 12

Configuring Devices and Setting up Storage Policies 13

About the Staging Policy 14

Configuring a Staging Policy 15

Selecting Content to Back Up 17

Using the Customize Database Feature 18

Overview of Backup Types 19

SharePoint Components Supported for Backup 21

Using Plan Builder to Back Up Data 23

Using Wizard Mode to Create a Backup Plan 23

Backup Schedule 28

Manual Maintenance 29

Snapshot Retention Policy 30

Using Form Mode to Create a Backup Plan 35
Running a Backup Job Immediately 35
Managing Plans 36
Configuring Run Now Interface 37
About InstaMount 38
InstaMount Mapping and Restore Index 38
About the Platform Backup and Restore for SQL Mirroring Database 39
About the Platform Backup and Restore for Failover Database 40
Performing a Restore 41
Building a Restore Plan 41
Building an In Place Restore Plan at Database Level 43
Building an In Place Platform Granular Restore Plan 45
Building an Out of Place Restore Plan at the Database Level 50
Building an Out of Place Platform Granular Restore Plan 53
Restoring a Raw Database 59
Options for Restoring Backed-up Web Front-end Files 59
Restoring Backed-up BLOB Data 60
Restoring Backed-Up Stub Database 60
Restoring Backed-Up Database Master Key 62
Deselecting the Restore Granular Content Feature 63
Restore Details for Specific Farm Components 63
Performing a Disaster Recovery 65
Performing a Farm Rebuild 66
Checking a Job Status 70
Performing a Full Farm DocAve Platform Out of Place Restore 71
Backing Up the Source Farm Using Platform Backup 71
Performing the Out of Place Platform Restore 71
Restoring Windows SharePoint Solutions, InfoPath Form Services and Global Search Settings 76
Restoring Web Applications and Content Databases 77
Restoring Service Applications 83
Restoring Backed up Web-Front-End Servers Data 102
DocAve 6 Platform Backup and Restore Use Case 104

Backing up the Entire SharePoint Farm 104
Restoring the Platform 104
Appendix A – Accessing Hot Key Mode 106
Backup Tab 106
Restore Tab 107
Time-Based Restore 107
Plan Manager Tab 108
Appendix B – SharePoint 2010 Components Supported in Platform Backup and Restore 109
Supported Web Parts 109
Service Applications Supported for Restore 111
Components Supported for Restore 113
Appendix C – SharePoint 2013 Components Supported in Platform Backup and Restore 116
Service Application Supported for Restore 116
Components Supported for Restore 118
Appendix D – SharePoint 2013 Social Features Supported in Platform Backup and Restore 119
Appendix E – SharePoint Object Security and Property 120
Appendix F – Advanced Settings in Configuration Files 121
AgentCommonWrapperConfig.config 121
Restoring Specified Web Properties 121
Appendix G – Customization Support Table 122
Notes for Appendix G 147
Workflow Definition and Instance 147
Backup and Restore FAST Search Server for SharePoint 2010 Farms 148
Notices and Copyright Information 152

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.

***Note:** 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. You can Submit Your Feedback 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.

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 components of the specified Search Service Application
- The SharePoint Foundation (Help) Search server where you want to back up the components of the SharePoint Foundation (Help) Search
- Each SharePoint server where you want to back up the following 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, make sure the **Agent Name** field matches the cluster virtual node name.

- 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.

***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 both SharePoint 2010 and SharePoint 2013, 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
    - Database Role of **public**, **dbcreator** and **Security Admin** to 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**.)

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 used to start 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) used to start the **SharePoint Server Search 14** service must be added to the **Administrators** group on the corresponding machine. In SharePoint 2013, the user (logon user) used to start 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

    - Database 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 SQL Server

1. Local System Permissions

    - Member of the **Backup Operator** local group
    - **Create global objects** permission and the **Impersonate a client after authentication** permission in the **Local Computer Policy** > **User Rights Assignment**
    - Full Control to the Registry of *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server*
    - Full Control to the directory of *C:\Windows\Temp*
    - DocAve Agent Service logon user
    - Full Control to the directory of the DocAve Agent installation directory *…\AvePoint\DocAve6\Agent*
    - Permission to cancel all the annotations in the **SMSvcHost.exe.config** file
    - **Read** and **Write** permissions to the directory of the database files in the restore destination

      ***Note**: The user used to enable the InstaMount must be a member of the **Administrators** local 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.
    - Database role of **dbreator** and **Process Admin** permission to SQL server.
    - **Read** and **Write** permissions to the **Temporary Buffer**, which is configured in **Control Panel** > **Agent Monitor** > **Configure**.

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

      The user used to restore 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

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**.

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 Hardware in DocAve 6 Platform Backup and Restore

Windows Storage Server 2008 R2 Enterprise and Dell EqualLogic FS7500 are supported.

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.

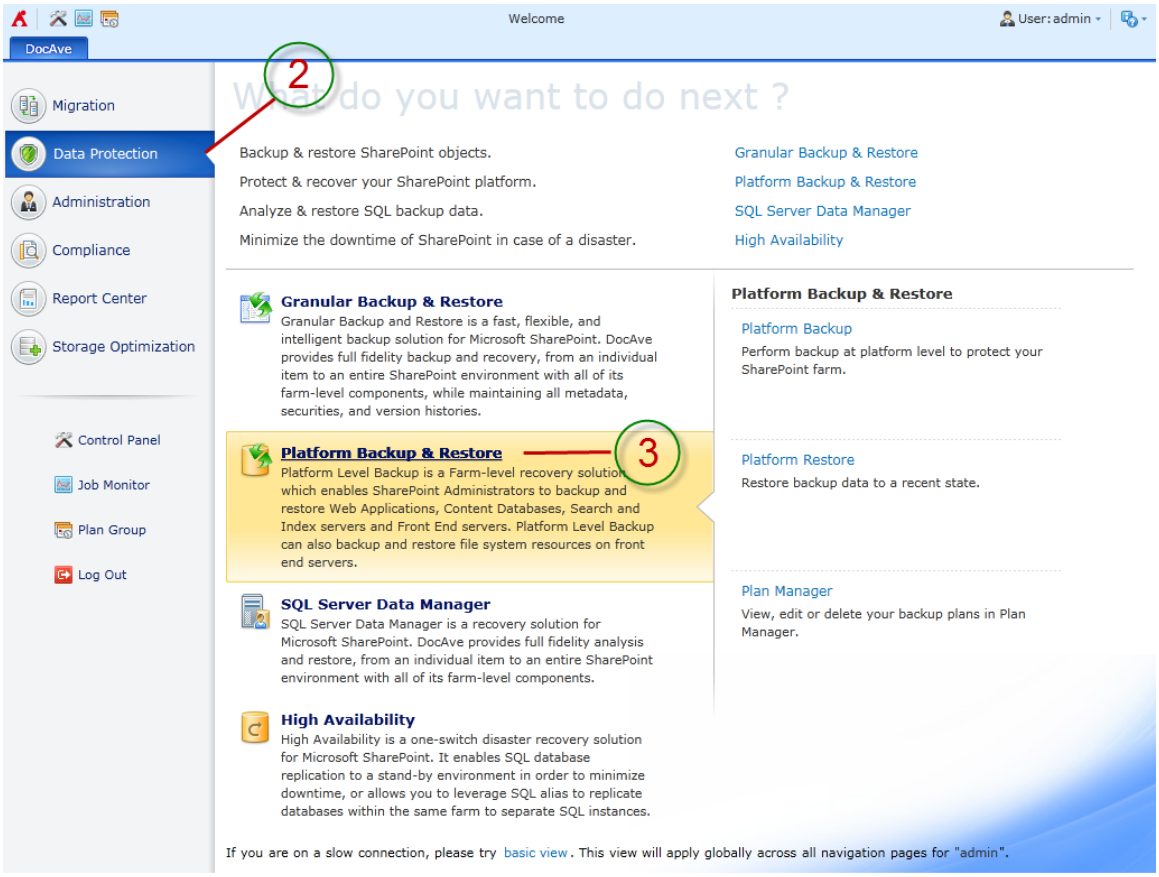


Figure 1: DocAve module launch window.

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.

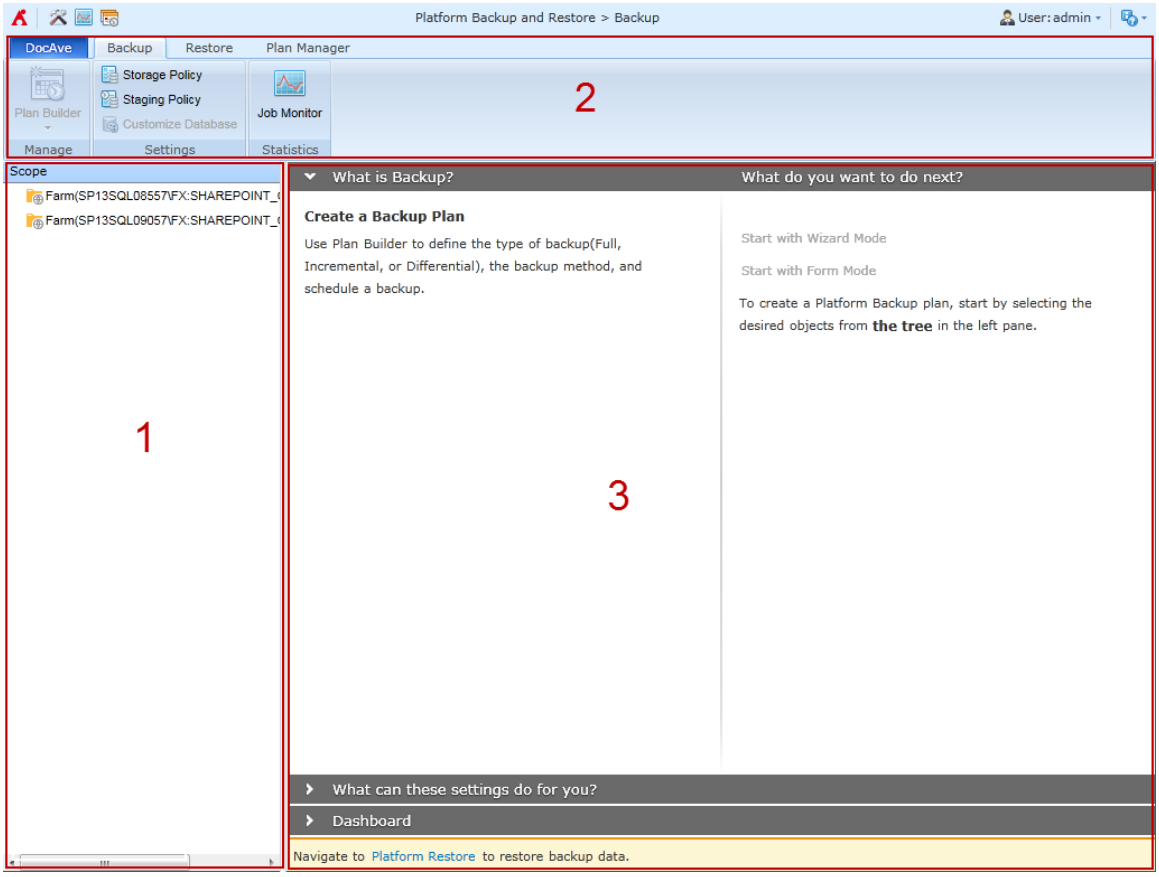


Figure 2: Platform Backup and Restore user interface.

1. The **SharePoint tree** (**Scope** panel) displays all content within your farms. Use this panel to select the content that you wish to perform actions on. Selecting content often reveals new tabs and functionality on the **ribbon**.
2. 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.
3. The **workspace** shows all form-based content that is used during the configuration of actions performed in DocAve products.

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 Net Share, FTP, TSM, EMC Centera, Cloud Storage, Dell DX Storage, Caringo Storage, and HDS Hitachi Content Platform device.

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

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 specified in the staging policy. When you perform the Platform granular level restore that uses InstaMount, the SQL Server specified 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 **Use InstaMount to Index Granular Content** option enabled. The backup data index used in the granular restore is generated from the InstaMount temporary database.

- If a staging policy is specified in the backup plan, the InstaMount temporary database is created on the SQL Server that you specified in the staging policy.
- If the staging policy is not specified 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 index mapping** option enabled and selecting a custom SQL server for InstaMount.

- If you select the **Customize SQL Server** radio button and specify a staging policy, the InstaMount temporary database is created on the SQL Server that you specified in the staging policy.
- If you select the **SQL Server for backup** radio button, 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 specified 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 specified 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 specified when running the restore job, the InstaMount temporary database is created on the SQL Server that you specified in the staging policy.

- If the staging policy is not specified 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. **Platform Type** – Describe the software platform that is going to use this staging policy.
    c. **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.
    d. **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 account and password. The specified account must be added to the **sysadmin** role in SQL Server.

          Click Validation Test to verify the access to the SQL Server.
    e. **Temporary Database Configuration** – Set up the configuration of the temporary database.

- **Minimum amount of free space to leave** – Specify the minimum amount of free 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 specified here does not exist in the specified location before a job starts, or if the entered amount will not exist after the temporary database is stored to the specified location, then the corresponding job will fail.
- **Temp database file location** – Specify 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** – Specify 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*.

Selecting Content to Back Up

After launching the Platform Backup and Restore user interface, the **Scope** panel on the left of the screen displays the root node of the farm.

***Note:** It is not supported to select the nodes both on the SharePoint 2010 tree and SharePoint 2013 tree.

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

1. Click the farm node to expand the tree; this displays all SharePoint components (databases, services, solutions, 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.

   If desired, select the **Include New** node to include any newly-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
   - Windows SharePoint 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
2. 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/newly-created Web applications under the **Microsoft SharePoint Foundation Web Application** node
   - The **Finance Web** and **HR Web** Web applications

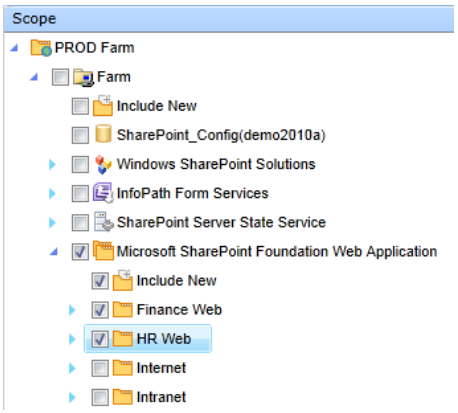


Figure 3: Selecting SharePoint farm content.

3. After selecting content, you are able to build a backup plan using Platform Backup and Restore.

Using the Customize Database Feature

Use the **Customize Database** feature to manually add to the SharePoint component tree any customized databases that are not listed. Such databases include the database of a solution, the database of third party software, and so on.

Once a customized database is added to the tree, it can be backed up as normal using a Full, Incremental, and Differential backup.

1. On the **Backup** tab, in the **Settings** group, click **Customize Database**. The **Customize Database** window appears.
2. In the **Customize Database** window, click the **Custom Database** node on the right panel to expand the tree. All customized databases on all of the SQL Servers that have DocAve Agents installed are listed under the corresponding SQL instance node in the tree.
3. Select the databases that you want to be displayed on the backup tree by selecting the checkbox next to the database.
4. When finished, click **OK**. The selected database is now shown on the backup tree under the **Customize Database** node.

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 specify the type of backup to perform: **Full**, **Incremental**, or **Differential**.

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 substantial in size, depending upon the size of your SharePoint environment. Unlike Incremental and Differential backups, all Full backups are independent of one another and do not have any dependencies on other backup data files. However, because each of the backups is comprehensive, 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. 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:

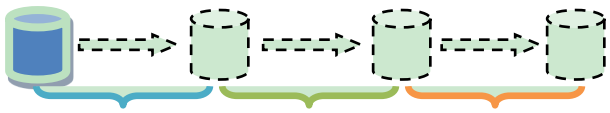


Figure 4: One Full backup followed by three Incremental backups.

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.

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:

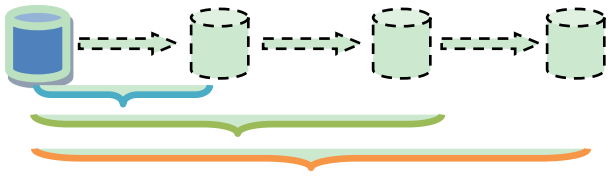


Figure 5: One Full backup followed by three Differential backups.

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

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, and search database are supported. These databases are backed up by the SQL Member Agent using Platform Backup.

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

- 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.

- 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 – 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 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.

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, and search 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.
- 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, 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.
- 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**: The following SharePoint 2013 objects are not supported to be backed up and restored by DocAve Platform Backup and Restore: SharePoint 2013 APP service and APP catalog, Windows Azure workflows, and Office 2013 Web Apps Server.

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. After selecting the content to back up, 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.

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

2. Select the backup option. Refer to Overview of Backup Types for supplemental information on backup types.

   - **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.

     - **Perform log backup after full backup** – Select this option to 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.

- **Use DocAve Platform Backup and Restore in addition to other existing SQL backup methods for SharePoint databases** – Select this option if DocAve Platform Backup and Restore is being used in addition to 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 in addition to other existing SQL backup methods for SharePoint databases**, only Full backup is supported.

Click **Next**. The **Storage Policy** page appears.

3. Specify 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.
4. Specify 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, better quality data set. Note that small data sets cause slower backup and restore times. 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 restore times. Select whether to leverage DocAve Media Server (**Media Service**) resources or SharePoint Server (**SharePoint Agent**) resources for encryption. Then select a security profile to be used 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 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.
5. Click **Next**. The **Backup Method** page appears.

6. Choose whether or not to **Create Persistent Snapshots** of the selected objects. Creating persistent snapshots retains the snapshot after the backup job is completed. This enables you to defer the coping of the backup data from the persistent snapshot to the corresponding storage policy until the specified maintenance job is performed. For more information, refer to Step 12: Maintenance Options.

   DocAve recommends using creating 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.

   If you select **Yes**, DocAve saves a snapshot on the specified hardware when each backup is initiated. This snapshot contains the content database's files and transaction log that will be backed up.

   As this option uses less system resources when **Copy data from snapshot to media server** is selected, it is recommended that you select **Create Persistent Snapshots** if you plan to run backups during working hours. If you select **No**, the snapshot will be deleted after the backup job. If you select **Yes**, the following options appear and must be configured.

   a. Configure the **Snapshot Retention Policy**. Enter in the textbox the maximum number of snapshots the current plan can take. Considering performance, it is not recommended that the value of this attribute 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 specified value. For more information, refer to Snapshot Retention Policy.

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

8. Choose whether or not to **Enable InstaMount Mapping for Granular Restore**. InstaMount makes item-level restore more efficient, as it uses 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 is supported for the storage policy using the storage type of Net Share, TSM, DELL DX Storage, or HDS Hitachi Content Platform.

   a. If selecting **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.

   b. **Associated Plan Group** – Select the plan groups from the drop-down list to add the plan to the corresponding groups. The added plan will run according to the related plan group settings. You can also choose to create a new plan group by clicking the **New Plan Group** link in the drop-down list. For more information on plan group, refer to the DocAve 6 Control Panel Reference Guide.

c. To inform specified 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.

d. **Agent Group** – Specify an Agent group to run the backup job for load balancing and performance. Click **View** to view the details of the specified Agent group.

9. Click **Next**. The **Schedule** page appears.
10. Define the **Schedule type** selection:

- **No schedule** – Select this option to run the plan immediately and save the plan 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 **X** 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.

11. Click **Next**. The **Maintenance** page appears.
12. Configure the following maintenance settings:

a. **Maintenance Options** – Choose the operations to be 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 specified number of latest backups is sent to the storage policy selected in the Storage Policy step.

- **Generate InstaMount mapping for last … backup(s)** – This option generates InstaMount mapping for the specified number of latest backups in the selected Storage Policy. The generated mapping is used in Platform granular restore.

  ***Note**: If you did not enable the InstaMount granular restore in the **Advanced** step but still want to generate InstaMount mapping, you can generate the InstaMount mapping in a later maintenance job using this selection.

- **Generate granular restore index for last … backup(s)** – This option generates the granular restore index for the specified number of latest backups in the selected Storage Policy. The index is used in Platform granular restore.

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

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

b. **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 **X** to delete a schedule.

c. **Maintenance Notification** – To inform specified 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.

13. When finished, click **Next**. The **Overview** screen appears.
14. 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.
15. 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.

16. On the lower-right section of the screen, or on the ribbon, click **Finish** to save the configuration of the plan without running it or **Finish and Run Now** to save the configuration and then run the saved plan immediately. The backup plan is now listed in Plan Manager.

Backup Schedule

Configure the following settings to build a new backup schedule.

1. **Backup Options** – Choose backup options 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.

   - **Transfer data from snapshot to media server** – Copies the snapshot data from the hardware to the corresponding logical device. If this option is unchecked, no backup data is written to the logical 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.

     - **Defer transferring data from persistent snapshot** – The snapshot data is not copied to the logical device during the backup job. If you select this option, the snapshot data is copied to the corresponding logical device in a scheduled/manual maintenance job that is run after the backup job completes.

   - **Defer generating InstaMount mapping** – The InstaMount mapping is not generated for the backup data in the corresponding logical device. The mapping can be generated using a scheduled or manual maintenance job that is run after the backup job completes, browsing the index in InstaMount when configuring the **Item Level Settings** in the **Data Selection** step of **Restore Wizard**, or selecting **Use InstaMount** in the **Restore Settings** step of **Restore Wizard**.

2. **Restore Granularity Level** – Select the restore granularity level for the scheduled backup job. After selecting the Restore Granularity Level, you can expand the tree to the level you specified when running a restore job. If you select **None**, no granular restore index is generated.

   - **Defer generating granular restore index** – Selecting this option does not generate a granular restore index for the backup data in the corresponding logical device. The index can be generated using a scheduled or manual maintenance job that is run after the backup job completes.

3. **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.

4. **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 specified BLOB data.

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

5. **Job Report** – Specify the level of reporting for the backup job**. Simplified** means to create a summary of the backup data**. Detailed** means to create a detailed report that contains all of the information of the Web front-end backup objects at the cost of performance.
6. **Type –** Select the interval at which the backup occurs.
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**, set up the advanced settings for the frequency. For more scheduling options, select the **Advanced** checkbox to reveal additional options.
8. **Range of Recurrence** – Select the start time and end time for the schedule.
9. 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; such deferred operations include defer copying data from persistent snapshot, defer generating InstaMount mapping, or defer generating a granular restore index.

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/finished with exception.

To inform specified 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.

***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 referred to 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/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** – The current job's oldest snapshot is deleted directly from the hardware, and all jobs related to the deleted snapshot fail. A new job for the current plan then starts.

   Note the following:

   - 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 specified in Platform Backup and Restore Plan Builder.

