



DocAve® 6.0.1 Platform Backup and Restore User Guide

Revision A
Issued April 2012

Table of Contents

Table of Contents.....	2
About DocAve Platform Backup and Restore	4
Complementary Products	4
Submitting Documentation Feedback to AvePoint	4
Before You Begin.....	5
Configuration	5
Agents	5
Licensing and Permissions	6
Local System Permissions	7
Supported Hardware in DocAve 6 Platform Backup and Restore	7
Getting Started.....	8
Launching Platform Backup and Restore	8
User Interface Overview	9
Configuring Devices and Setting Up Storage Policies	10
About the Staging Policy	11
Configuring a Staging Policy.....	12
Selecting Content to Back Up	13
Using the Customize Database Feature.....	14
Performing a Backup.....	15
Overview of Backup Types.....	15
SharePoint Components Supported for Backup.....	17
Using the Plan Builder.....	18
Using Wizard Mode.....	18
Using Form Mode.....	27
Running a Backup Job Immediately	28
Backing Up Extended IIS Web Sites	28
About InstaMount.....	29
InstaMount Mapping and Restore Index.....	29
Recommendations for Using InstaMount.....	29

Performing a Restore	30
Building a Plan.....	30
Building an In Place Restore Plan at Database Level	31
Clearing the Temp Folder before Restoring Database to Most Recent State.....	33
Building an In Place Platform Granular Restore Plan.....	34
Building an Out of Place Restore Plan at the Database Level.....	36
Building an Out of Place Platform Granular Restore Plan	38
Restoring a Raw Database	41
Deselecting the Restore Granular Content Feature	42
Restore Details for Specific Farm Components	43
Selecting the Tree to Restore the Whole Site Collection.....	44
Checking a Job Status.....	45
DocAve 6 Platform Backup and Restore Use Case.....	46
Backing up the Entire SharePoint Farm	46
Restoring the Platform.....	46
Appendix A: SharePoint 2010 Components Supported in Platform Backup and Restore.....	48
Supported Web Parts.....	48
Service Applications Supported for Restore	50
Components Supported for Restore.....	53
Appendix B: SharePoint Object Security and Property.....	56
Index.....	57
Notices and Copyright Information	59

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.

Complementary Products

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

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

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. Click the following URL to access the **Submit Your Feedback** form on our Web site:

<http://www.avepoint.com/resources/documentation-feedback/?flush=1>

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, 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 object(s): IIS Settings, SharePoint Hive, Global Assembly Cache, Custom Features, SharePoint Site Definitions and Extra File System Folders
- Each FAST Search server where you want to back up the FAST Search server settings
- The server with Microsoft SQL Server installed
- Each node of Microsoft SQL Cluster

***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](#).

Licensing and Permissions

To install and use Platform Backup and Restore properly, certain permissions ensure that the agent account has the following permissions.

Control Agent Account

1. **Local System Permissions:** These permissions are automatically configured by DocAve during installation. Refer to Local System Permissions for a list of the permissions automatically configured upon installation. If there are no strict limitations within your organization on the permissions that can be applied, you can simply add the **DocAve Agent Account** to the local **Administrators** group to apply all of the required permissions.
2. **SharePoint Permissions:** These permissions must be manually configured prior to using DocAve 6 Platform Backup and Restore; they are not automatically configured.
 - Member of the Farm Administrators group
 - Full control to all zones of all Web applications via User Policy for Web Applications
 - User Profile Service:
 - User Personal Features
 - Create Personal Site
 - Use Social Features
 - Managed Metadata Service: Term Store Administrator
 - Business Data Connectivity Service: Full Control
 - Search Service: Full Control
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 content databases, SharePoint configuration database, and Central Admin database
 - Database Role of public, dbcreator and Security Admin to SQL Server.
 - Database permission of View server state to SQL Server.
 - One of the following database permissions to SQL Server:
 - Create any database
 - Alter any database
 - View any definition

Member Agent Account (Member Agent Account configured on other SharePoint Servers except the SQL Server)

1. Local System Permissions
 - Member of the following local groups:
 - Administrators
 - FASTSearchAdministrators (this permission is only required for the Member Agent Account configured on the Fast Search server)

Member Agent Account (Member Agent Account configured on the SQL Server)

1. Local System Permissions
 - Member of the **Administrators** local group
2. SQL Server
 - Database Role of sysadmin to SQL Server

***Note:** In order to back up the SharePoint Help Search, the username who enable it must be added to the **Administrators** group on the corresponding machine.