***Note**: 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.

   Note the following:

   - 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:

<VolumeConfig providerOption="0" MaxSnapshotCount="32">

<DriverLetter path="c:"/>

</VolumeConfig>

```
<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 6: Modified configuration file.

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

- **providerOption** – Specify 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 specified provider. The provider ID in **providerId** attribute must be specified 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 7.

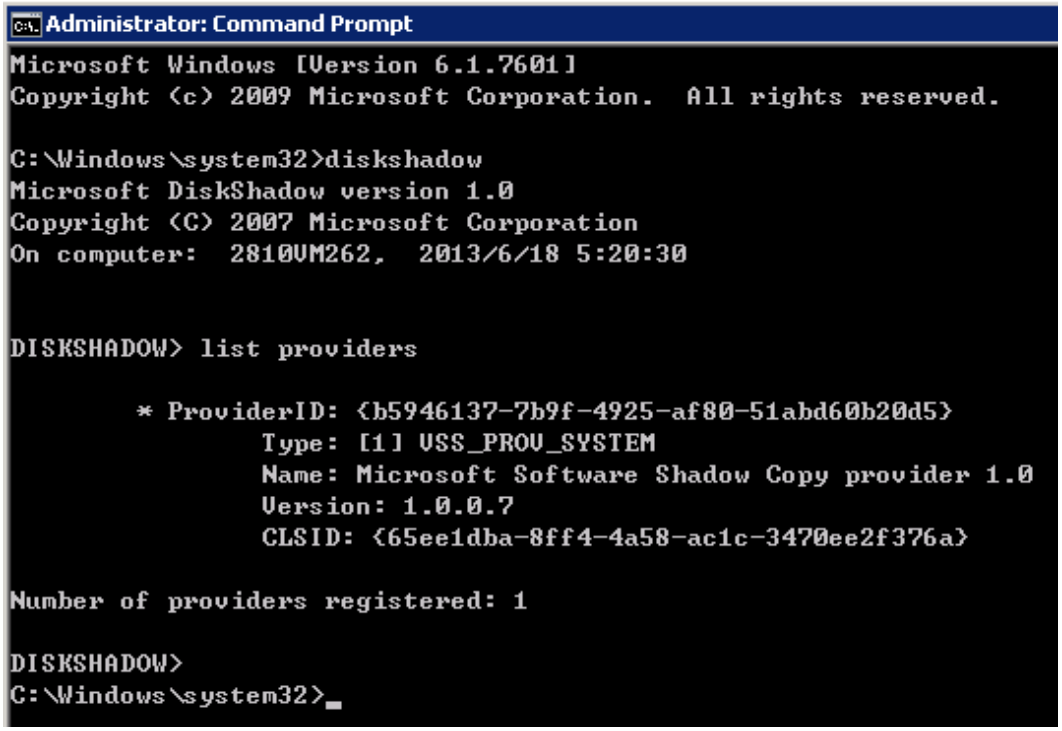


Figure 7: Viewing the provider IDs.

- **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.

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 **OK 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**.

Customize how these plans are displayed in a number of different ways:

- **Search** – Filter the plans to be displayed by the keyword entered in the **Input Keyword** text box (the keyword is not case sensitive). The keyword must be contained in a column value. You can select **Search all pages** or **Search current page** to define the search scope. **Search all pages** means that the plans in all of the pages whose column contains the keywords will be displayed; while **Search current page** means that only the plans in the current page whose column contains the keywords will be displayed.
- **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.
- **Filter the column** (▽) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column heading in a column you want to filter, and then select the filter the column button (▽). Check the checkbox next to the item name to have that item shown in the list.

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

- **View Details** – Select a plan and click **View Details**. The backup scope and the plan settings are displayed on the **View Details** interface. When you want to change the nodes you selected or want to modify the migration 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, configure the settings below:

- **Options** – Specify the type of the backup job you want to run on the selected plan. You can select the **Full Backup**, **Incremental Backup**, or **Differential Backup** from the drop-down list, and then specify whether or not to transfer the data from snapshot to media server immediately after snapshot is complete (**Transfer data from snapshot to media server**), defer transferring data from persistent snapshot until the specified time in Maintenance schedule (**Defer transferring data from persistent snapshot**), or defer generating the InstaMount mapping until the specified time in Maintenance schedule (**Defer generating InstaMount mapping**).

  ***Note:** The incremental backup does not support to configure the settings above.

- **Restore Granularity Level** – Select the granular restore index level for browsing the restore content. You can select **Site Collection Level**, **Site Level**, **Folder Level**, **Item Level**, **Item Version Level**, and **None** as the granular restore index level. Selecting the **Defer generating granular restore index** checkbox will defer the generation until the specified time in Maintenance schedule.
- **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.
- **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 specified BLOB data.

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

- **Job Report** – Specify the job report type. **Simplified** means to create a summary of the backup data. **Detailed** means to create a detailed report that contains all of the information of the Web front-end backup objects at the cost of performance..
- 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 Granular Restore** 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 reading speed of your device is slow, using InstaMount may lead to the job failover for session timeout. DocAve recommends not using InstaMount in this case.

***Note**: For DocAve 6 Service Pack 3 Platform Backup and Restore, only the physical device in the storage type of DELL DX Storage, TSM, HDS Hitachi Content Platform, or Net Share supports to use InstaMount.

InstaMount Mapping and Restore Index

The InstaMount mapping file is generated from backup data; it is used to generate the temporary files used by the InstaMount function. The granular restore index is used for Platform granular restore. The mapping file can be generated when browsing the index in InstaMount or during a Platform Backup job, a Platform Restore job, or by a maintenance job. The granular restore index can be generated during a Platform Backup job or by a maintenance job.

- When running a Platform backup job with **InstaMount Granular Restore** 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 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 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 Failover Database

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

- Content Database
- PerformancePoint Service Application Database
- Managed Metadata Service Database
- Secure Store Service Application 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 failover databases supported for Platform Backup and Restore.

- Content Database
- PerformancePoint Service Application Database
- Managed Metadata Service Database
- Secure Store Service Application Database
- User Profile Service Databases
- App Management Service Database
- Subscription Service Database
- Session State Service Database
- Application Registry 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 Restore Details for Specific Farm Components for important information regarding the restore of farm components.

***Note**: To successfully restore a SharePoint configuration database, first delete the existing configuration database from the SQL Server before attempting to restore it using DocAve Platform Backup and Restore.

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 a specified SQL Server.

***Note**: For information regarding the SharePoint components supported in Platform Backup and Restore, refer to Appendix B – SharePoint 2010 Components Supported in Platform Backup and Restore and Appendix C – 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 is to filter the full backup jobs in the last seven days.
    a. **Plan Filter** – 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. **Job Filter** – 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. **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 specify a time period. All of the Finished/Finished with Exception Platform backup jobs whose start time is in the specified time period are displayed.

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.
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 the Database Level
   - Building an Out of Place Platform Granular Restore Plan
   - Restoring a Raw Database
   - Options for Restoring Backed-up Web Front-end Files
   - Restoring Backed-up BLOB Data

***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** – 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 a content database to restore.
3. **Restore Type** – Configure the restore type and specify 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** – Specify an Agent group to run the restore job for load balancing and performance. Click **View** to view the details of the specified Agent group.
4. **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 restores the backed-up database, and then modifies the database to its most recent status using the log files that were backed up during an Incremental backup. Select **No** to restore only the backed up database.

    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 **Not Overwrite** 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. **Restore Option** – Specify 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.

   - **Not Overwrite** – 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. Configure the email **Notification** settings. 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.

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

5. **Schedule** – Choose whether or not to run 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.

6. 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.
7. Click **Finish** to save the job's configuration.

- If the restore job does not have a schedule, **Finish** runs the job immediately.
- If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Building an In Place Platform Granular Restore Plan

1. Follow the instructions given in Performing a Restore to begin building the plan.
2. **Data Selection** – Select the database that includes the granular content you wish to restore. Click the **View Details** link besides the specified node to view detailed information about the selected database.
3. Click the **Global Setting for Restoring Content, Property, and Security** link and configure the **Item Level Settings**:
    - **Restore Granular Content** – Configure the **Restore Granular Content** settings. If you do not select this option, the tree in the **Backup Data** pane can only be expanded down to the site collection level; the granular content cannot be selected. Refer to Deselecting the Restore Granular Content Feature for detailed information. Configure the following settings:
        - **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 E – SharePoint Object Security and Property.
            - **Only restore security –** Only restore the container's security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security of the container in the backup to the conflict container in the destination. **Replace** will delete the security of the conflict container in the destination first, and then add the security of the container in the backup to the conflict container in the destination.

              ***Note**: The **Only restore security** feature 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 E – SharePoint Object Security and Property.
- **Only restore security** – Only restore the content's security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security settings of the content in the backup into the conflict content in the destination. **Replace** will delete the security settings of the conflict content in the destination first, and then add the security of the content in the backup to the conflict content in the destination.

  ***Note**: The **Only restore security** feature 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.

- **Browse the stored index** – Select this option to browse the index that was generated according to the restore granularity specified when setting up the backup job or maintenance job.
- **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. If you want to change the location of the InstaMount temporary database, click the **Configure** link to select a staging policy for storing the InstaMount temporary database generated during browsing. For more information, refer to About the Staging Policy.

  ***Note**: If a granular restore index is generated for the specified Platform backup job, **Browse the stored index** will be selected by default; if the granular restore index is not generated for the specified Platform backup job, the **Browse the index in InstaMount** option must be used when restoring the backup using Platform granular restore.

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

   a. **Security** – Refer to Appendix E – SharePoint Object Security and Property for detailed information related to security.

   b. **Property** – Refer to Appendix E – SharePoint Object Security and Property for detailed information related to property.

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 specify 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. Specify the database authentication to use to access the customer backed up stub database.
    - Select **No** to restore the stubs from the original Connector device.
7. **BLOB Settings** – Choose whether or not to restore the granular data from the backed up BLOB data.
    - Select **Yes** to restore the granular data from the backed up BLOB data. If you select **Yes**, you are required to specify which backup method you 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.
8. When finished, click **Next**. The **Restore Type** page appears.
9. **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** – Specify an Agent group to perform the restore job for load balancing and performance. Click **View** to view the details of the specified Agent group.
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.
            - **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. **Include Recycle Bin Data** – 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 **Include Recycle Bin Data** 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.

c. **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.

d. **Use InstaMount** – Specify 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 Mapping and Restore Index for more information.

e. **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.

f. **Workflow** – Decide how the backed-up workflows are restored.

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

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

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

   ***Note:** If you did not select **Property** 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.

h. **Exclude User/Group Without Permission** – If you select **Yes**, the users/groups that have no permissions will not be restored. By default, **No** is selected.

i. **Version Settings** – Choose the Version Settings for the content being restored to SharePoint. To improve performance, limit the versions restored. **Restore all versions**

restores all versions of the backup data; while **Restore the latest version(s)** only restores the latest several **Major** or **Major and Minor** versions of the backup data as specified. The other versions are not restored.

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

j. **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.

2. When finished configuring Restore Settings, click **Next**. The **Schedule** page appears.
3. **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. 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.

4. 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.
5. 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 the 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** – 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 database.
3. **Restore Type** – Choose where the content will be restored.

   ***Note:** It is not supported to restore the data backed up from SharePoint 2010 to SharePoint 2013 or to restore the data backed up from SharePoint 2013 to SharePoint 2010. 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.
- **Agent Group** – Specify the Agent group that will perform the restore job for load balancing and performance. Click **View** to view the details of the specified Agent group.

4. Click **Next**. The **Destination Component Options** page appears.
5. **Destination Component Options** – Specify the restore options 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/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 specified here.
   - **Database and Log File Mapping** – Click **Details** to specify 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 specified 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 specified account and password. The specified account must be added to the **sysadmin** role in SQL Server.
   - **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.

6. **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 **Not Overwrite** 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.

    - **Restore Option** – Specify 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.

        - **Not Overwrite** – 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.

    - **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.

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

8. **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. 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.

9. 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.

10. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Building an 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** – Select the database that includes the granular content to restore. Click **View Details** next to the selected database to view the detailed backup data for the selected database.
3. In the **Global Setting for Restoring Content, Property and Security** interface, configure the **Item Level Settings**:

    - **Restore Granular Content** – Select this option to restore the granular content. If you do not select this option, the tree in the **Backup Data** pane can only be expanded down to the site collection level and you cannot select granular content. Refer to Deselecting the Restore Granular Content Feature for detailed information.
        - **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 E – SharePoint Object Security and Property.
            - **Only restore security –** Only restore the container's security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security of the container in the backup to the conflict container in the destination. **Replace** will delete the security of the conflict container in the destination first, and then add the security of the container in the backup to the conflict container in the destination.

              ***Note**: The **Only restore security** feature 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 E – SharePoint Object Security and Property.
            - **Only restore security** – Only restore the content's security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add

the security settings of the content in the backup into the conflict content in the destination. **Replace** will delete the security settings of the conflict content in the destination first, and then add the security of the content in the backup to the conflict content in the destination.

***Note**: The **Only restore security** feature 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.

- **Browse the stored index** – Browse from the index that was generated according to the specified restore granularity when backing up this database or performing the maintenance job.