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\EventLog6
 - 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, Dell EqualLogic FS7500, and NetApp DataOntap 7.3.3 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, follow the instructions below:

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

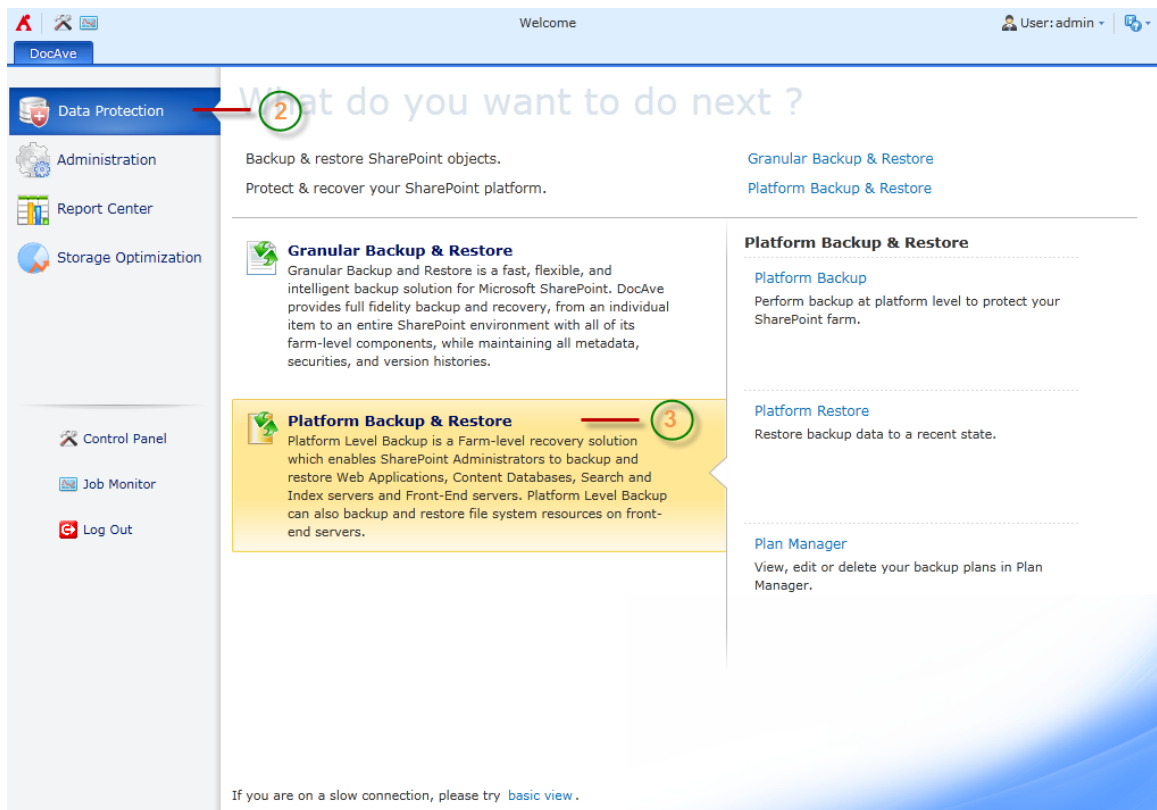


Figure 1: DocAve module launch window.

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.