- **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, click the **Configure** link to select a staging policy for storing the InstaMount temporary database generated during browsing. For more information, refer to About the Staging Policy.

  ***Note**: If a granular restore index is generated for the specified Platform backup job, **Browse the stored index** will be selected by default; if the granular restore index is not generated for the specified Platform backup job, the **Browse the index in InstaMount** option must be used when restoring the backup using Platform granular restore.

4. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the **Item Browser** pop-up window. Specify the configuration of the container being restored.
   - **Security** – Refer to Appendix E – SharePoint Object Security and Property for detailed information related to security.
   - **Property** – Refer to Appendix E – SharePoint Object Security and Property for detailed information related to property.
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 specify 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. Specify the database authentication to use to access the customer backed up stub database.

- Select **No** to restore the granular data from the original Connector device.

7. **BLOB Settings** – Choose whether or not to restore the granular data from the backed up BLOB data.
   - Select **Yes** to restore the granular data from the backed up BLOB data. If you select Yes, you are required to specify which backup method you 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:** It is not supported to restore the data backed up from SharePoint 2010 to SharePoint 2013 or to restore the data backed up from SharePoint 2013 to SharePoint 2010. Make sure that the source node and the destination node are in the same version of SharePoint. If the site within SharePoint 2013 is a SharePoint 2010 mode site, it can only be restored to the same mode site.

   a. **Restore Type** – Select the location where to restore the backup data. In this case, select **Out of place restore** to restore the content to another SharePoint farm or a different location in the original farm.

   b. **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.

c. **Agent Group** – Specify the Agent group that will perform the restore job for load balancing and performance. Click **View** to view the details of the specified Agent group.

d. **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.

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

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

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. l
  - **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. **Include Recycle Bin Data** – 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 **Include Recycle Bin Data** 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.

c. **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.

d. **Use InstaMount** – Specify 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 Mapping and Restore Index for more information.

e. **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.

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

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

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

***Note:** If you did not select **Property** 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.

h. **Exclude User/Group Without Permission** – If you select **Yes**, the users/groups that have no permissions will not be restored. By default, **No** is selected.

i. **Version Settings** – Choose the Version Settings for the content being restored to SharePoint. To improve performance, limit the versions restored. **Restore all versions** restores all the versions of the backup data; while **Restore the latest version(s)** only restores the latest several **Major** or **Major and Minor** versions of the backup data as specified. The other versions are not restored.

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

j. **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. This links to the corresponding setting page, allowing you to edit the configuration.
15. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

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 specified 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 specified SQL instance.
2. **SQL Instance** – Specify an SQL Instance to store the restored content database.
3. **Database Access Credentials** – Specify 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 specified account and password. The specified 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 specified here.
    b. **Database and Log File Mapping** – Click **Details** to specify the name and path of the destination database file/log file.

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

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 is used for checking the program installation status on the specified Web front-end server when backing up the specified Web front-end server components, as well as the current program installation status.
- **Download Backup List** – This function is used for checking data status on the selected Web front-end server when backing up the specified Web front-end server components, as well as the current data status. Click the **Download Backup List** button on the ribbon, select the corresponding checkboxes and click **OK**. A .zip file that contains detailed lists is downloaded to the specified local path. The list is recorded in the .csv file in the .zip file.

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

- **Restore 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 F – 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:** Only one BLOB node supports the granular level restore.

Restoring Backed-Up Stub Database

Select one stub database to restore the backed up stubs.

***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.

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**.

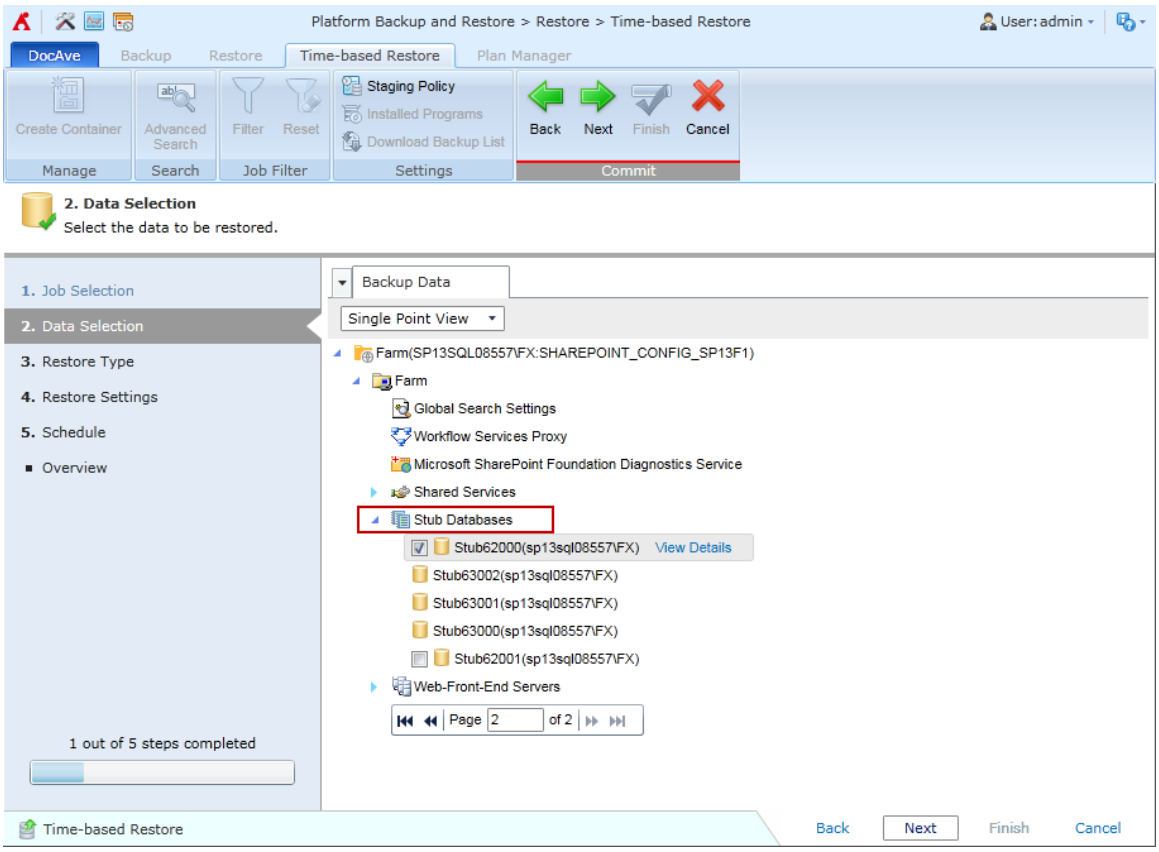


Figure 8: Select a stub database to restore.

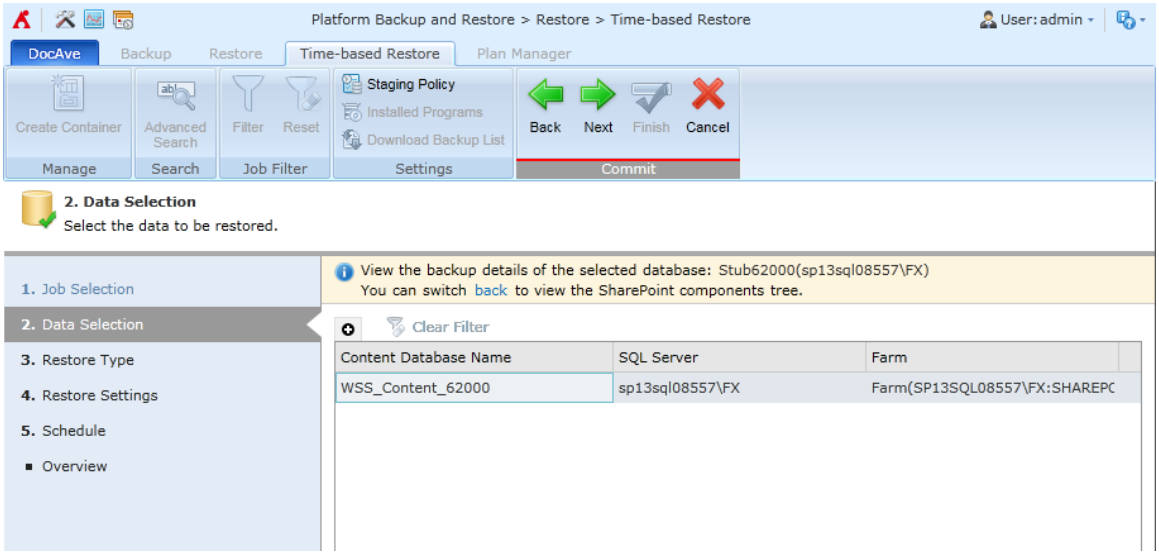


Figure 9: View the details of the stub database.

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** – Specify an Agent group to run the restore job for load balancing and performance. Click **View** to view the details of the specified Agent group.

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 **Restore Option** 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 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 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 **Not Overwrite** as the **Restore Option**.
5. Run the Platform Restore job to restore the backed-up database master key.

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 do not select **Restore Granular Content**, the tree in the **Backup Data** pane can only be expanded down to the site collection level, so granular content cannot be selected.

Restore Details for Specific Farm Components

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

- **Configuration database** – This is the core component of the SharePoint farm. It can only be restored using the **Restore Database Only** or Restoring a Raw Database. The SharePoint Configuration database can only be backed up and restored if the backup/restore includes the SharePoint Central Administration Content 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 settings and associated IIS sites. 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 solution will be restored to the related Web application and set the status as **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 database and index backups must be available.
- 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**: The SQL server cannot be installed on the SharePoint server. Otherwise, you will fail to restore the databases.

- 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.

***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.

Performing a Farm Rebuild

After you have backed up the whole farm using Platform Backup, you can use the **Farm Rebuild** function to perform a rebuilding of your farm when it is corrupted.

***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.

***Note**: The backed up **Web-Front-End Servers** nodes will not be restored during the farm rebuild, if necessary, restore the desired **Web-Front-End Servers** nodes after the farm rebuild.

To perform the farm rebuild, the following requirements must be met:

- A backup copy of the data for the entire farm (including the SharePoint configuration database and the central administration database) must be available.
- The SharePoint server topology should be identical to the topology at the time of backup. 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 (no matter SharePoint servers or SQL servers) on all of the servers in the farm rebuild environment.

  ***Note**: The SQL server cannot be installed on the SharePoint server. Otherwise, you will fail to restore the databases.

- All related software installed on the rebuilt destination should be the identical version and the patch level as before. Examples of related software are: SharePoint, SQL Server, DocAve, as well as the .NET Framework.

- User permissions on both the local server and SQL Server should be set to the same as before.

To perform a farm rebuild, complete the following steps:

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.

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

   a. **Plan Filter** – 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. **Job Filter** – 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. **Time Range** – Filter the full farm backup data by completion time range using this drop-down list.

      - **All Jobs** – Select this option to display all Finished/Finished with Exception Platform backup jobs.
      - **Backup jobs start within …** – Select this option to specify a time period. All of the Finished/Finished with Exception Platform backup jobs whose start time is in the specified time period are displayed.

   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/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 button 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.
3. **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.
4. **Disconnect Connection** – Disconnect the connections of 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 all the displayed SharePoint servers have already been disconnected from this farm, go to the next step directly.

5. **Restore Database** – Restore all the backed up databases in the full farm backup job. The databases are all restored with no attempt to connect them to the SharePoint environment according to the selected restore option.

    ***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.

    - **Restore Setting** – Specify whether or not to overwrite the original contents if there is a conflict between the original database name and that of the backed-up database.
        - **Not Overwrite** – 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.
6. 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, specify the restore setting and perform the restore job again. **SharePoint Configuration** – Configure the settings required for reconfiguring the restored SharePoint farm. You must enter the passphrase for this farm before reconnecting all the servers back. Select the **Specify Port Number** checkbox, and you are able to change the port used by the SharePoint 2010/2013 Central Administration. For now, only **NTLM** is supported as the security authentication type.

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

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

8. Click **Next**. The **Restore Index** page appears. DocAve restores the backed up index components to the target farm.
9. **Restore Index** – Restore all the index components of the search service applications backed up in the full farm backup job. The details about restoring the index components are listed in the table. Select a desired number from the **Show rows** drop-down menu to specify the number of index components displayed per page. Select **<** or **>** to turn to the previous or next page. 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.
10. **Overview** – View the current farm settings you have configured in Step 6.
11. Click **Finish** to finish the farm rebuild.

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.

Refer to the DocAve 6 Job Monitor Reference Guide for more information.

Performing a Full Farm DocAve Platform Out of Place 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 DocAve and navigate to **Data Protection** > **Platform Backup & Restore** > **Platform Backup**.
2. Click the farm name to load the tree and select the data (farm data and web front-end servers' data) that you want to back up from the tree.
3. Click **Plan Builder** > **Form Mode** on the ribbon and create a new plan. Then run this plan. For more detailed information, refer to Using Form Mode to Create a Backup Plan.

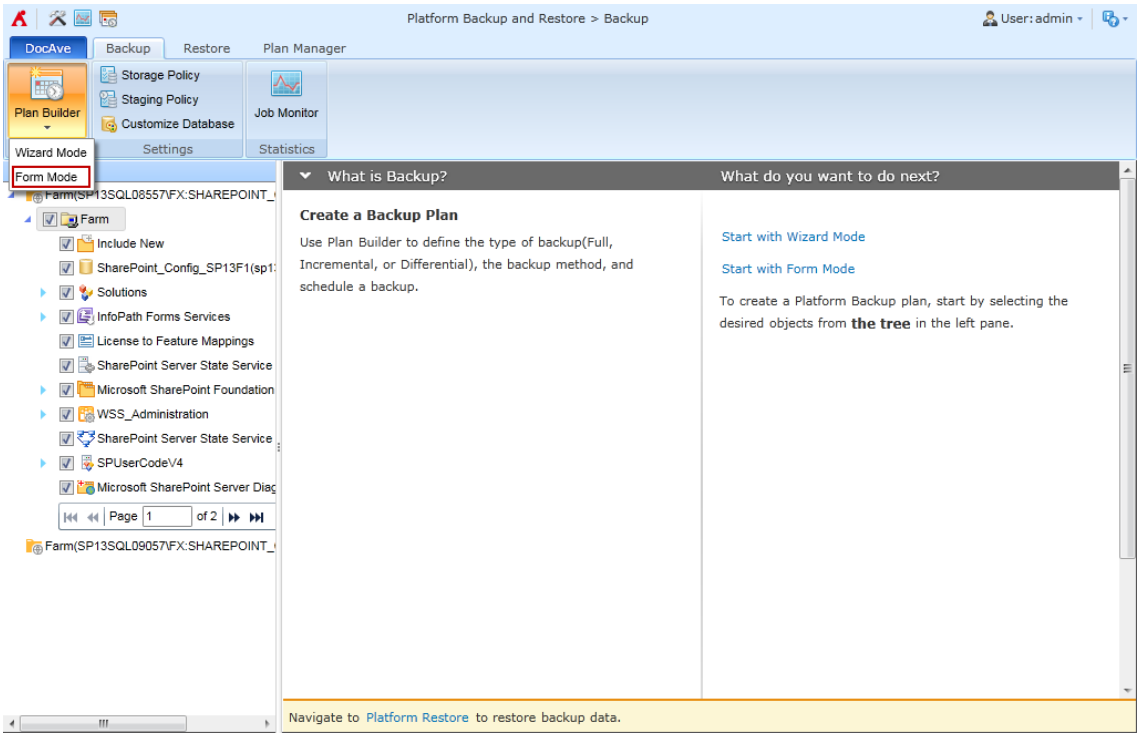


Figure 10: Create a new plan using the Form mode.

Performing the Out of Place Platform Restore

The out of place platform restore supports to restore one or multiple supported nodes to another farm according to the customers' requests. Refer to the detailed steps below:

1. Login 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.

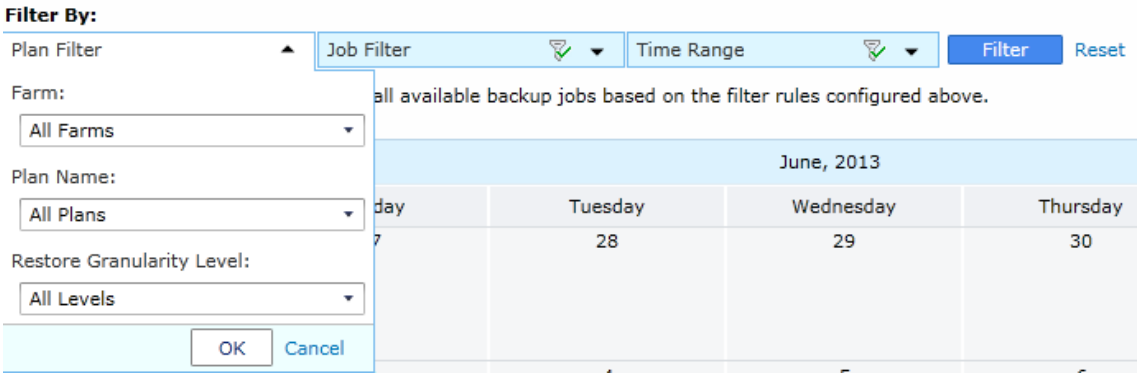


Figure 11: Filters used to filter the backup jobs.

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.

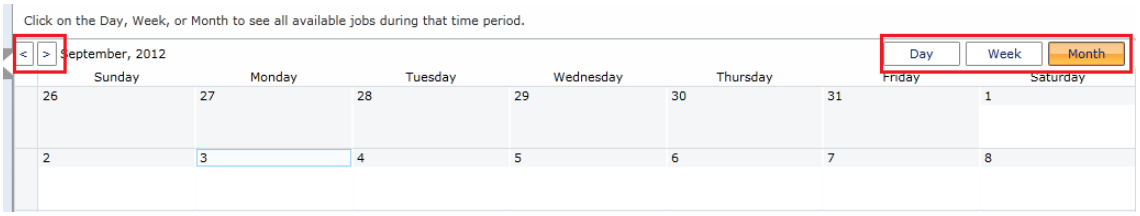


Figure 12: Change the view and turn the page.

In this case, select the backup job performed in 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.

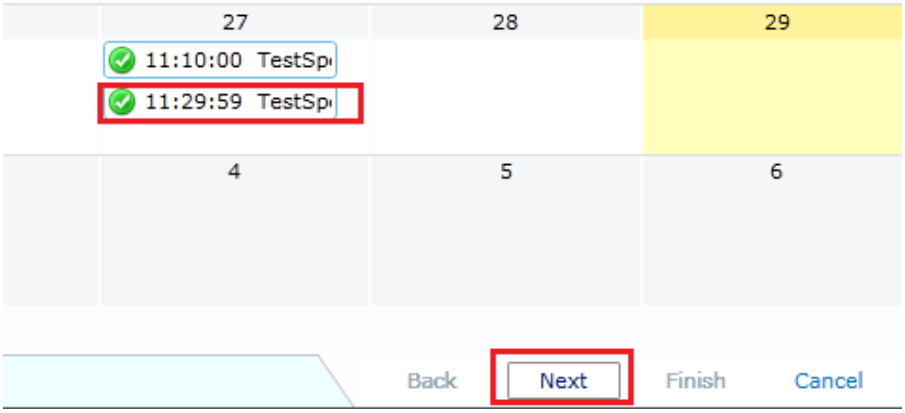


Figure 13: Select a backup job and click the Next button.

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 B – SharePoint 2010 Components Supported in Platform Backup and Restore or Appendix C – SharePoint 2013 Components Supported in Platform Backup and Restore.

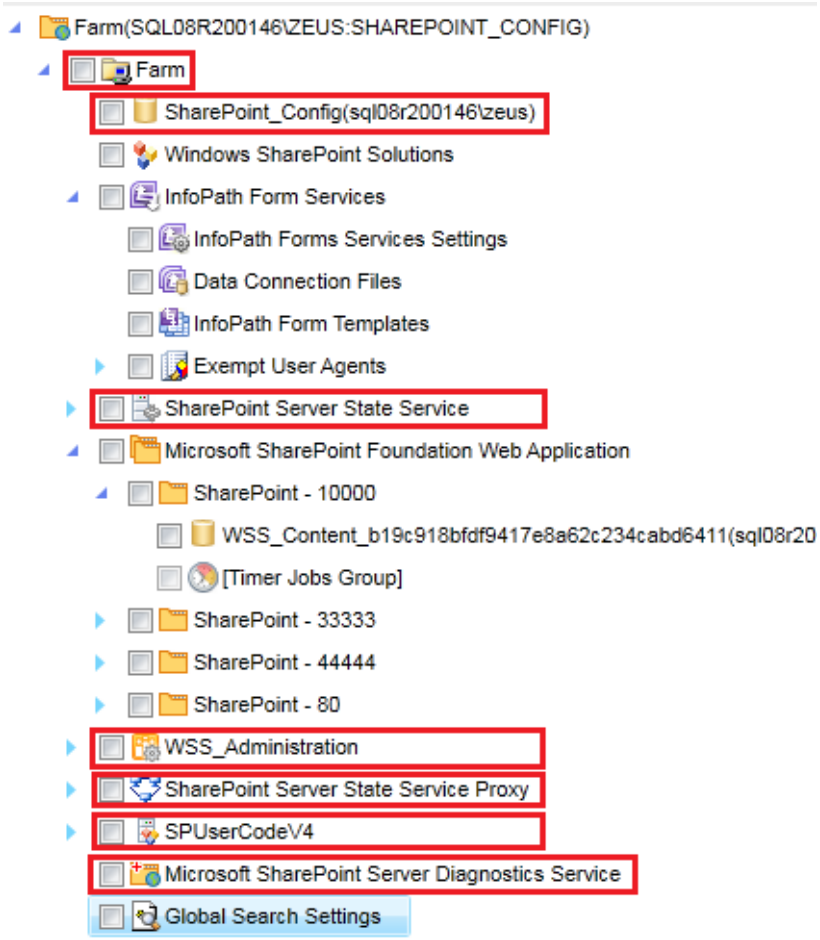


Figure 14: Nodes that cannot be restored using out of place platform restore.

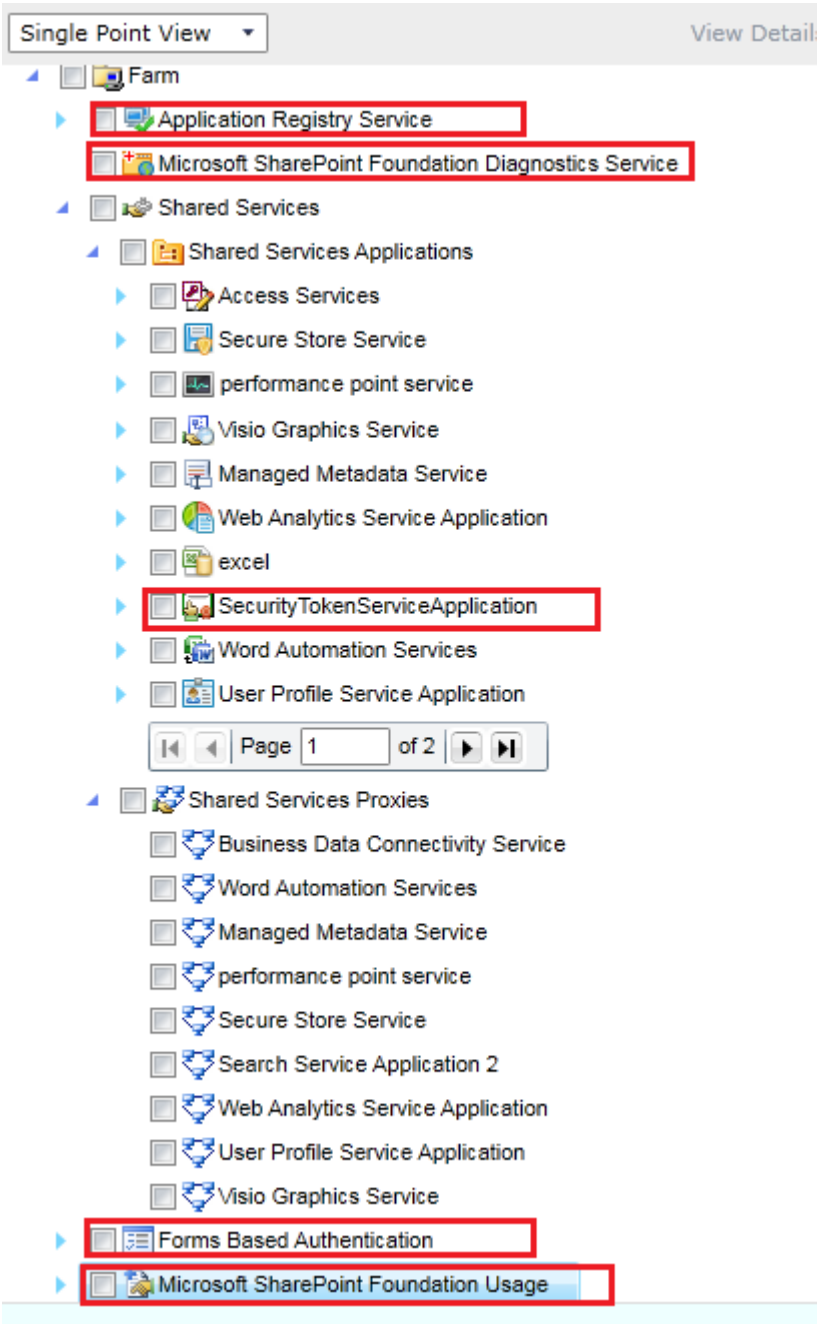


Figure 15: Nodes that cannot be restored using the out of place platform restore.

5. After selecting the content to be restored, refer to the corresponding sections below for the other configurations.

Restoring Windows SharePoint 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 **Windows SharePoint Solutions**, **InfoPath Form Services** and **Global Search Settings** nodes on the tree.

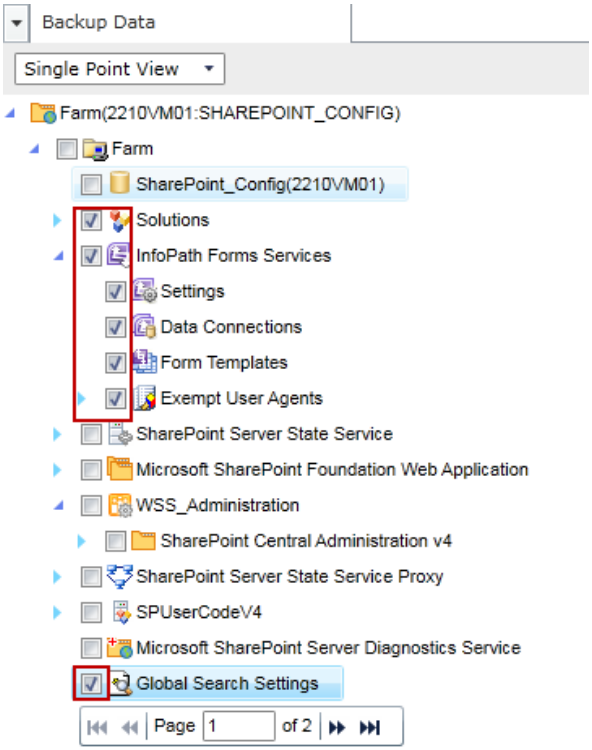


Figure 16: Selected nodes on the tree.

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.

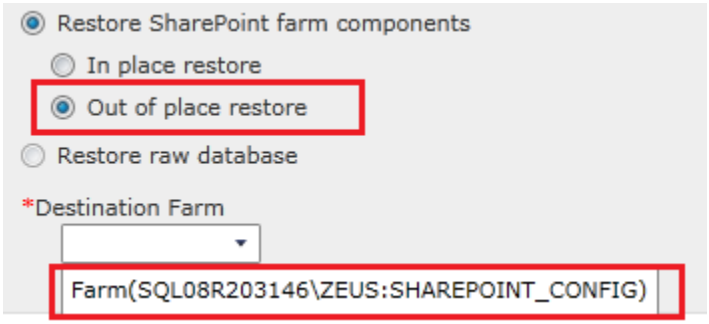


Figure 17: Configure the Restore Type field.

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 the 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 the Database Level in this user guide.

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

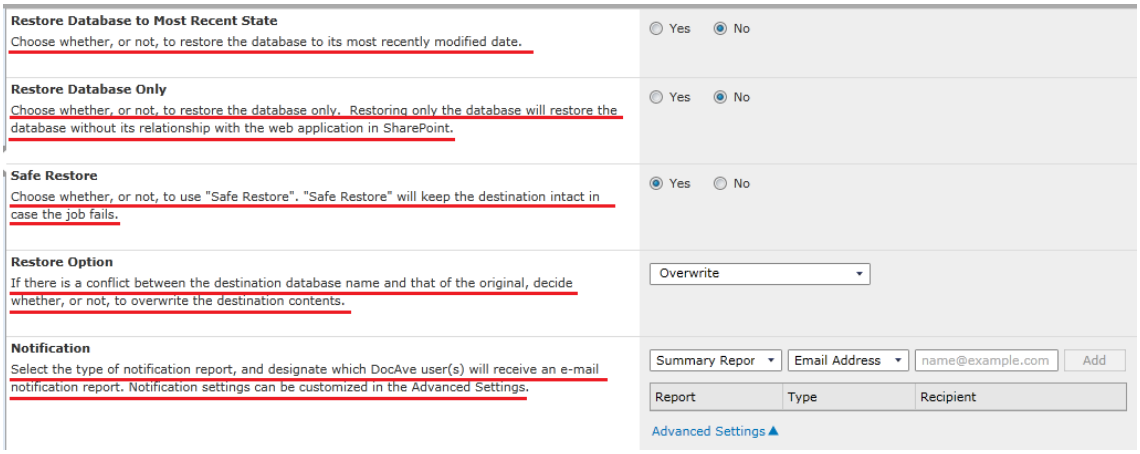


Figure 18: Restore Settings page.

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 the 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. In the following case, we choose 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, you must create the same master key as the source one in the destination. On the destination server, use the following SQL statement to create the same master key as the source one:

"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.

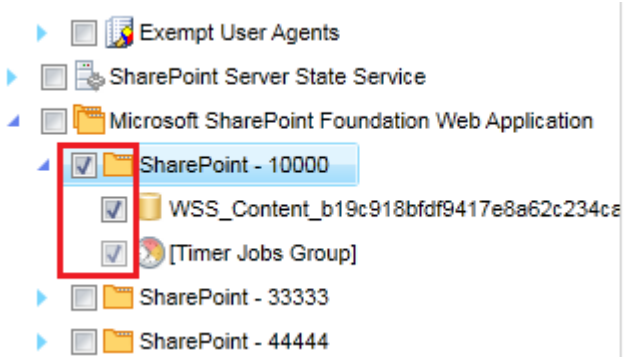


Figure 19: Select the web application and its database.

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.

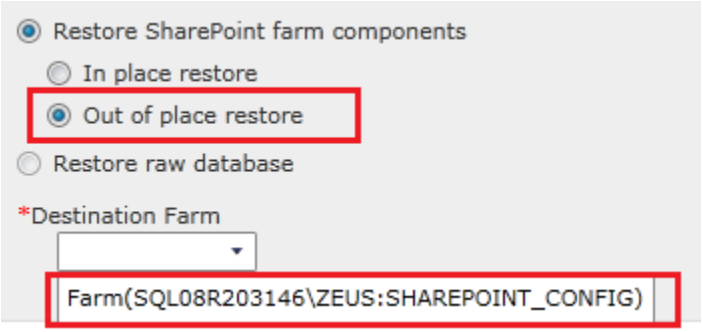


Figure 20: Configure the Restore Type field.

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 to be 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.

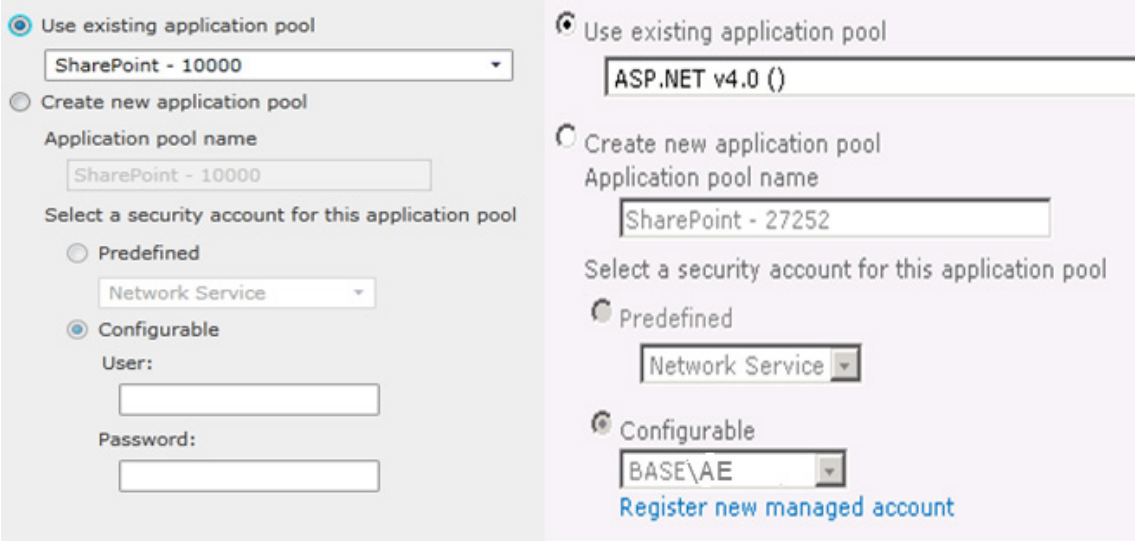


Figure 21: DocAve configuration (the one on the left) and the SharePoint configuration page (the one on the right).

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 the content database configuration. The options to be 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 the Database Level.

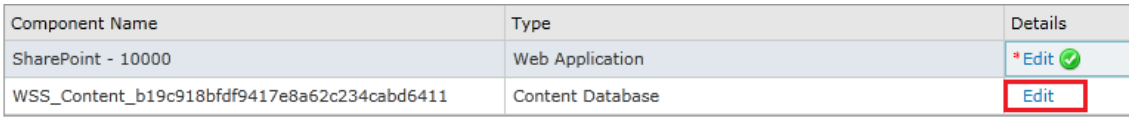


Figure 22: Edit the content database configuration.

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. For the detailed explanation of each option, refer to the DocAve 6 Platform Backup and Restore user guide.

   In this case, select **Overwrite** as the Restore Option 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 the 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**.

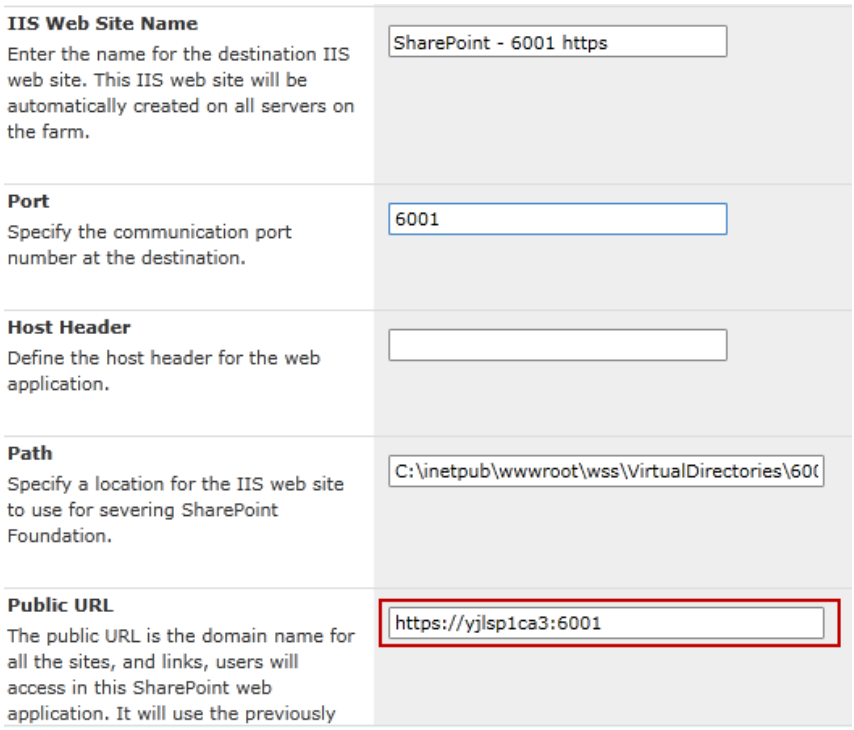


Figure 23: Public URL of the HTTPS web application.

- 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.

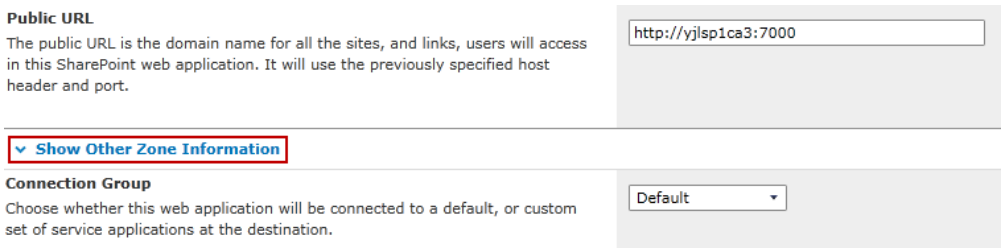


Figure 24: Show Other Zone Information link.

For example, the Intranet zone settings.

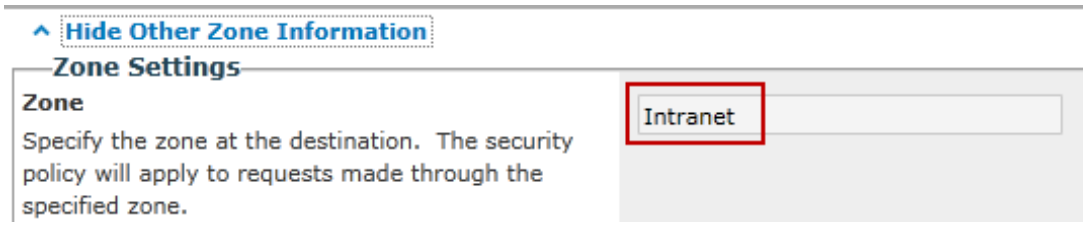


Figure 25: Settings of the Intranet zone.

- When restoring multiple content databases at one time, you must configure the detailed settings for each of the content database that will be restored.

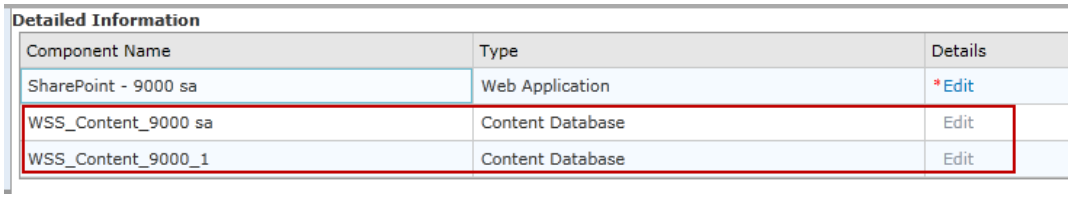


Figure 26: Configure the settings for each content database.

- If one content database has more than one **NDF** files, all its **NDF** files will be loaded when configuring the detailed settings for this content database.

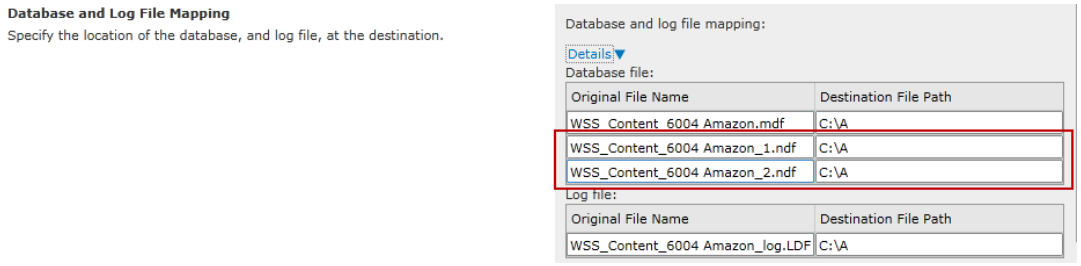


Figure 27: Detailed settings for one content database having multiple NDF files.

- 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.

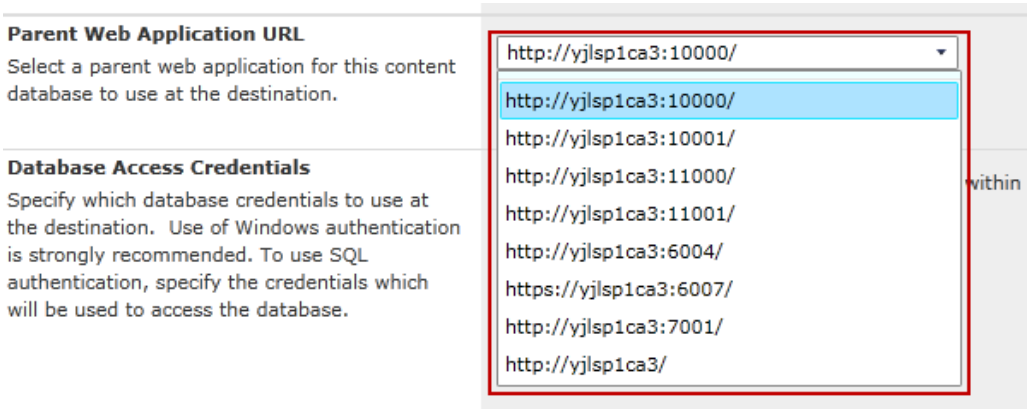


Figure 28: Configure the Parent Web Application URL field.

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 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.

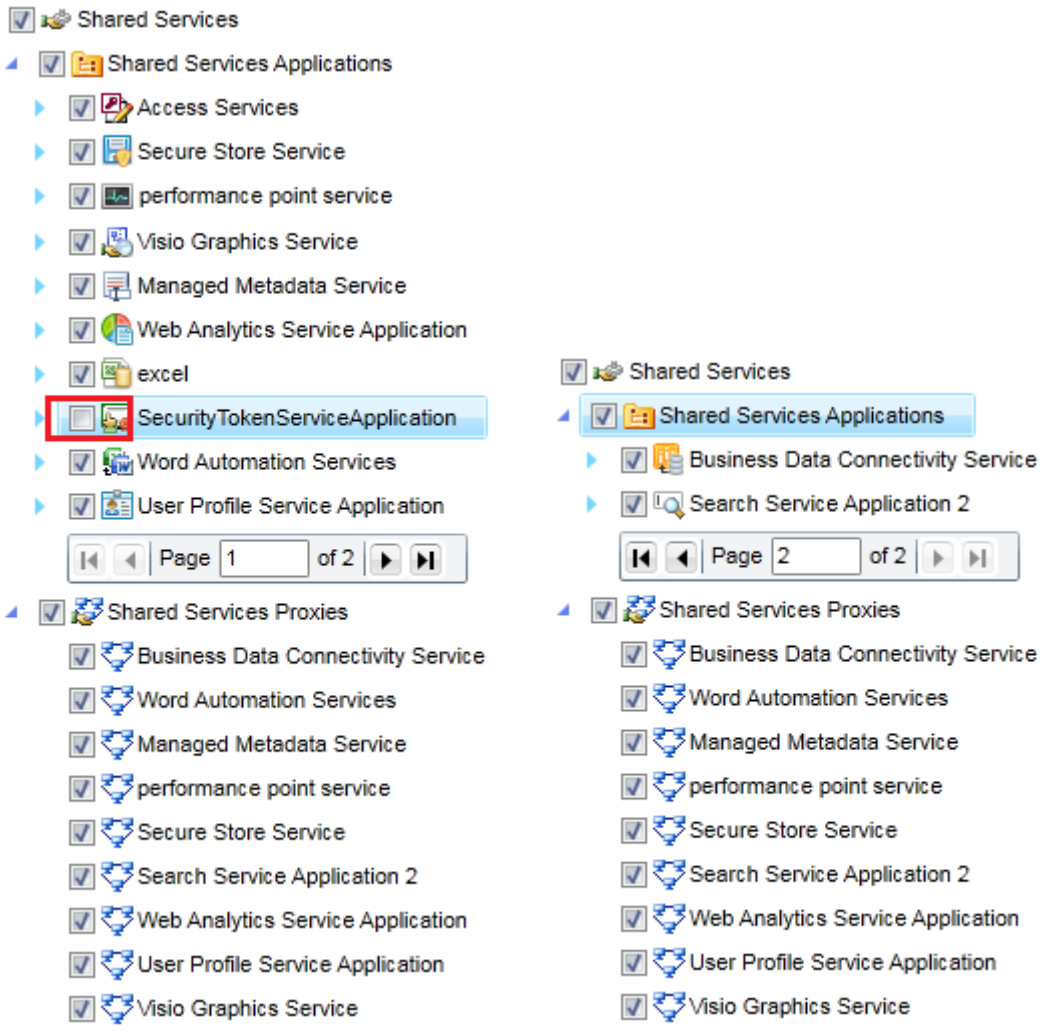


Figure 29: Select all the service applications of SharePoint 2010 that are supported in the out of place platform restore.

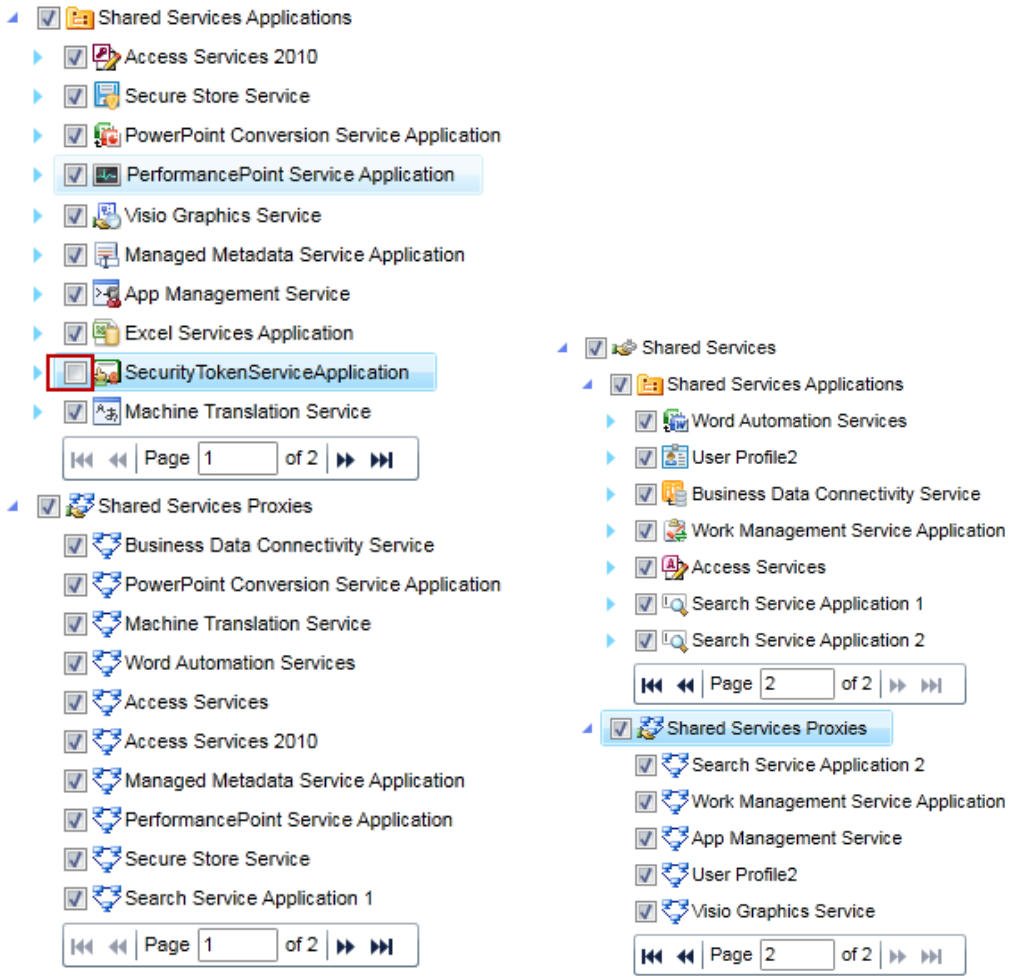


Figure 30: Select all the service applications of SharePoint 2013 that are supported in the out of place platform restore.

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.

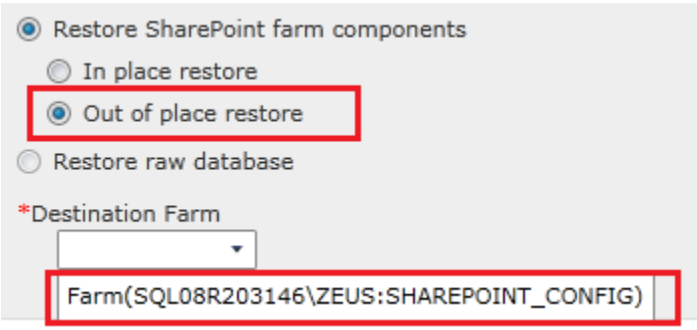


Figure 31: Configure the Restore Type field.

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 the service application configuration. The options to be 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.

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 32: 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** — Specify 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.

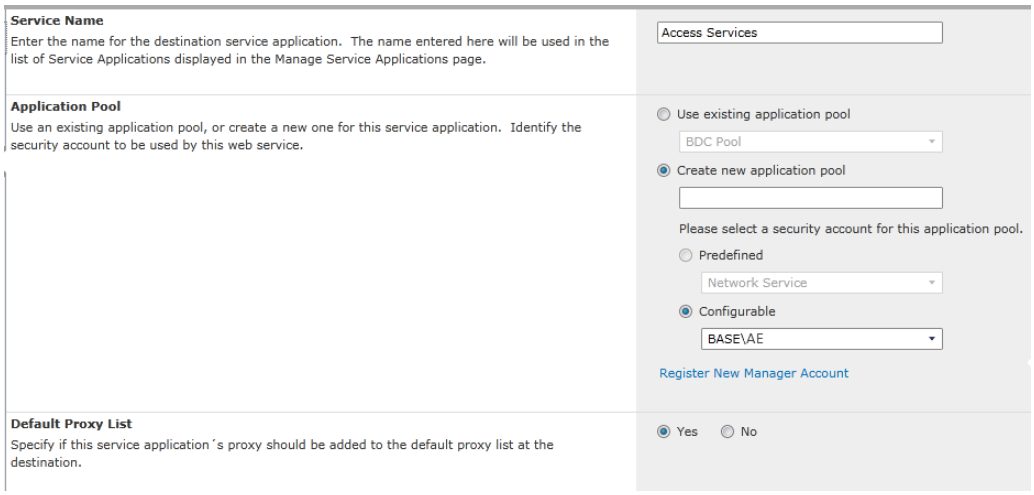


Figure 33: Access Services 2010 Web Service Application (SharePoint 2013)/Access Service Web Service Application (SharePoint 2010) settings.

- **Access Services Web Service Application** (SharePoint 2013) – Configure the following settings for the SharePoint 2013 Access Service Web Service Application:
    - **Database Server –** Specify the database server for this service application and specify the access credentials. We recommend you use Windows authentication. If you want to use the SQL authentication, specify the credential to access the database server.

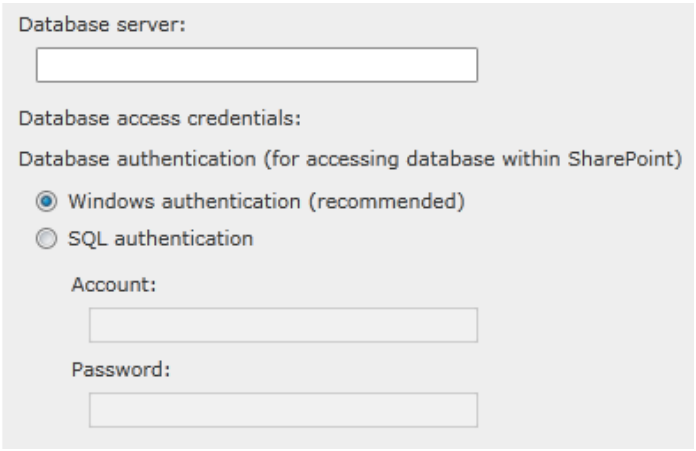


Figure 34: Access Services Web Service Application (SharePoint 2013) settings.

- **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.

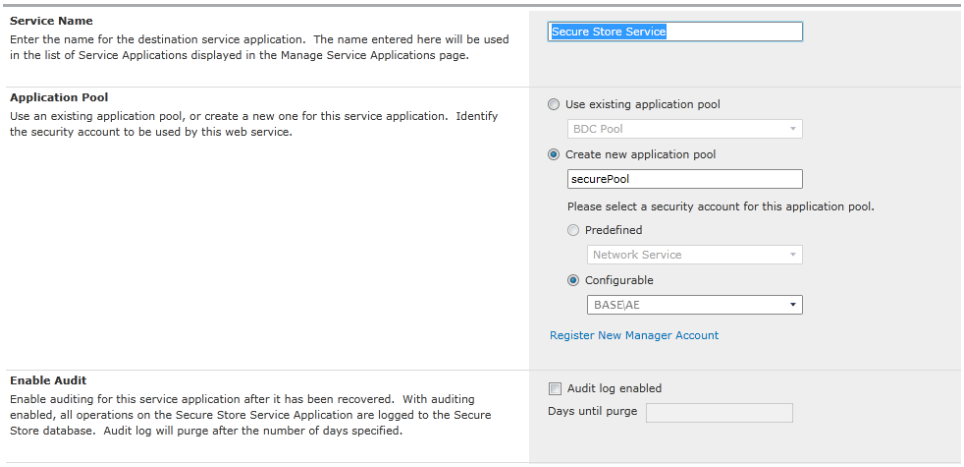


Figure 35: Secure Store Service Application settings.

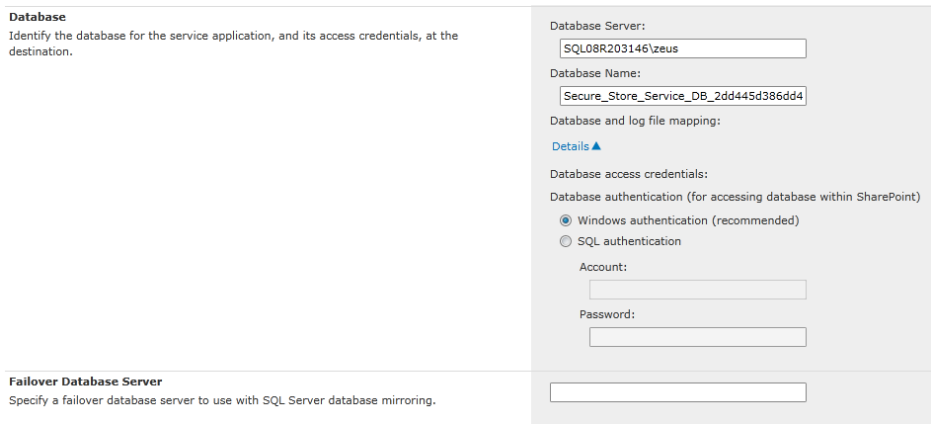


Figure 36: Secure Store Service Application settings.

Configure the same settings for other service applications according to the detailed information above.

- **PerformancePoint Service Application**

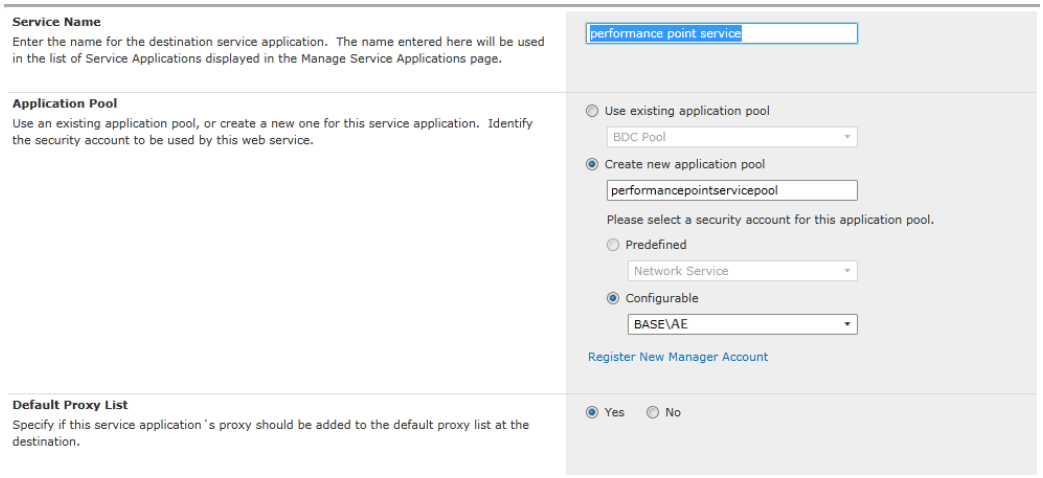


Figure 37: PerformancePoint Service Application settings.

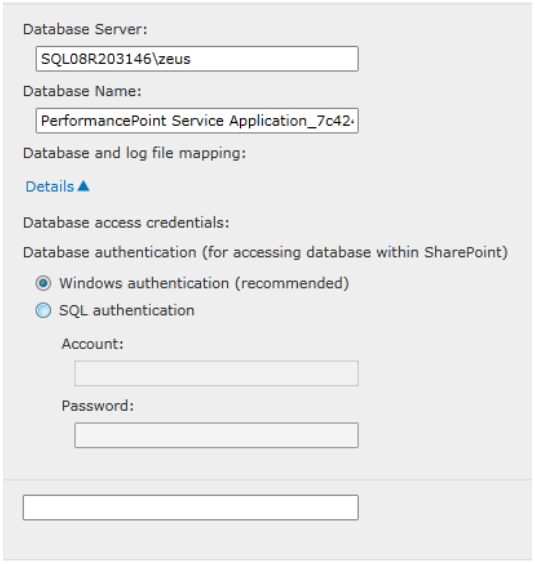


Figure 38: PerformancePoint Service Application settings.

- **Project Service Application** (SharePoint 2010)

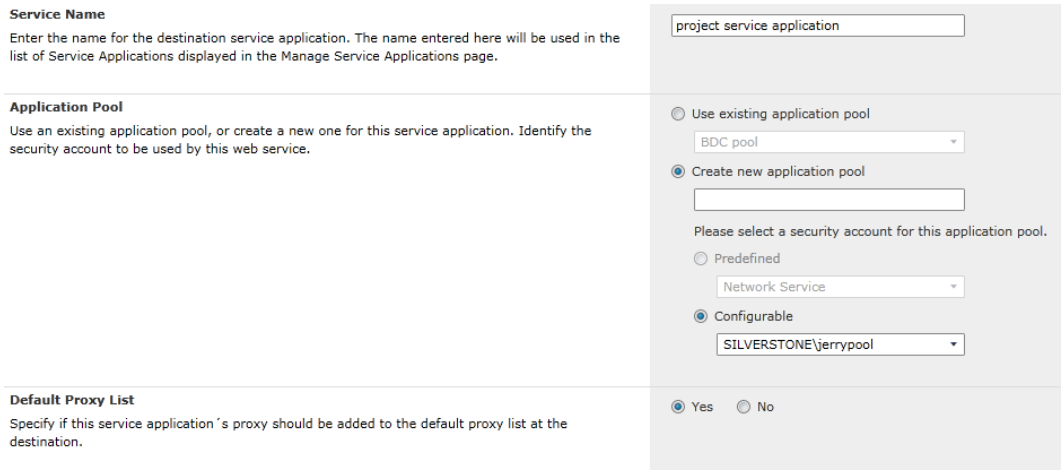


Figure 39: Project Service Application (SharePoint 2010) settings.

- **Project Service Application** (SharePoint 2013)

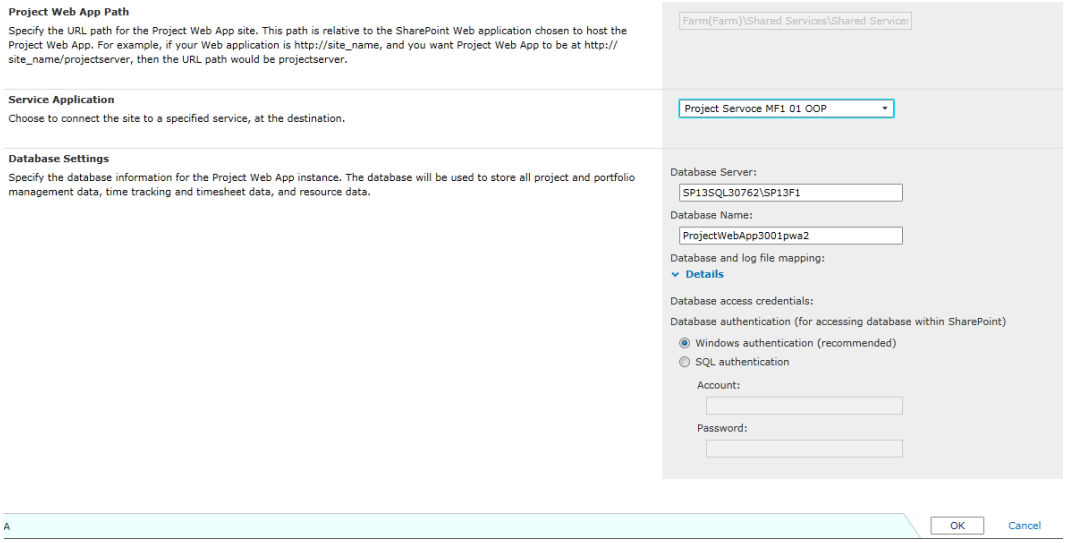


Figure 40: Project Service Application (SharePoint 2013) settings

- **Visio Graphics Service**

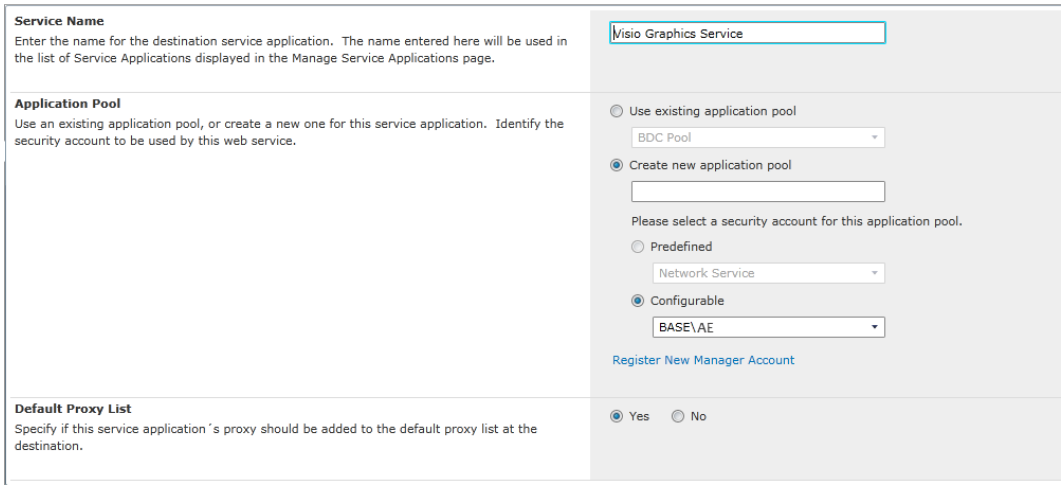


Figure 41: Visio Graphics Service Application settings.

- **Managed Metadata Service**

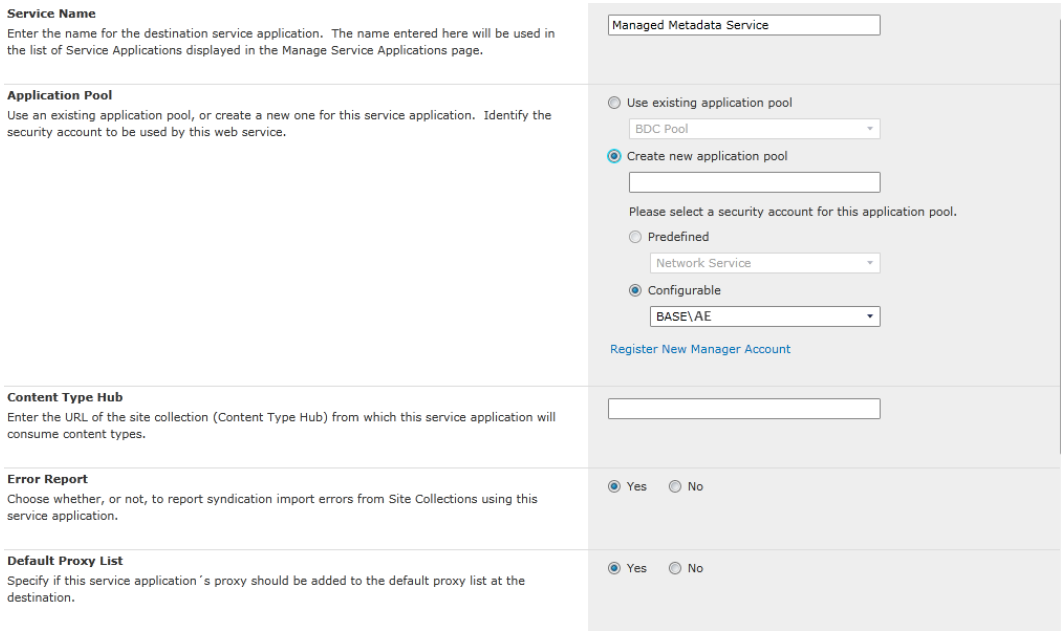


Figure 42: Managed Metadata Service Application settings.

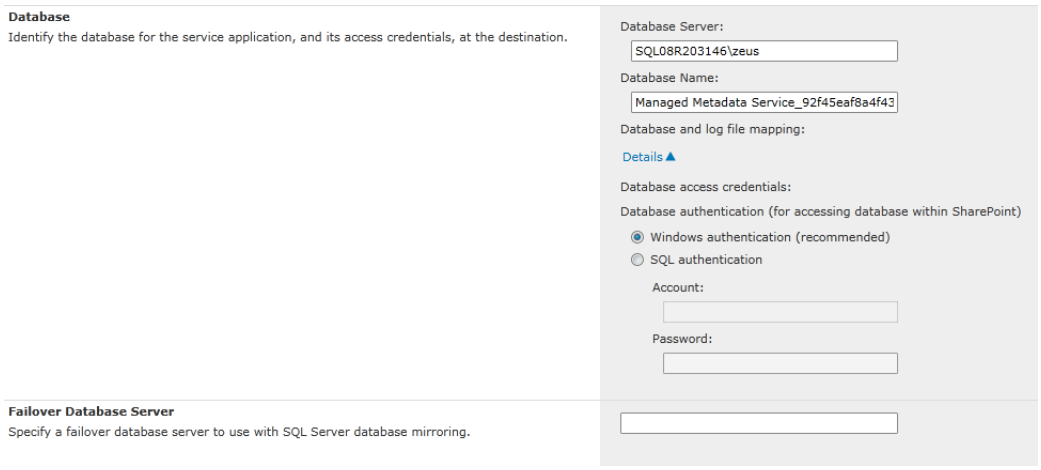


Figure 43: Managed Metadata Service Application settings.

- **Web Analytics Service Application**

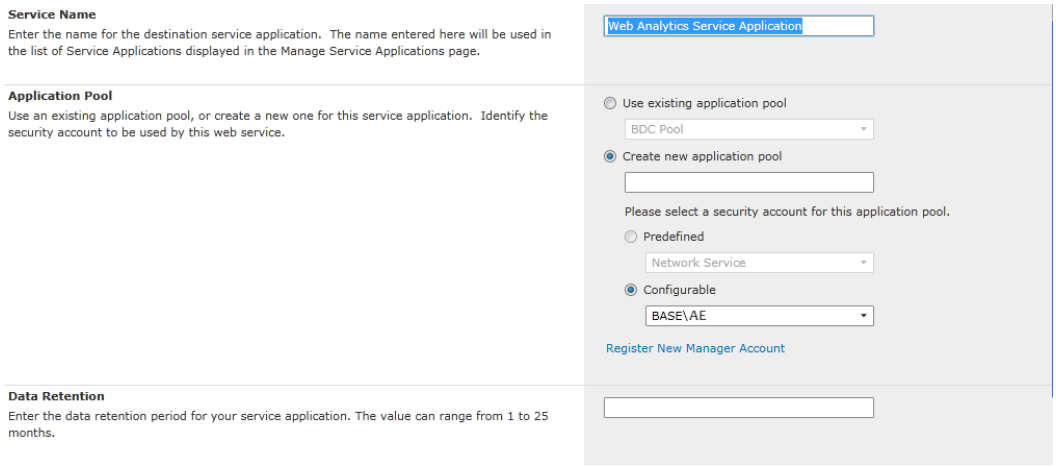


Figure 44: Web Analytics Service Application settings.

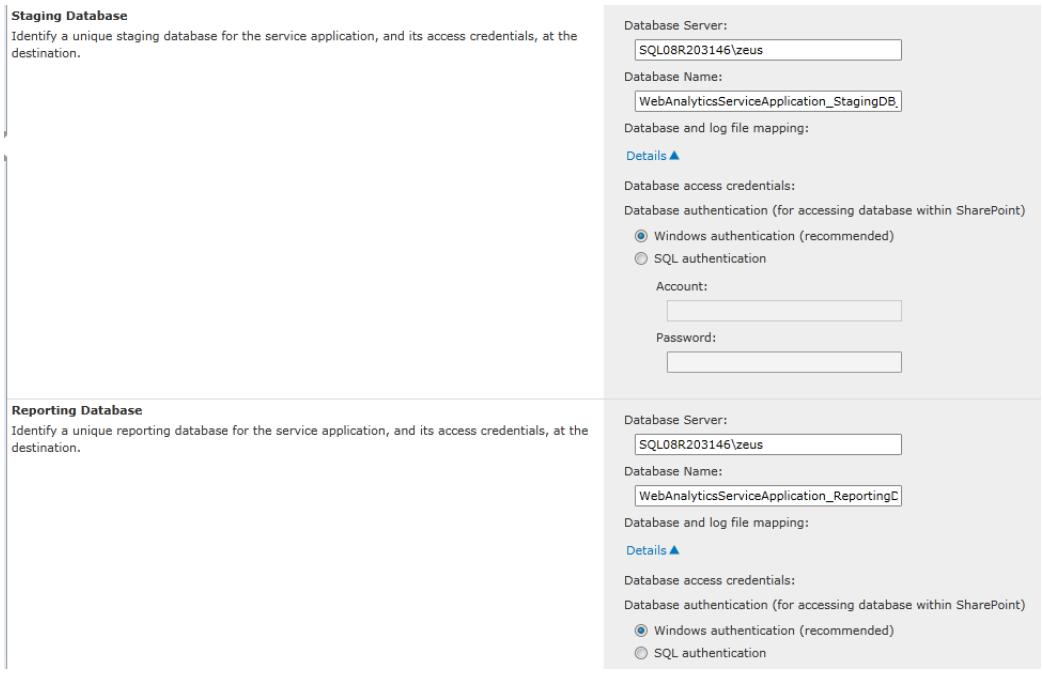


Figure 45: Web Analytics Service Application settings.

- **Excel Services Application**

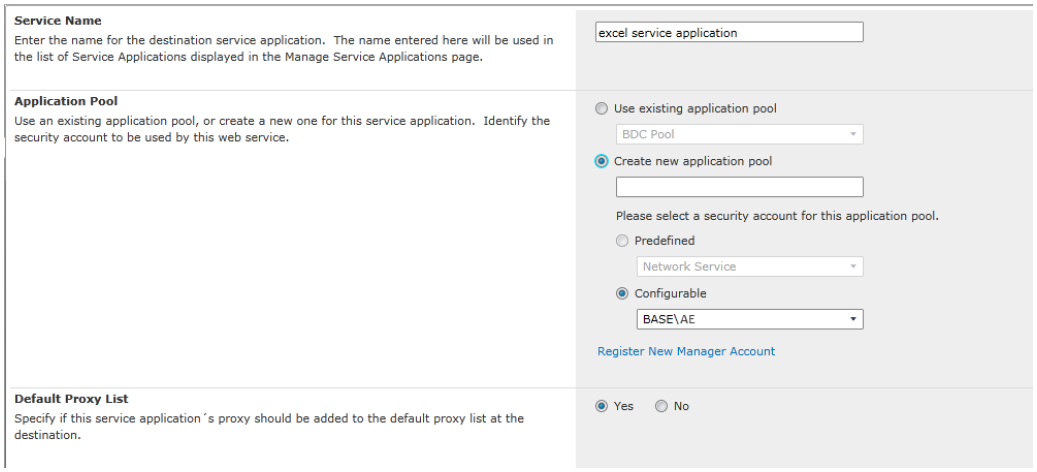


Figure 46: Excel Services Application settings.

- **Word Automation Services**

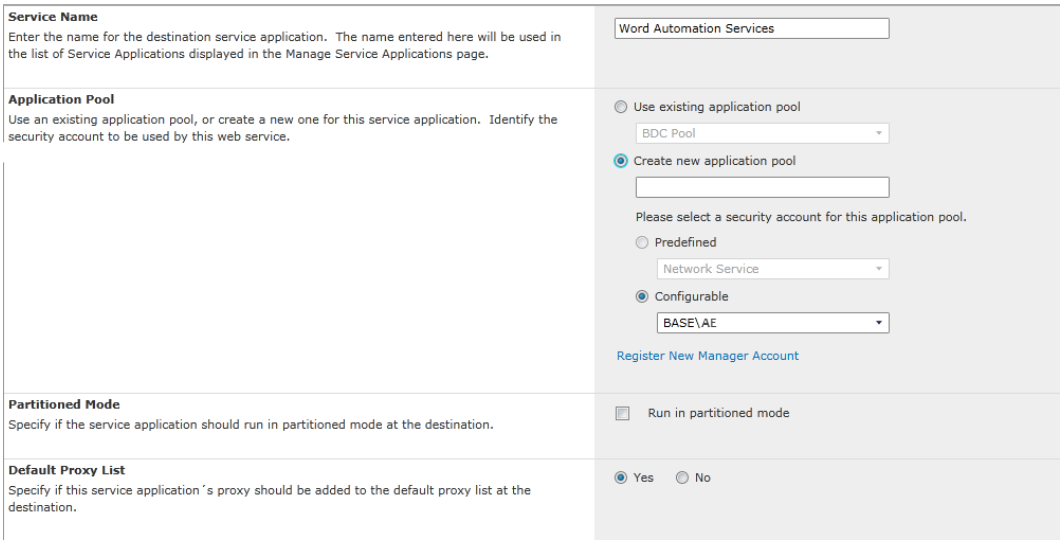


Figure 47: Word Automation Services settings.

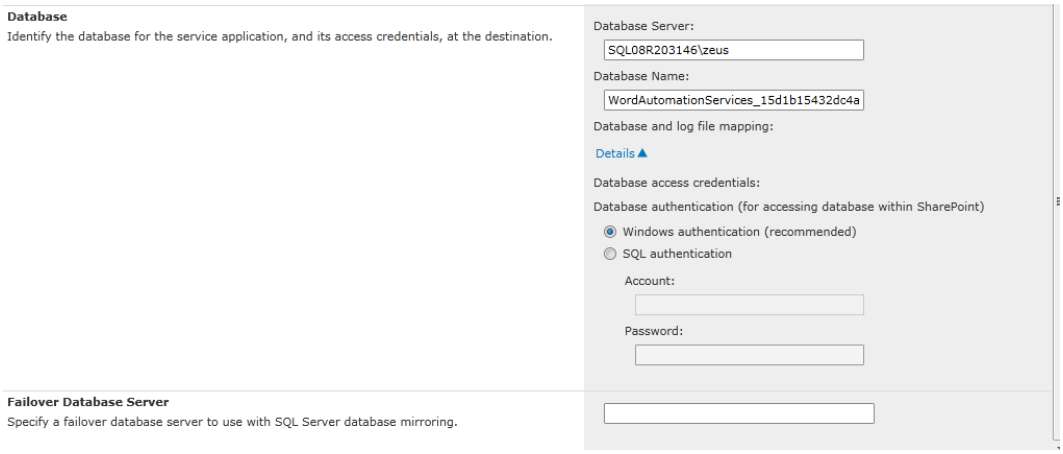


Figure 48: Word Automation Services settings.

- **App Management Service Application** (SharePoint 2013)

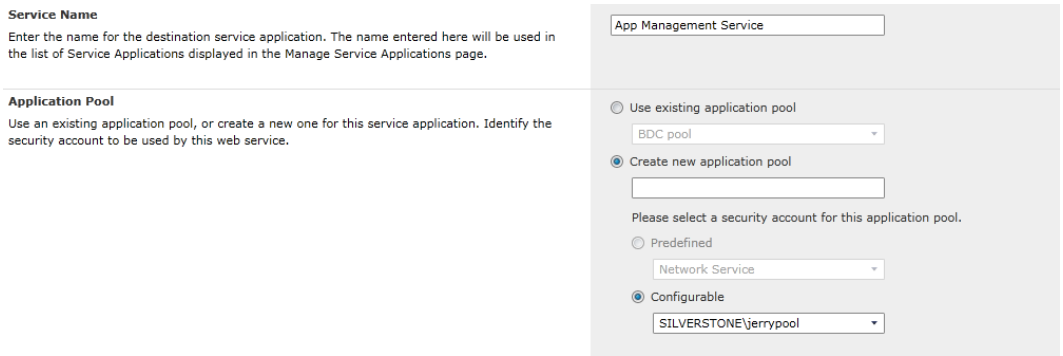


Figure 49: App Management Service Application settings.

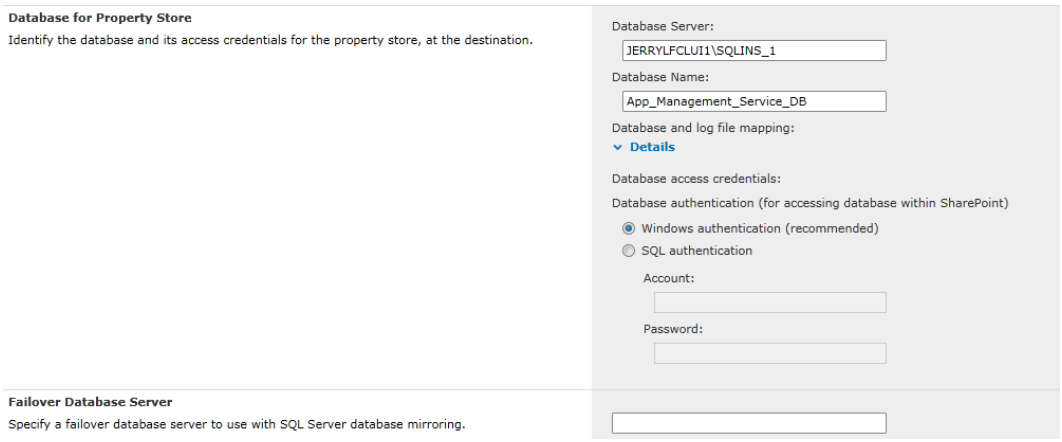


Figure 50: App Management Service Application settings.

- **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 specify 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.

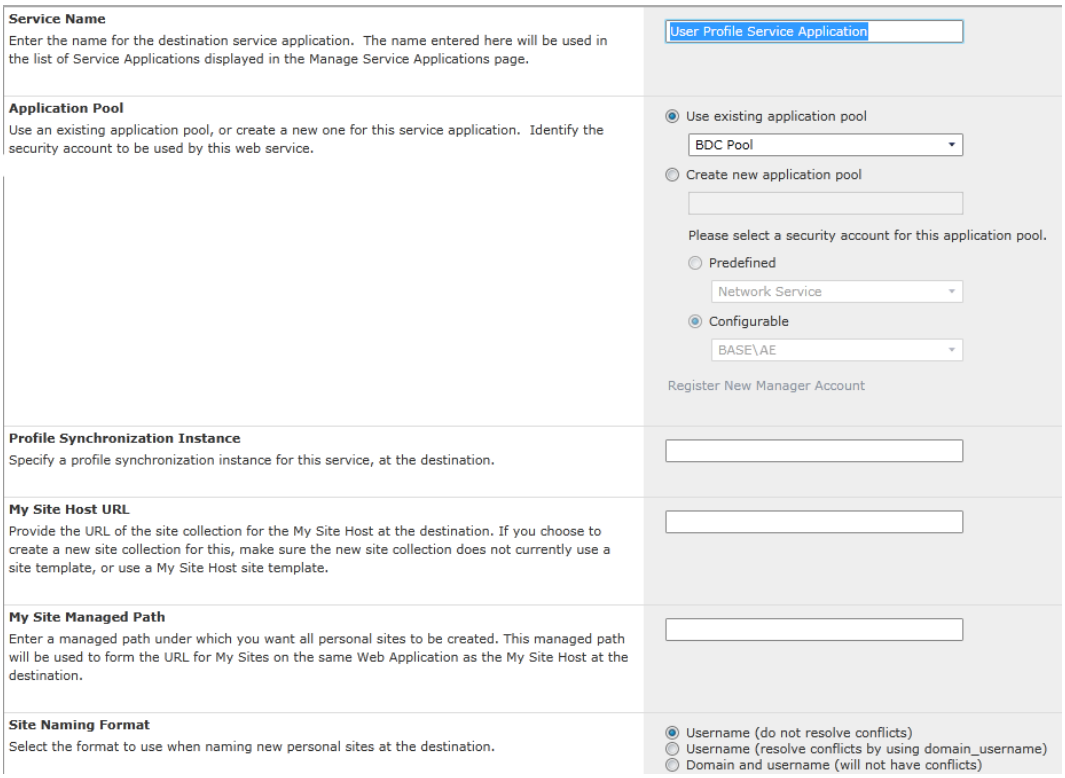


Figure 51: User Profile Service Application settings.

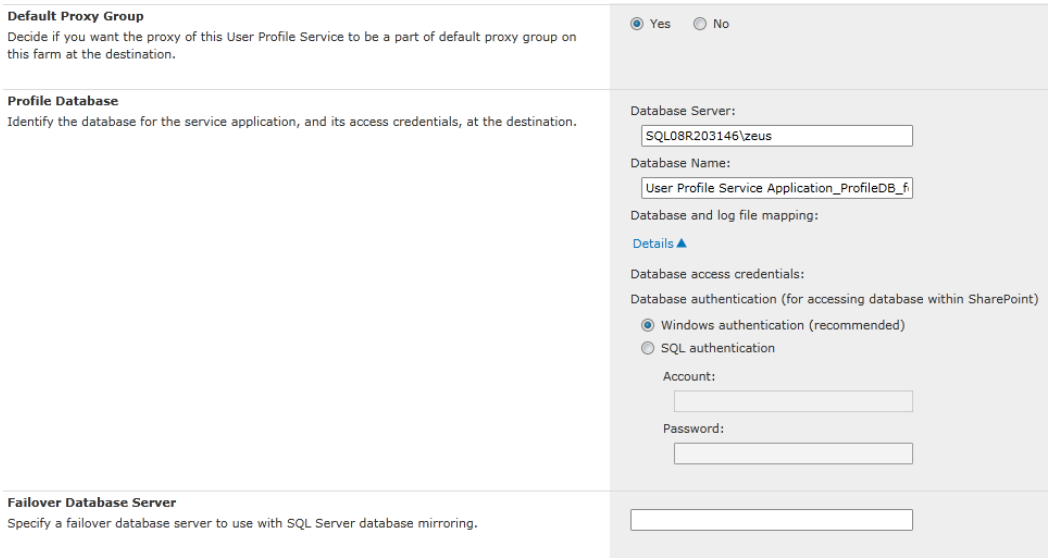


Figure 52: User Profile Service Application settings.

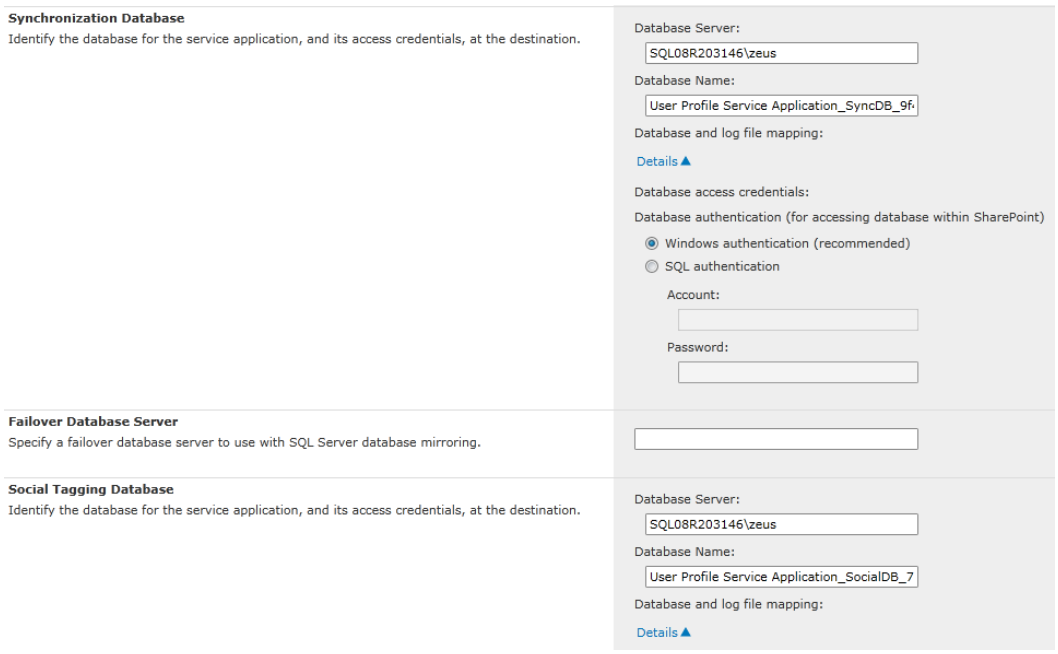


Figure 53: User Profile Service Application settings.

- **Business Data Connectivity Service**

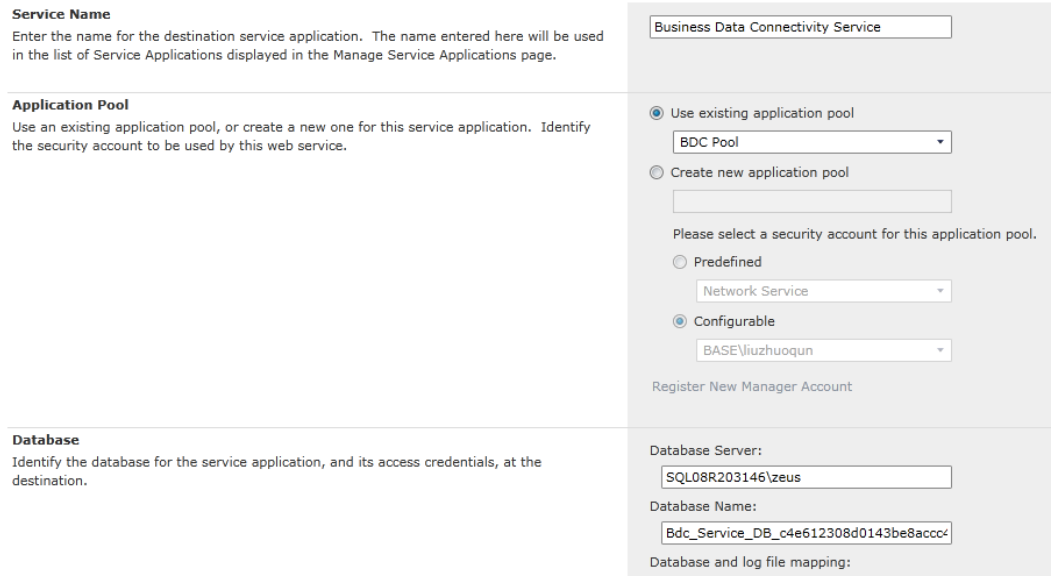


Figure 54: Business Data Connectivity Service settings.

- **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.

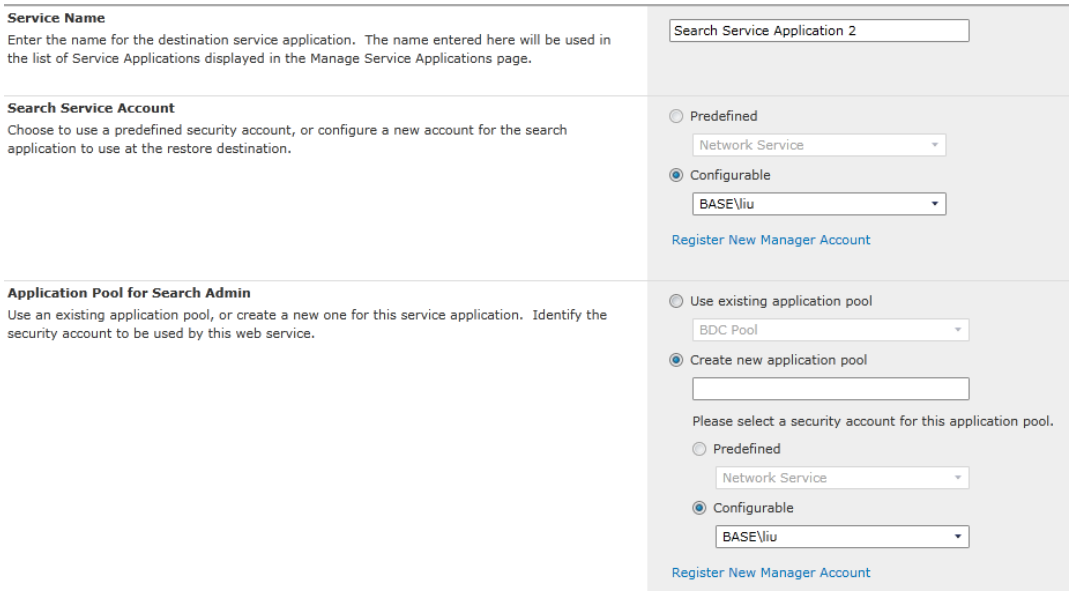


Figure 55: Search Service Application settings.

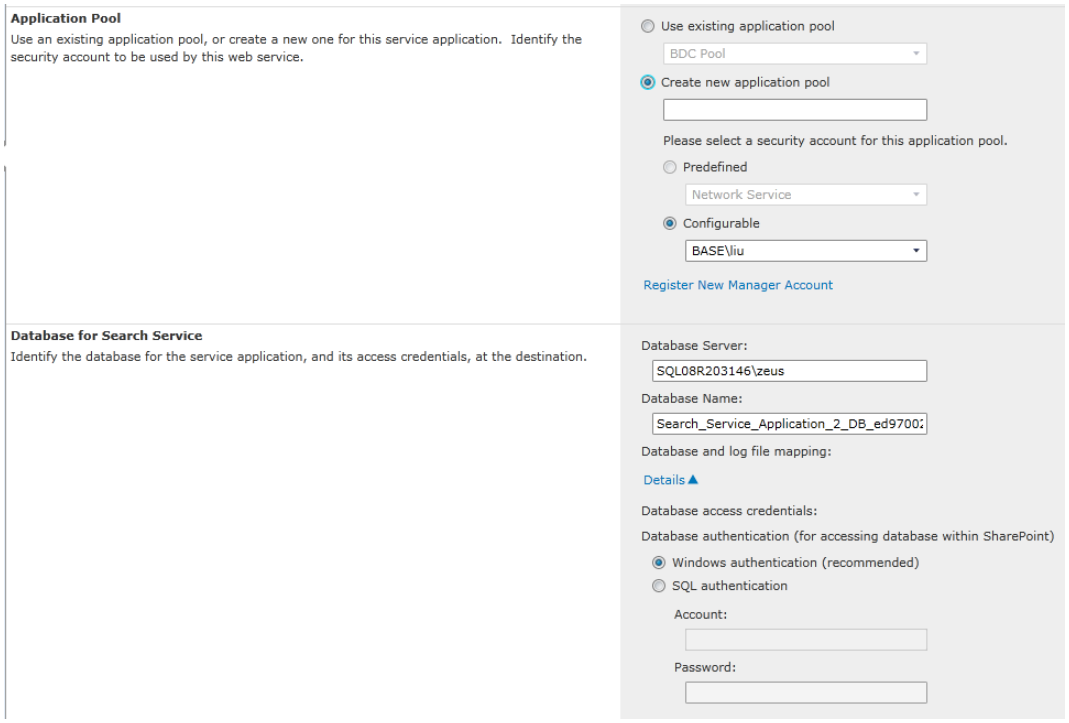


Figure 56: Search Service Application settings.

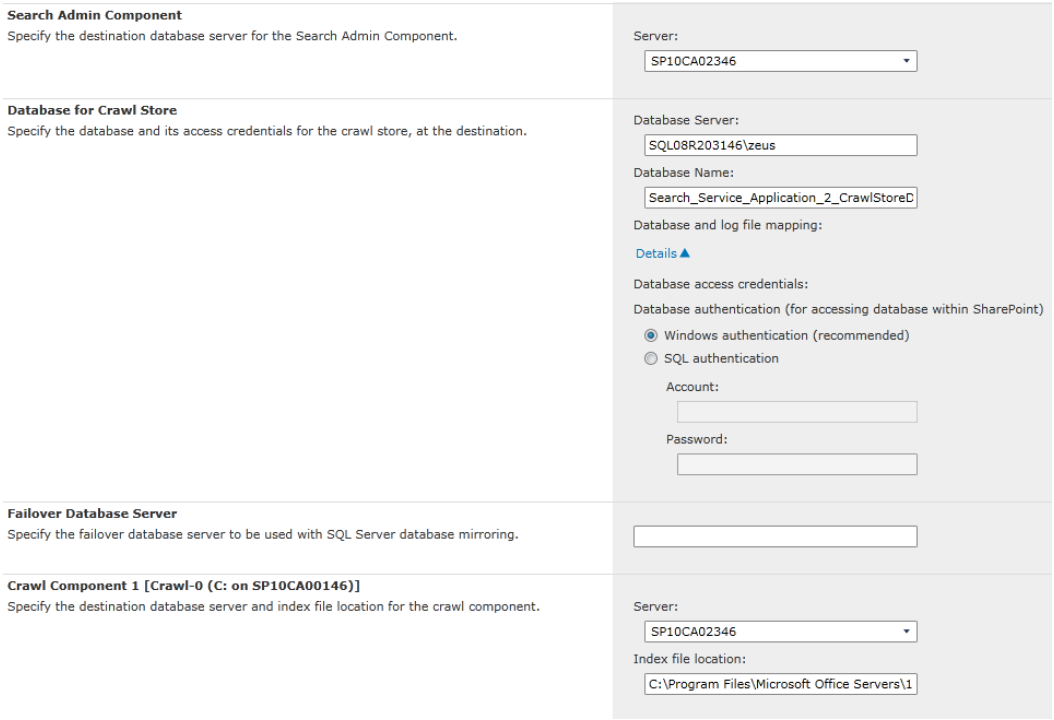


Figure 57: Search Service Application settings.

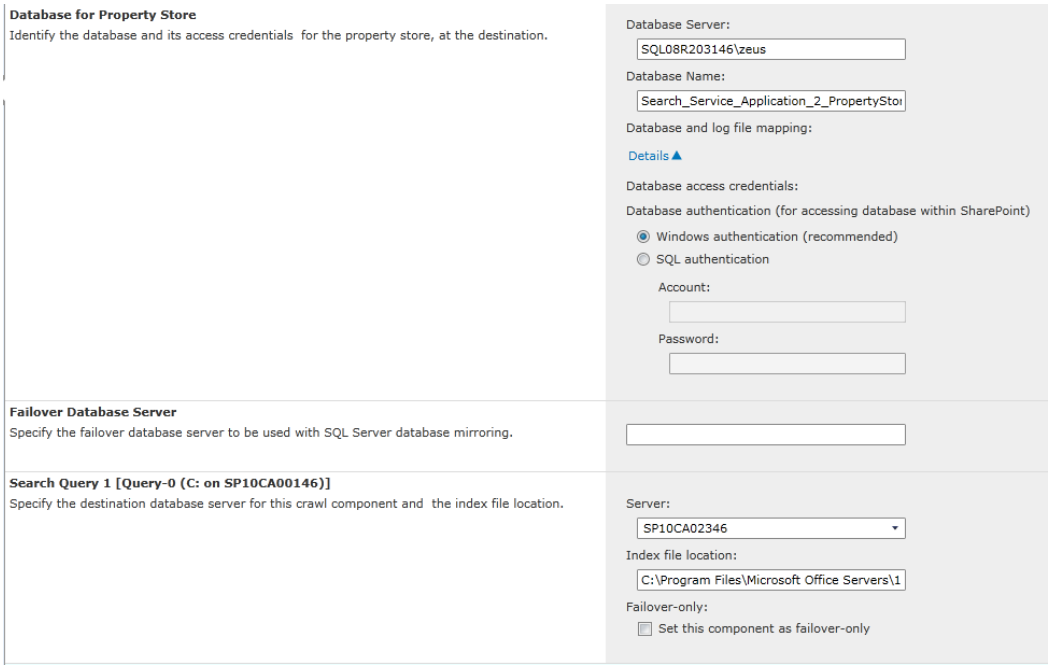


Figure 58: Search Service Application settings.

- **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.

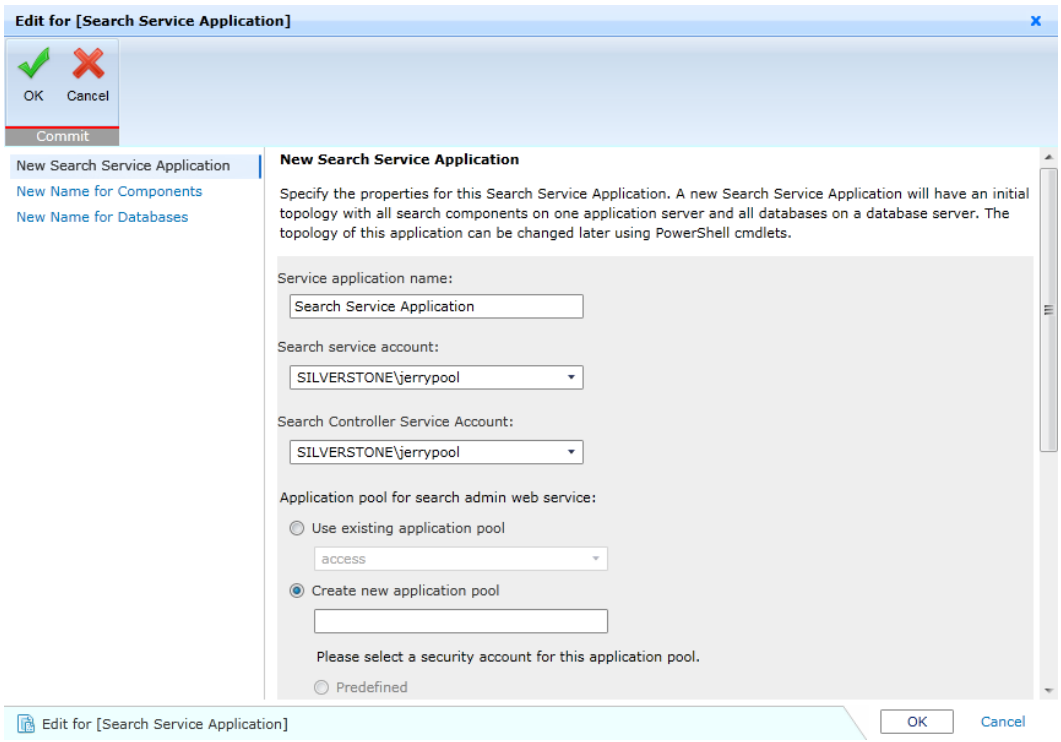


Figure 59: Search Service Application Settings.

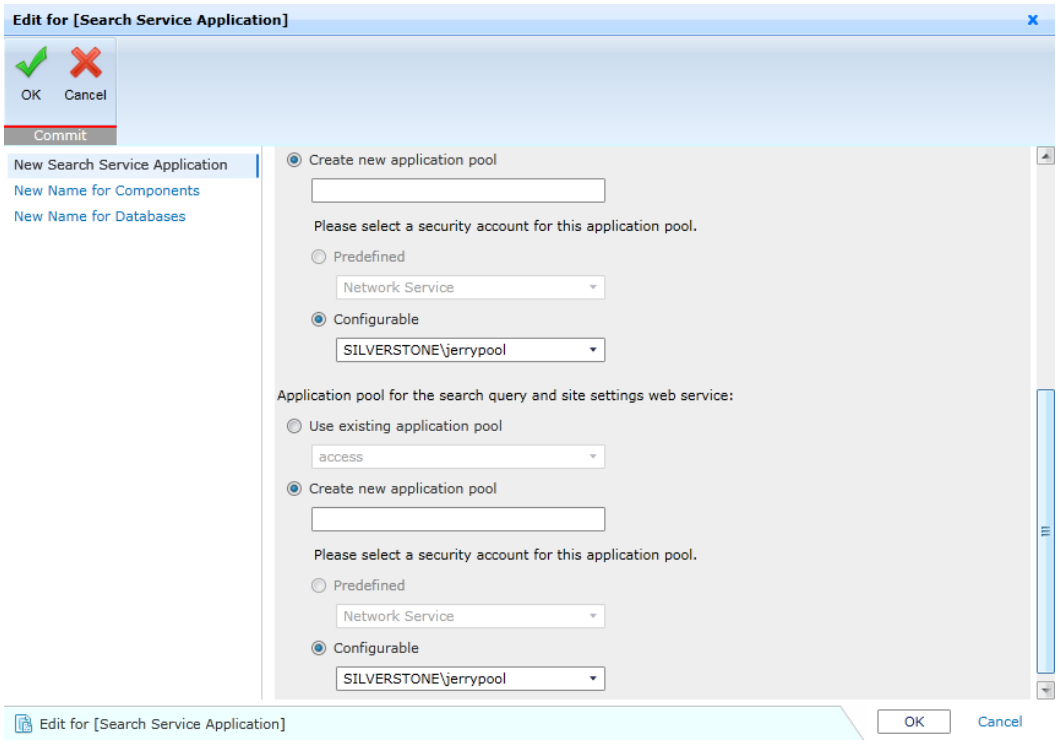


Figure 60: Search Service Application Settings.

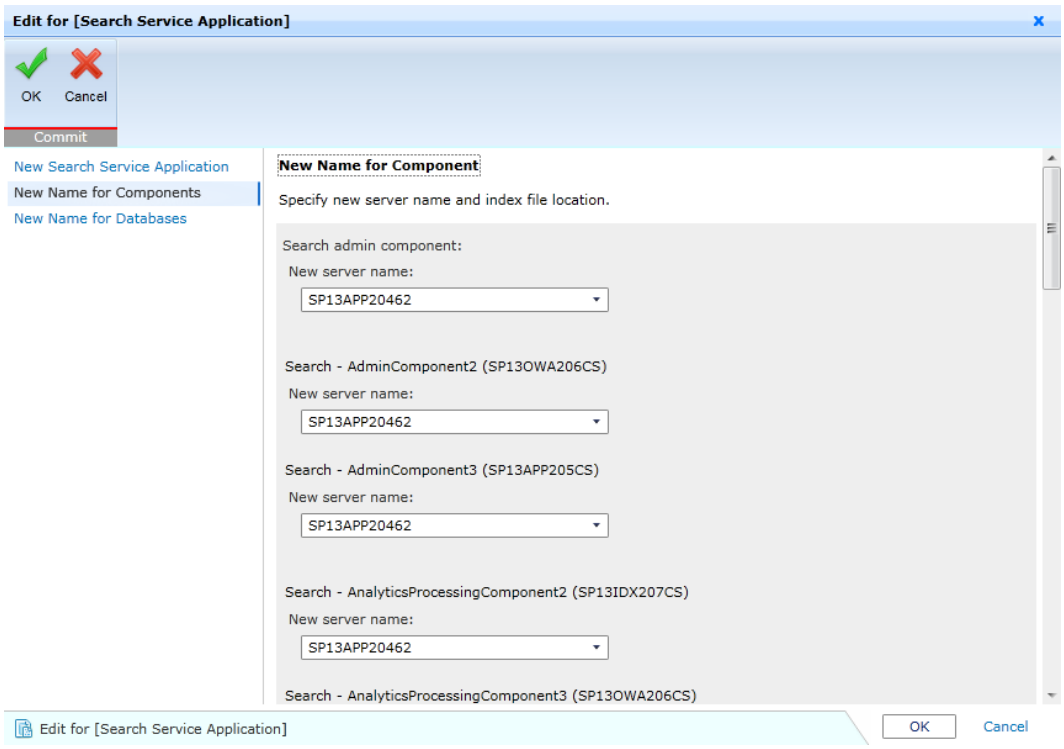


Figure 61: Search Service Application Settings.

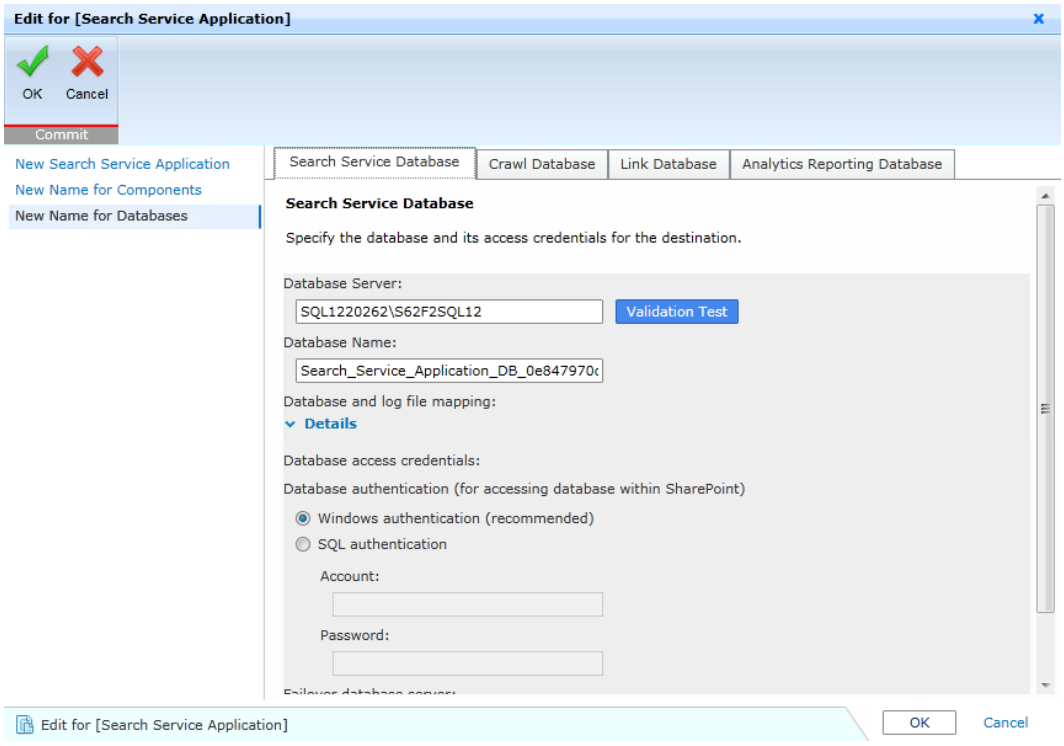


Figure 62: Search Service Application Settings.

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 the Database Level.

   In this case, select **Overwrite** as the **Restore Option** 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 the 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** — Specify whether to add this proxy to the default proxy list in the destination farm.

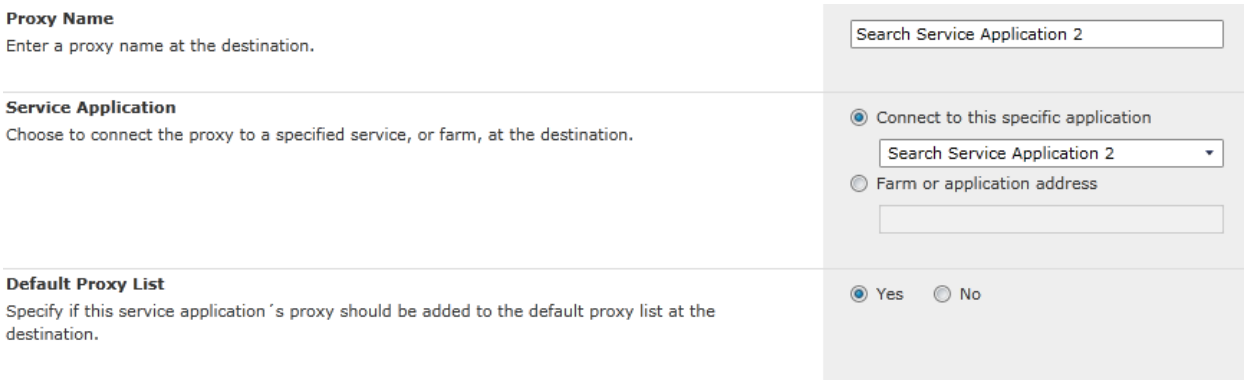


Figure 63: Proxy settings.

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

To restore backup Web-frontend servers data, complete the following steps:

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

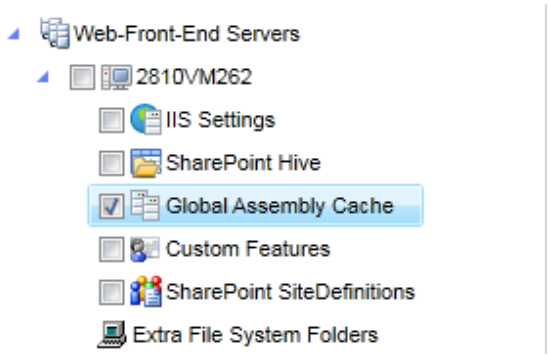


Figure 64: Selected nodes on the tree.

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.

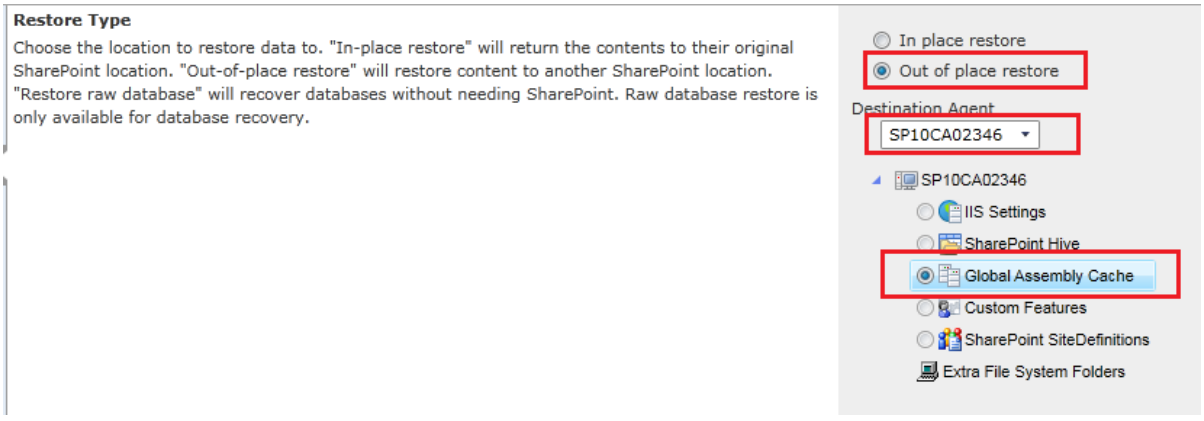


Figure 65: Configure the Restore Type field.

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 the 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 the 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.

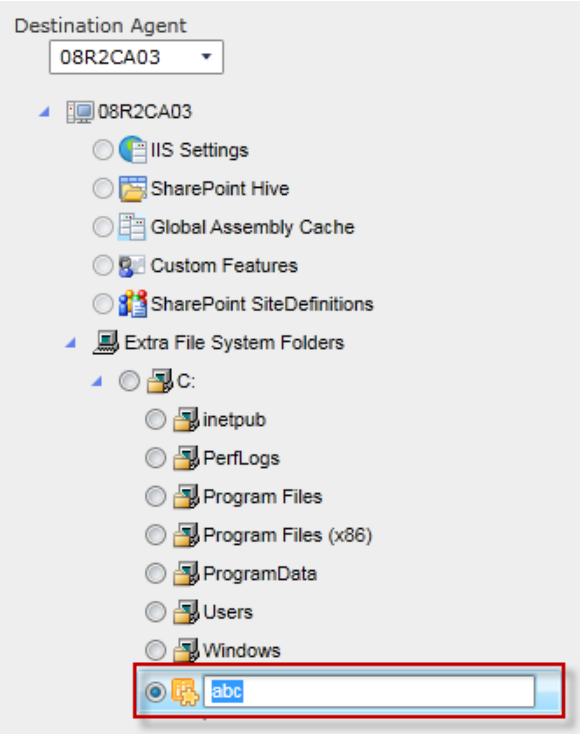


Figure 66: Restore to a manually inputted file system folder.

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. Of equal importance, 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 'moving parts' to a SharePoint platform, a failure in any one component could adversely affect the entire environment.

The SharePoint administrator, Joe, is facing a situation in which his organization's SharePoint deployment incurs a catastrophic failure. Joe 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, Joe had created and run scheduled Incremental backup jobs:

- Joe selected the entire farm to back up and selected the **Include New** checkbox to ensure that newly-created objects are backed up.
- Joe 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, Joe chose not to **Create Persistent Snapshots**.

Restoring the Platform

As a result of the catastrophic SharePoint farm failure, Joe 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 front-end Web 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, Joe 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 front-end Web servers can be attached, Joe must first restore the configuration database and the Central Administration databases.

After completing this, Joe can bring the front-end Web 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 front-end Web servers should host the central administration Web application.

After the front-end Web servers are online, Joe 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 front-end related components (for example, IIS settings, SharePoint site definitions, and custom features), should be restored on all of the front-end Web servers of the SharePoint farm.

Appendix A – 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
Plan Manager	P
DocAve Home Page	1
DocAve Online Community	2
Control Panel	3
Job Monitor	4
Plan Group	5

Backup Tab

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

Functionality Name and Hot Key							
Plan Builder	P	Wizard Mode	W	Storage Policy	S		
				Back	B		
				Next	N		
				Finish	F	Finish	F
						Finish and Run Now	FR
				Cancel	C		
		Form Mode	F	Storage Policy	S		
				OK	O	OK	O
						OK and Run Now	OR
				Cancel	C		
Storage Policy	S						
Staging Policy	A	Create	N	OK	O		
				Cancel	C		
		Edit	E	OK	O		
				Cancel	C		
		Delete	D				
		Close	C				
Customize Database	C	OK	O				
		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	F	Filter	FI
		Reset	CL
		Disconnect	D
		Restore	R
		Connect	CO
		Back	B
		Next	N
		Finish	FN
		Cancel	CX
Staging Policy	A		
Job Monitor	J		

Time-Based Restore

Functionality Name and Hot Key					
Time-based Restore	T	Create Container	T	OK	O
				Cancel	C
		Advanced Search	AS	Search	S
				Cancel	C
		Filter	PE		
		Reset	RE		
		Staging Policy	ZC		
		Installed Programs	I	Close	X
		Download Backup List	D	OK	O
				Cancel	C
		Back	B		
		Next	N		
		Finish	F		
		Cancel	C		

Plan Manager Tab

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

<table>
<tr><th colspan="8">Functionality Name and Hot Key</th></tr>
<tr><td rowspan="8">View Details</td><td rowspan="8">V</td><td rowspan="6">Edit</td><td rowspan="6">E</td><td>Storage Policy</td><td colspan="3">ZP</td></tr>
<tr><td>Staging Policy</td><td colspan="3">ZC</td></tr>
<tr><td>Customize Database</td><td colspan="3">ZD</td></tr>
<tr><td rowspan="2">Save</td><td rowspan="2">S</td><td>Save and Run Now</td><td>SR</td></tr>
<tr><td>Save</td><td>S</td></tr>
<tr><td>Save As</td><td colspan="3">A</td></tr>
<tr><td>Cancel</td><td colspan="3">C</td></tr>
<tr><td>Plan Group</td><td colspan="5">P</td></tr>
<tr><td>Close</td><td colspan="5">C</td></tr>
<tr><td rowspan="7">Edit</td><td rowspan="7">E</td><td colspan="3">Storage Policy</td><td colspan="3">ZP</td></tr>
<tr><td>Staging Policy</td><td colspan="5">ZC</td></tr>
<tr><td>Customize Database</td><td colspan="5">ZD</td></tr>
<tr><td rowspan="2">Save</td><td rowspan="2">S</td><td>Save and Run Now</td><td colspan="2">SR</td></tr>
<tr><td>Save</td><td colspan="2">S</td></tr>
<tr><td>Save As</td><td colspan="5">A</td></tr>
<tr><td>Cancel</td><td colspan="5">C</td></tr>
<tr><td>Delete</td><td colspan="7">D</td></tr>
<tr><td>Test Run</td><td colspan="7">T</td></tr>
<tr><td rowspan="2">Run Now</td><td rowspan="2">R</td><td>OK</td><td colspan="5">O</td></tr>
<tr><td>Cancel</td><td colspan="5">C</td></tr>
</table>

Appendix B – SharePoint 2010 Components Supported in Platform Backup and Restore

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.

Supported Web Parts

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

Web Part		Supported	Unsupported
	Text Filter	√	
Forms	HTML Form Web Part	√	
	InfoPath Form Web Part		√
Media and Content	Content Editor	√	
	Image Viewer	√	
	Media Web Part	√	
	Page Viewer	√	
	Picture Library Slideshow Web Part	√	
Outlook Web App	My Calendar	√	
	My contacts	√	
	My Inbox	√	
	My Mail Folder	√	
	My Tasks	√	
Search	Advanced Search Box	√	
	Dual Chinese Search	√	
	Federated Results	√	
	People Refinement Panel	√	
	People Search Box	√	
	People Search Core Results	√	
	Refinement Panel	√	
	Related Queries	√	
	Search Action Links	√	
	Search Box	√	
	Search Core Results	√	
	Search Paging	√	
	Search Statistics	√	
	Search Summary	√	
	Top Federated Results	√	
Social Collaboration	Contact Details ***Note**: The user related properties of this Web part will be backed up and restored together with the Web part.	√	
	Note Board	√	
	Organization Browser	√	
	Site Users	√	
	Tag Cloud	√	
	User Tasks	√	

Service Applications Supported for Restore

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

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

Service Application	Databases of the Service Application	Supported in In-place Restore	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)	√	√
Visio Graphics Service	This Service Application does not have a database	√	√
Web Analytics Service Application	WebAnalyticsServiceApplication_StagingDB (Web Analytics Staging Database) WebAnalyticsServiceApplication_ReportingDB(Web Analytics Warehouse Database)	√	√
Word Automation Services(Word Conversion Service)	WordAutomationServices_Database(Microsoft.Office.Word.Server.Service.QueueDatabase)	√	√
Lotus Notes Connector	–	×	×
Usage and Health data collection	WSS_Logging	√	×
Word Viewing Service	–	×	×
PowerPoint Service Application	–	×	×
Project Service Application	–	√	√
SQL Server PowerPivot Service Application	–	×	×
Subscription Settings Service Application	Subscription Settings Database	√	√

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	√(Restore Database Only must be used)	×	
Central Admin Web Application	√(Restore Database Only must be used)	×	
Admin Content Database	√	×	
Web Application	√	√	
Content Database	√	√	
Global Search Settings	√	√	Farm-level search settings and Crawler impact rules are supported.
SharePoint Help Search	√	×	
InfoPath Form Services	√	√	InfoPath Forms Services Settings and InfoPath Forms Services Form templates are supported.
FBA Databases	√	×	The FBA Database and some configurations in the Web.config under WebApp IIS Setting (such as MemberShipProvider) are supported.
Windows SharePoint Solutions	√	√	• 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.

Features	Supported in In-place Restore	Supported in Out-of-place Restore	Notes
FAST Search Server 2010 for SharePoint	√	×	DocAve Platform Backup and Restore backs up FAST components, configuration files, index data and so on. You can also refer to the link below for the manual full backup and restore of FAST Search Server: http://technet.microsoft.com/en-us/library/ff460221.aspx
Knowledge Lake Imaging	√	×	
NewsGator	√	×	Social Sites (NewsGator) 1.2 and 2.5 are supported in DocAve 6 Service Pack 1 and later.
Nintex Workflow	√	×	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	√	√	• 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	√	√	• IIS Settings (such as Form Authentication, SSL certification and so on) can be configured individually on the front-end Web 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 front-end Web server are saved in this directory. • DocAve Platform Backup and Restore can also backup and restore the files in the file system of the front-end Web server.

Appendix C – SharePoint 2013 Components Supported in Platform Backup and Restore

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	√	√
Access Services 2010	This Service Application does not have a database	√	√
App Management Service	AppMng_Service_DB (App Management Database)	√	√
Business Data Connectivity Service	Bdc_Service_DB(Business Data Connectivity Database)	√	√
Excel Services Application	This Service Application does not have a database	√	√
Lotus Notes Connector	–	×	×
Managed Metadata Service	Managed Metadata Service_Database(Service Application Database)	√	√
PerformancePoint Service Application	PerformancePoint Service Application_Database(Microsoft.PerformancePoint.Scorecards.BIMonitoringServiceDatabase)	√	√
PowerPoint Conversion Service Application	This Service Application does not have a database	√	√
Project Service Application	Project Database	√	√
Search Service Application	Search_Service_Application_DB(Administration Database) Search_Service_Application_CrawlStoreDB(Crawl Database) Search_Service_Application_PropertyStoreDB(Property Database)	√	√
Secure Store Service	Secure_Store_Service_DB(Secure Store Service Database)	√	√
Security Token Service Application	This Service Application does not have a database	√	×

Service Application	Databases of the Service Application	Supported in In-place Restore	Supported in Out-of-place Restore
Session State Service	SessionStateService_Database	√	×
State Service	StateService_Database(State Service Database Settings)	√	×
Subscription Settings Service Application	Subscription Settings Database	√	√
Usage and Health data collection	WSS_Logging	√	×
User Profile Service Application	User Profile Service Application_ProfileDB (Microsoft.Office.Server.Administration.ProfileDatabase) User Profile Service Application_SyncDB(Microsoft.Office.Server.Administration.SynchronizationDatabase) User Profile Service Application_SocialDB (Microsoft.Office.Server.Administration.SocialDatabase)	√	√
Visio Graphics Service	This Service Application does not have a database	√	√
Word Automation Services(Word Conversion Service)	WordAutomationServices_Database (Microsoft.Office.Word.Server.Service.QueueDatabase)	√	√
Workflow Service Application	–	√	√
Work Management Service	This Service Application does not have a database	√	×

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	√	√	
Configuration Database	√(Restore Database Only must be used)	×	
Windows SharePoint Solutions	√	√	For in place restore, restoring the uploaded solution and its status in the Solution Management is supported.
InfoPath Form Services	√	√	InfoPath Forms Services Settings and InfoPath Forms Services Form templates are supported.
Global Site Template	√	√	
Custom DB	√	×	
Web-Front-End Server	√	√	
Item Level Restore	√	√	• If you want to do Platform granular Restore, the Platform granular Restore index must be generated. • InstaMount function is supported.
FBA Databases	√	×	The FBA Database and some configurations in the Web.config under WebApp IIS Setting (such as MemberShipProvider) are supported.
BLOB	√	×	

Appendix D – 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		Not Supported	Supported	
SkyDrive Pro		Not 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	Not Supported	Supported	
	Reply	Not Supported	Supported	
	Like	Not Supported	Supported	
	Picture	Not Supported	Supported	
	Link	Not Supported	Supported	
	@	Not Supported	Supported	
	Mentions	Not Supported	Supported	
	Tag	Not Supported	Supported	The tags must be restored with Managed Metadata Service.
Follow	People	Not Supported	Supported	
	Site	Not Supported	Supported	
	Document	Not 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		Not Supported	Supported	

Appendix E – 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 F – Advanced Settings in Configuration Files

AgentCommonWrapperConfig.config

Configure the **AgentCommonWrapperConfig.config** file to specify 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

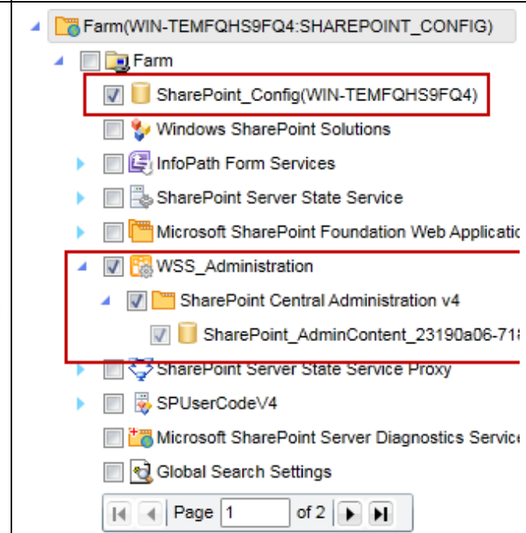
Open the **AgentCommonWrapperConfig.config** file and find the **WrapperCommon** node. Within this node, find the **<RestoredAllWebProperties>False</RestoredAllWebProperties>** node and the **<SpecialWebPropertyNames></SpecialWebPropertyNames>** node. These two nodes are added to the configuration file automatically when you first run a Platform Backup and Restore job at the item level.

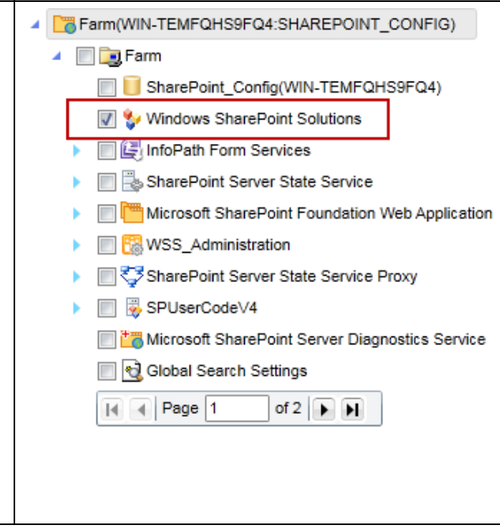
- If you do not want to restore custom properties in property bag, use the default **False** value. When using the **False** value, you can also add the specific custom properties in the **SpecialWebPropertyNames** node, and the custom properties you specified will be restored. Use the semicolon sign to separate the custom properties, for example, **<SpecialWebPropertyNames>property1; property 2; property3</SpecialWebPropertyNames>**. Note that the build-in properties in property bag are all restored.
- If you want to restore all properties including the custom and build-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.

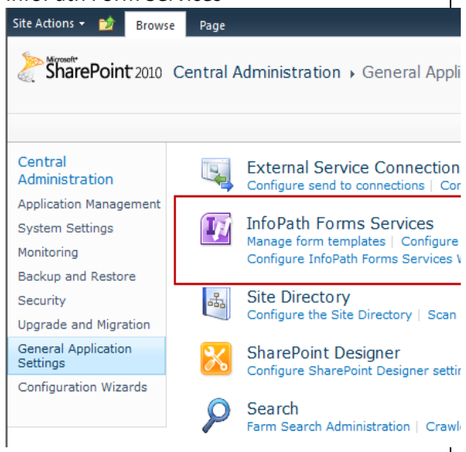
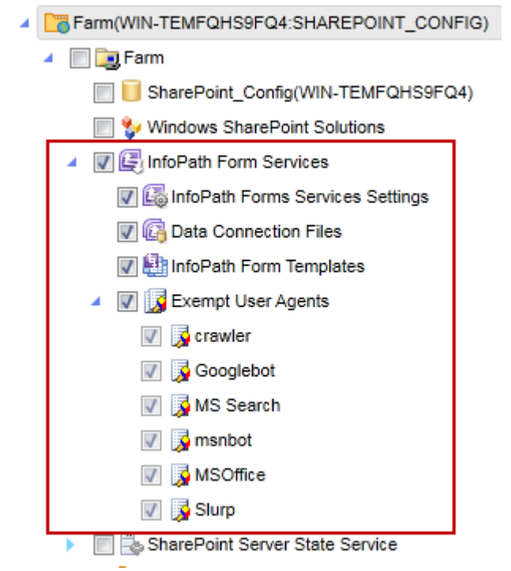
Appendix G – Customization Support Table

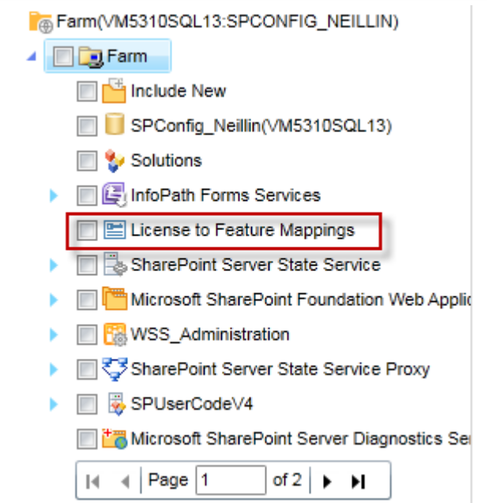
***Note**: Before you restore any content at the specified Restore Granularity, make sure the related higher level SharePoint objects are restored at the farm level or database level. For example, if you want to use the customized feature correctly, you must restore the backed up features in the **Custom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

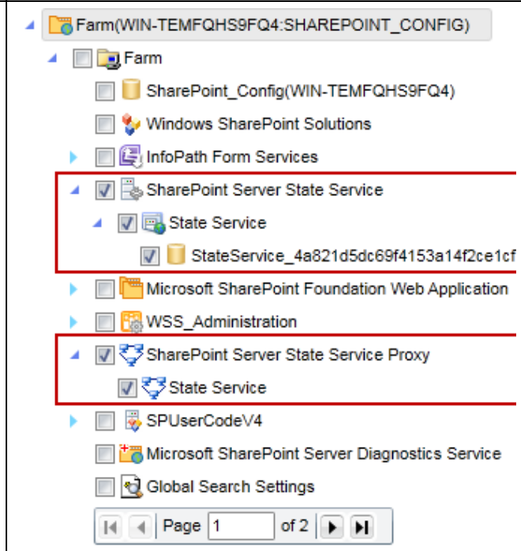
√ means the restore is **Supported** at this level and a blank area means the restore is **Not Supported** at this level.

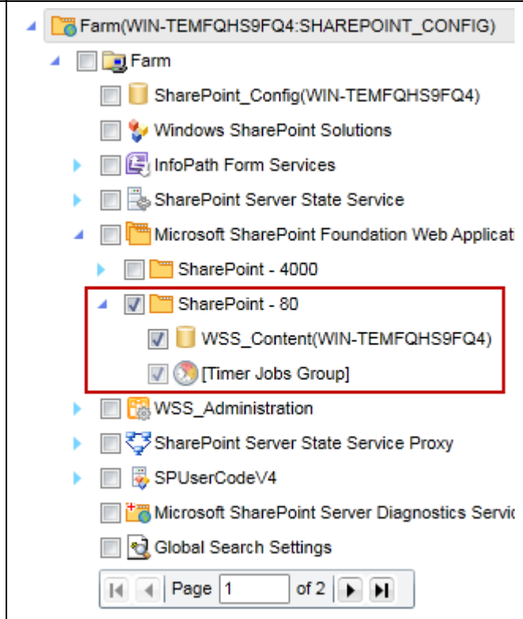
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Central Administration and SharePoint Configuration Database	√	√						The SharePoint Configuration database and the SharePoint Central Administration content database are related to each other, and they can only be restored using In Place restore (with the **Restore Database Only** option enabled). 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.	

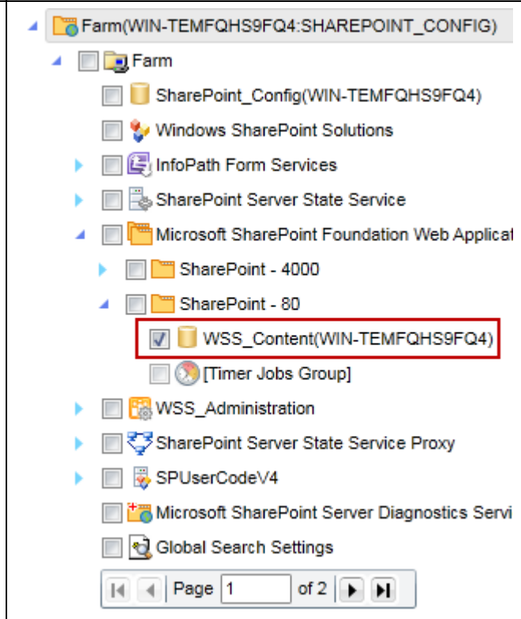
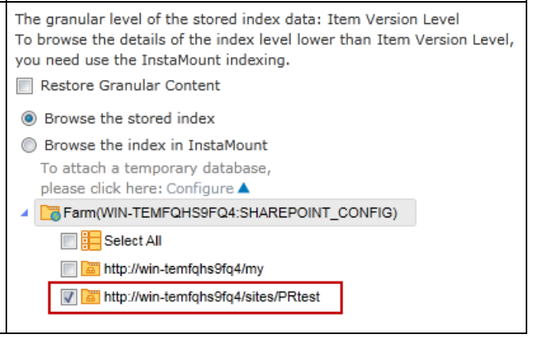
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Windows SharePoint Solutions	√	√							

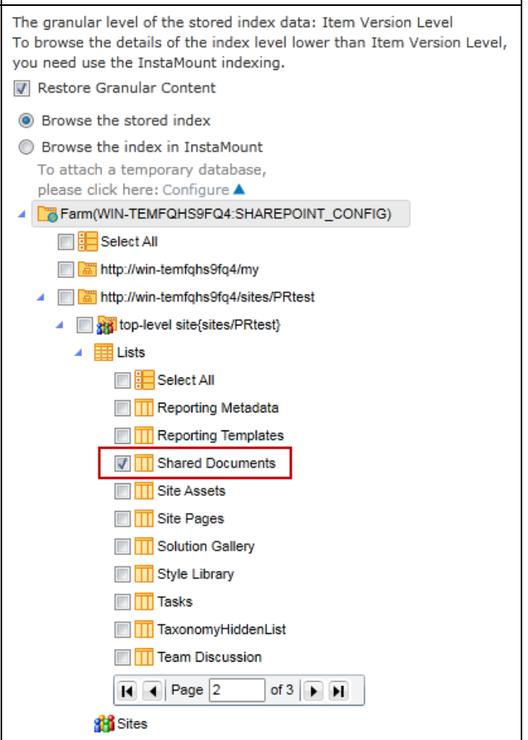
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
InfoPath Form Services 	√	√							

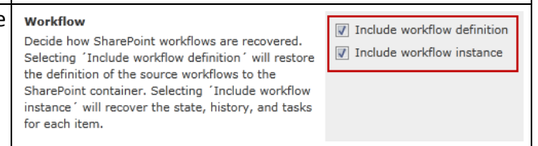
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
License to Feature Mappings	√							This feature is specific to SharePoint 2013.	

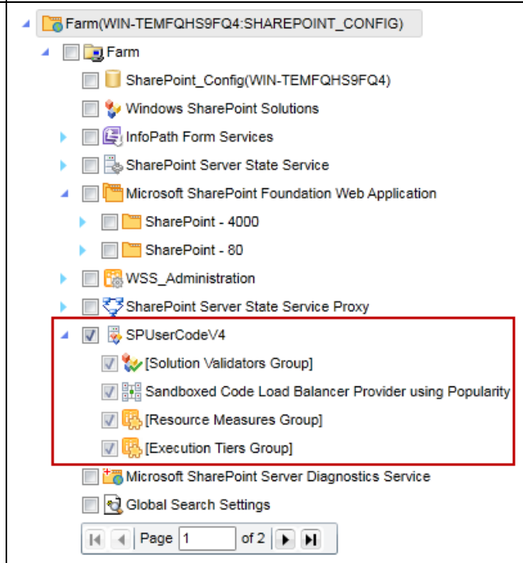
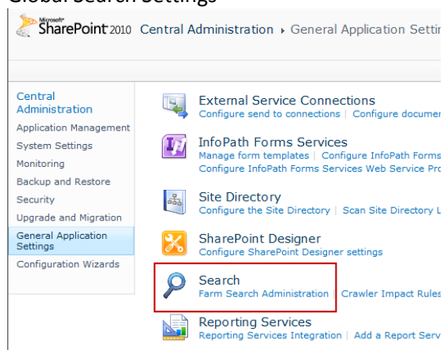
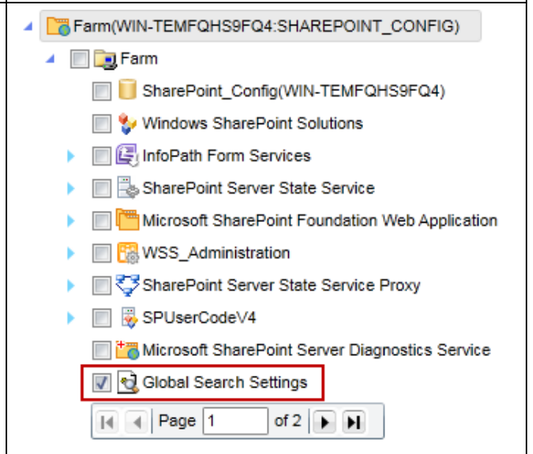
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Server State Service	√	√							

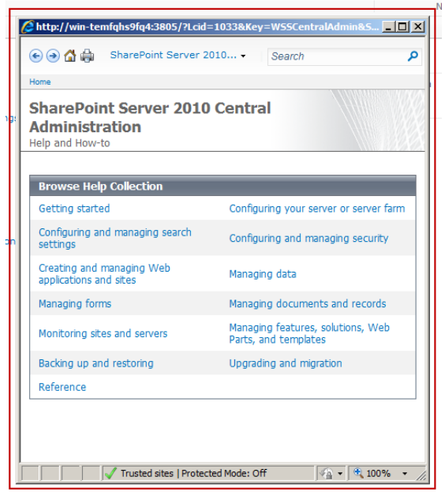
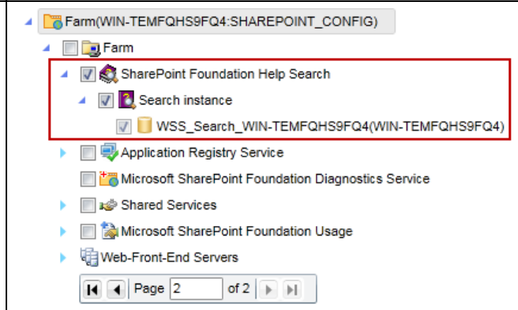
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Web Application	√	√						1. In an **In Place** restore, if you choose to overwrite 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.	

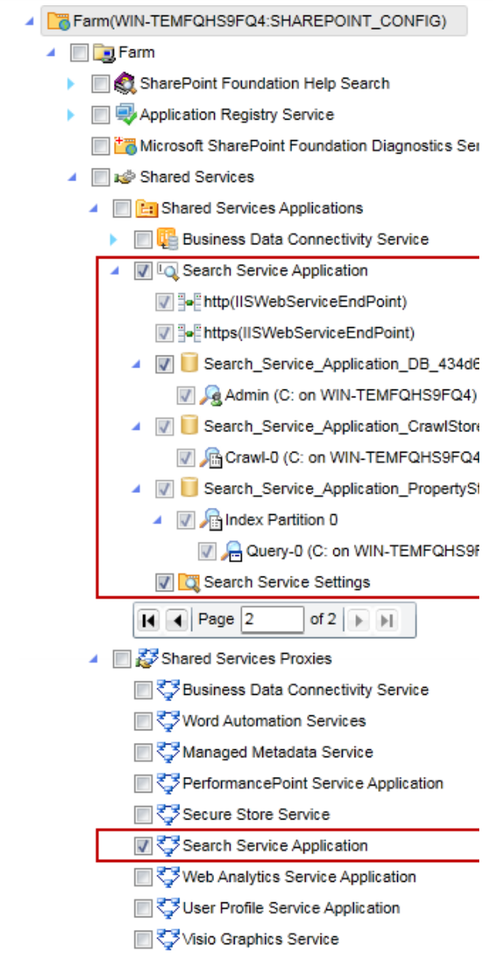
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Content Database	√	√	√	√	√	√	√	For features, they can be restored at Farm Level, Database Level, Site Collection Level, and Site Level. However, when restoring at Site Collection Level, and Site Level, DocAve only restore 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.	

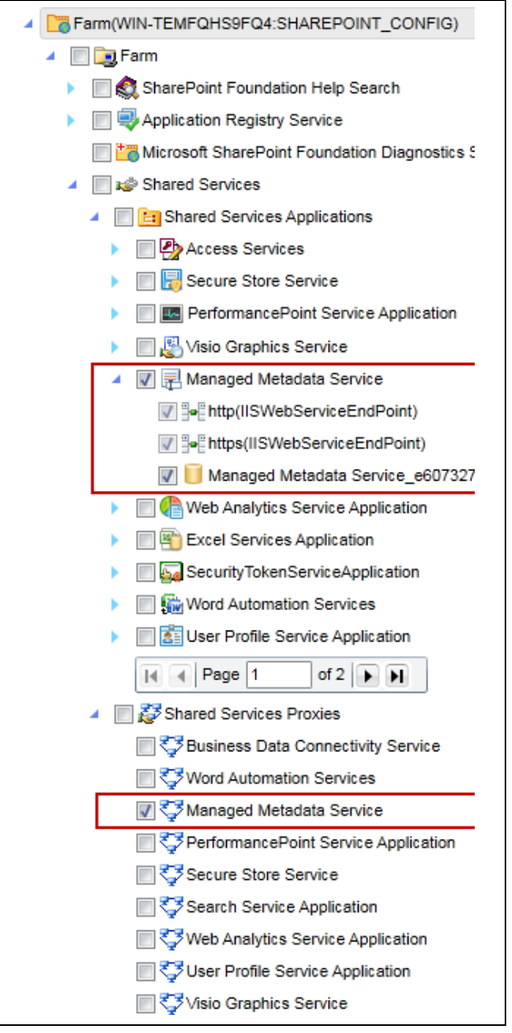
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Lists with Content Types	√	√	√	√	√			The content types in the list will be restored together with the list.	

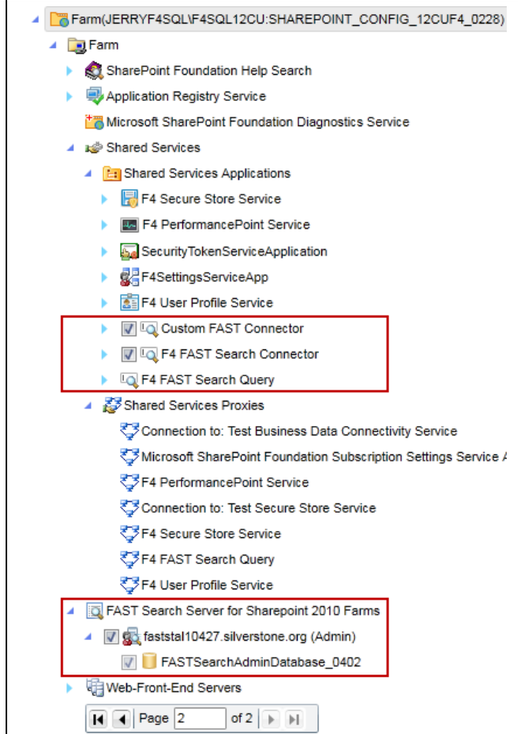
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Built-in Workflow	√	√	√	√	√	√	√	1. If you want to restore the Workflow, 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 G.	
SharePoint Designer Customizations	√	√	√	√	√	√	√	The SharePoint Designer customizations can be restored together with the selected content in the content database.	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

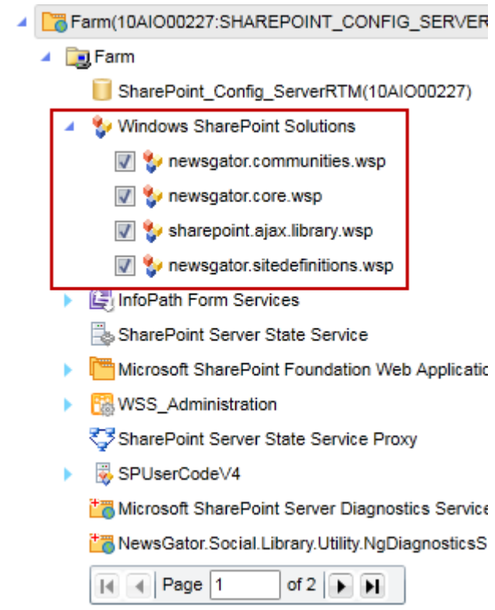
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SPUserCode V4	√	√						Type: Microsoft SharePoint Foundation Sandboxed Code Service Description: Settings for the Sandboxed Code Service.	
Global Search Settings 	√	√							

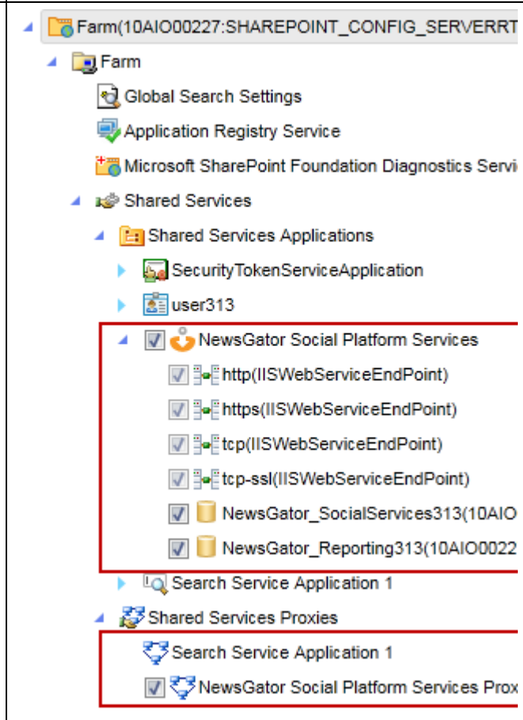
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
SharePoint Foundation Help Search 	√	√						Type: Index files and Databases Description: Search instances for Microsoft SharePoint Foundation	

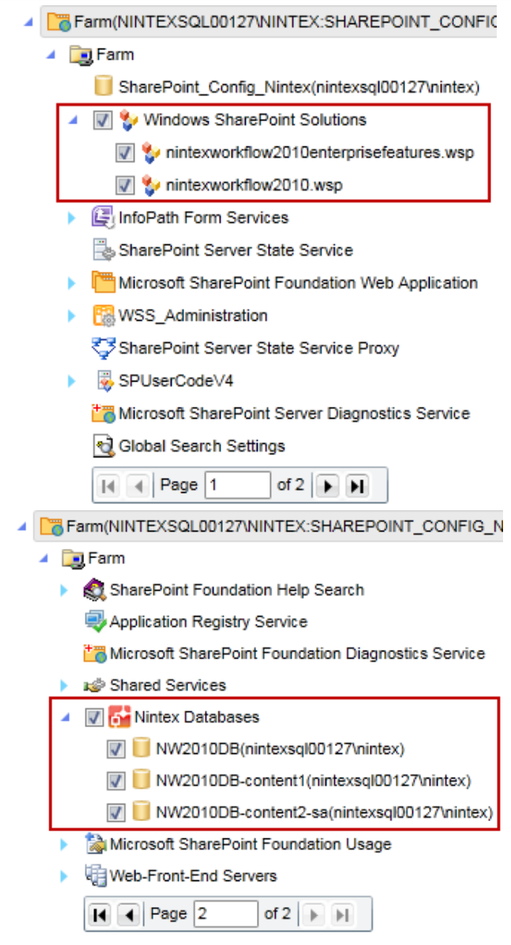
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Search Service Application	√	√						1. Search Service Settings: It is a virtual 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.	

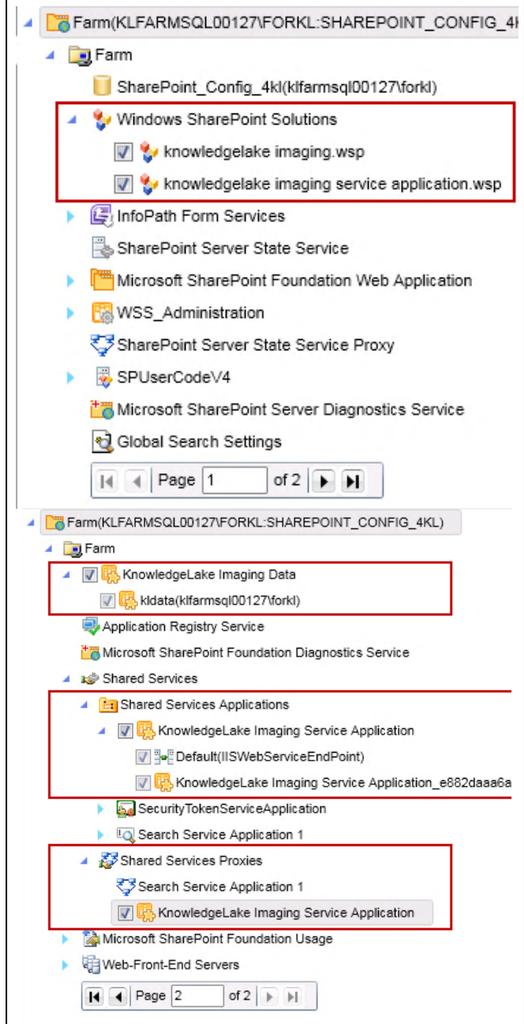
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Service Application	√	√						1. **http (IISWebServiceEndPoint)** and **https (IISWebServiceEndPoint)** 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.	

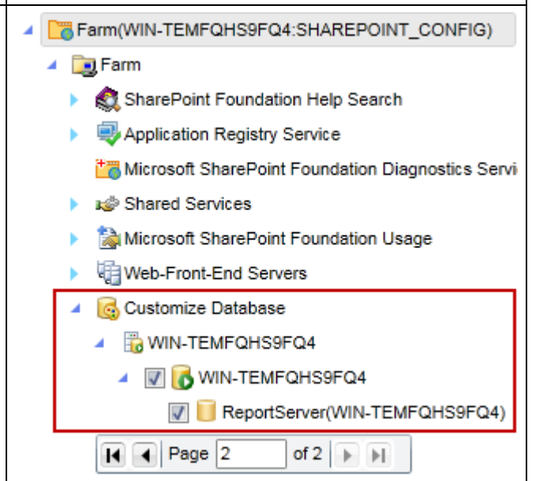
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
FAST Search Server for SharePoint 2010 Farms	√	√						This feature is specific to SharePoint 2010.	

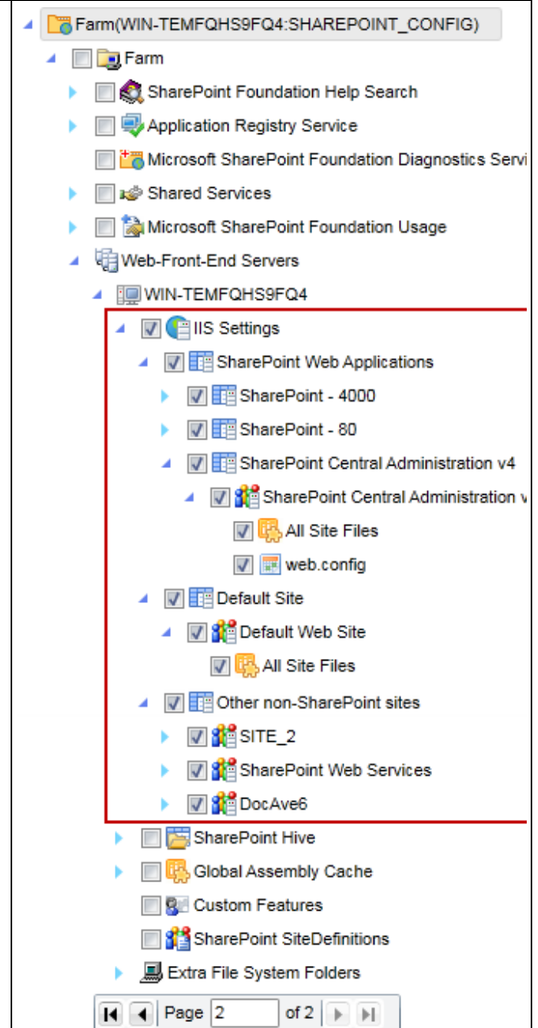
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
NewsGator Social Site 2010	√	√						This feature is specific to SharePoint 2010. 1. NewsGator Social Site 2010 must be installed in the target farm first. 2. If you have uninstalled the NewsGator Social Site and want to restore it, make sure all the nodes are selected. 3. Only **In Place** restore type is enabled when restoring NewsGator Social Site 2010. 4. If NewsGator Service exists in the farm, select **Overwrite** to overwrite the old files; if it has been uninstalled, either **Overwrite** or **Not Overwrite** can be used.	

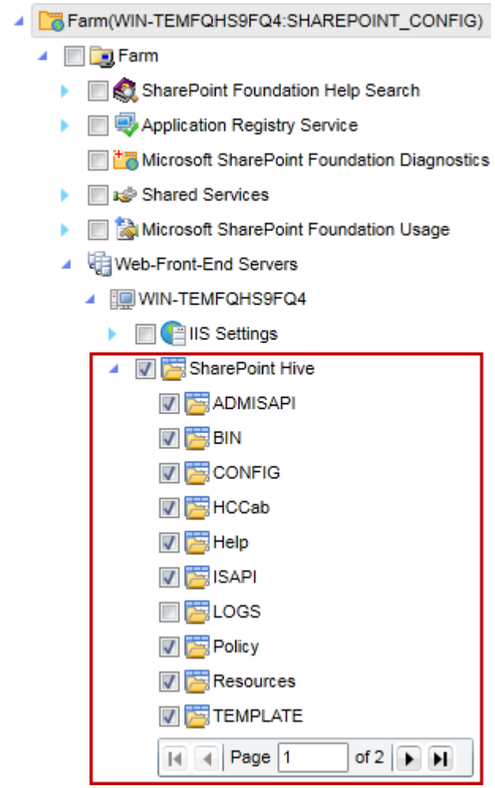
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
									

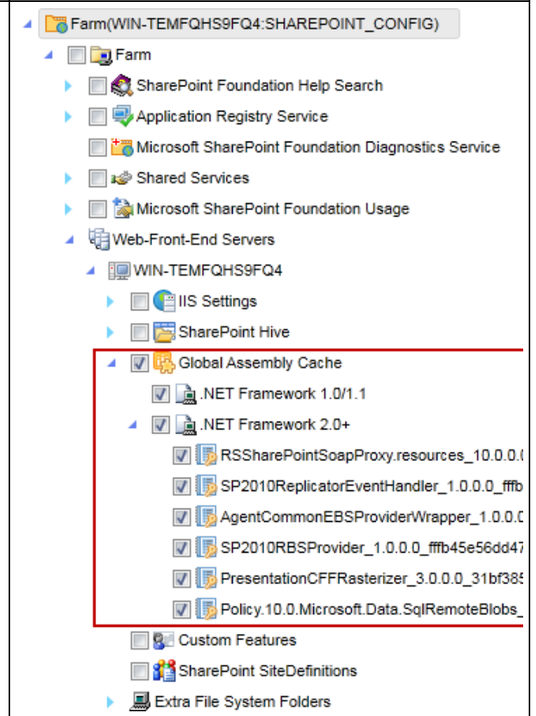
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Nintex Workflow 2010	√	√						This feature is specific to SharePoint 2010. 1. Nintex Workflow 2010 must be installed in the target farm first. 2. Only **In Place** restore type is enabled when restoring Nintex Workflow 2010. 3. If Nintex Workflow exists in the farm, select **Overwrite** to overwrite the old one; if it has been removed, either **Overwrite** or **Not Overwrite** can be used. 4. Nintex Workflow 2013 is not supported.	

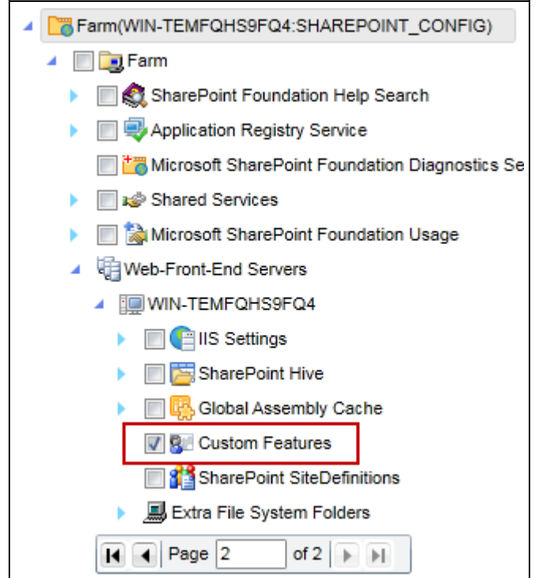
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
KnowledgeLake Imaging 2010	√	√						This feature is specific to SharePoint 2010. 1. KnowledgeLake Imaging 2010 must be installed in the target farm first. 2. Only **In Place** 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 **Not Overwrite** can be used.	

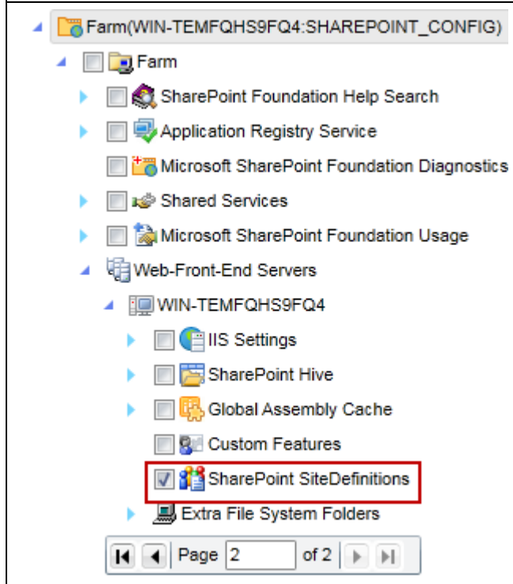
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Customized Database	√	√						You cannot select detailed content inside the database to restore. You can only restore the whole database.	

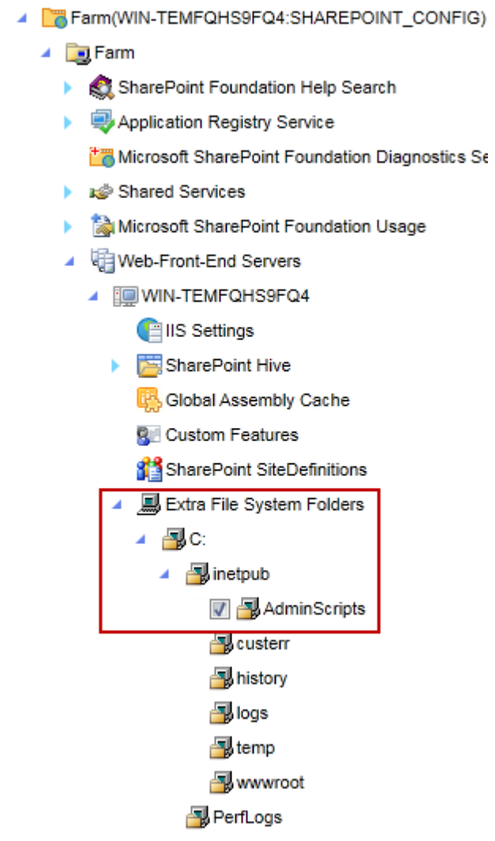
What to Restore / Restore Level	Farm Level	Database Level	Platform Restore with Specified Granularity					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
IIS Settings	√	√						1. If the data you want to restore does not exist in the destination, the data will be restored to the destination no matter you choose **Overwrite** or **Not Overwrite** option. 2. 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 **Not Overwrite** 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					Note	What to Select When Restoring
			Site Collection Level	Site Level	Folder Level	Item Level	Item Version Level		
Global Assembly Cache	√	√						1. 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 **Not Overwrite** option. 2. 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 **Not Overwrite** 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	√	√							

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 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 G

Below are the detailed notes that are referenced in Appendix G – Customization Support Table.

Workflow Definition and Instance

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

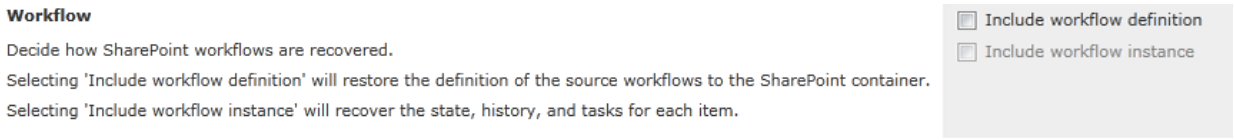


Figure 67: Workflow restore options.

1. **Workflow Definition** – The user-created workflow definition in the site, list, or library.
    - For SharePoint 2010, SharePoint built-in workflows, workflows defined by SharePoint Designer, and workflows defined by Nintex are supported. Workflows defined by Visio Studio are not supported.
    - For SharePoint 2013, SharePoint built-in workflows, list level workflows and reusable workflows defined by SharePoint 2013 designer are 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.

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 there is an existing destination workflow definition that has the **same name** as the one in the source, then the destination workflow instances are deleted, and the source workflow instances are 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 many contents**. 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.

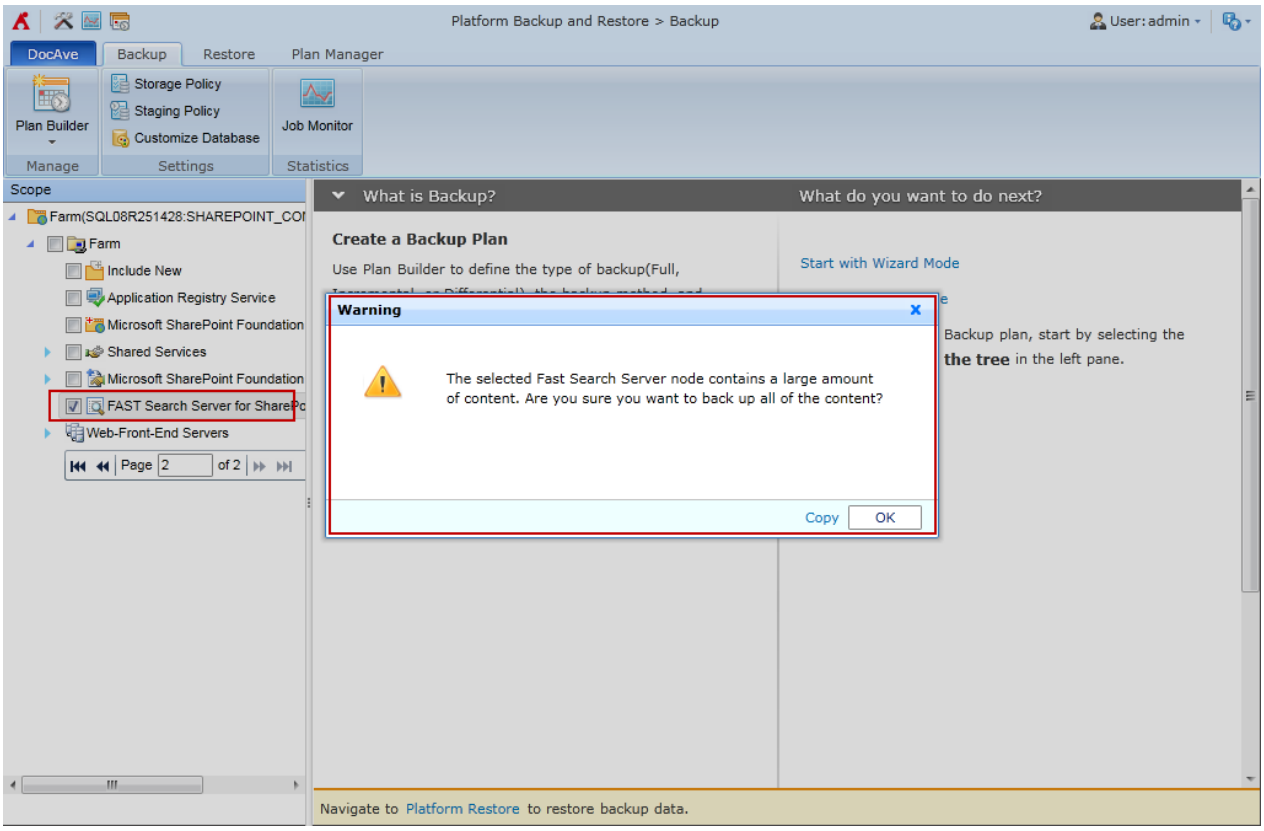


Figure 68: Warning message after selecting the content to back up.

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.

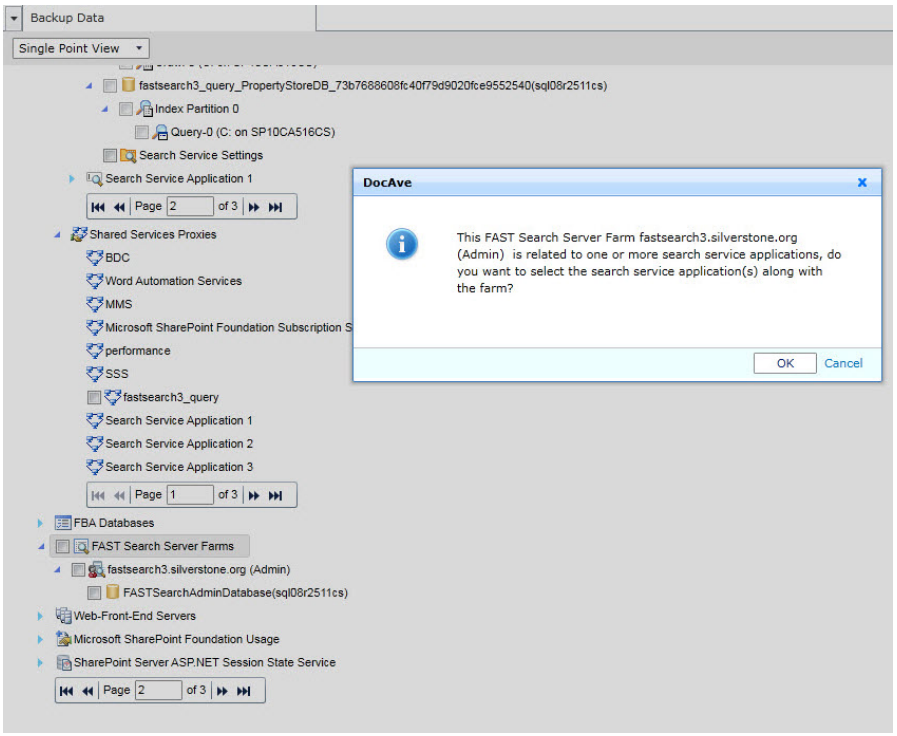


Figure 69: Prompt window after selecting the content to restore.

4. Only **In Place** restore type and **Overwrite/Not Overwrite** restore options 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)	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 © 2012-2013 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States copyright law 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.

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, Microsoft Office SharePoint Servers 2007/2010/2013, SharePoint Portal Server 2003, Windows SharePoint Services, Windows SQL server, and Windows are either registered trademarks or trademarks of Microsoft Corporation.

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 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.
3 Second Street
Jersey City, NJ 07311
USA