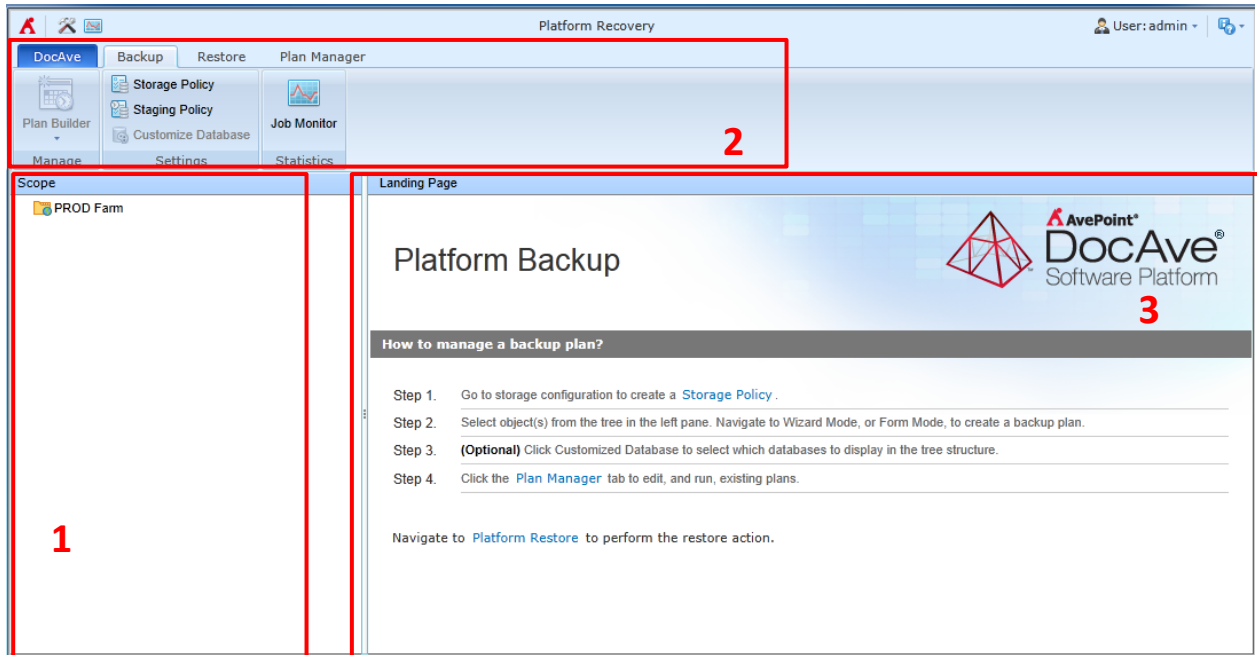


Figure 2: Platform Backup and Restore user interface.

1. The **SharePoint tree (Scope panel)** displays all content within your farm(s). 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 device(s) and then set up a storage policy.

Platform Backup and Restore can write to any Net Share, FTP, TSM, EMC Centera, Cloud Storage, or Dell DX Storage device.

In addition, 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.

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 is used to store the temporary databases that are generated during a backup and restore process.

For ordinary Platform item level Restore, the data is restored to a temporary database first. If there is insufficient space on the SQL Server you are restoring to, you can specify a staging policy to make the restore job run successfully.

When the InstaMount function is enabled, the SQL Server specified in the staging policy stores the InstaMount temporary database. Refer to the scenarios below for details regarding when and how to use the staging policy.

- **Example Job 1** – A Platform granular Restore job with InstaMount granular restore enabled. The backup data index used in the granular restore is generated in the InstaMount temporary database.
If the staging policy is not specified when running the backup job, the InstaMount temporary database is created on the SQL Server that you are backing up.
- **Example Job 2** – A Platform granular Restore job that browses the index in InstaMount. The backup data index used to browse the backup data tree is generated in the InstaMount temporary database.
If the staging policy is not specified when browsing the index in InstaMount, the InstaMount temporary database is created on the original SQL Server that DocAve has backed up.
- **Example Job 3** – A Platform granular Restore job that uses the InstaMount function. The InstaMount temporary database is used to restore the granular content.
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 scenarios, the temporary database cannot be stored on the default SQL Server. To ensure the proper execution of Platform Backup and Restore jobs, the staging policy must be used.

- The SQL Server of the farm is damaged and you want to restore to that farm.
- You do not have the corresponding permissions to the SQL Server you are restoring to.
- There is not enough space to store the temporary database on the SQL Server where you are performing the corresponding Platform Backup and Restore job.

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 **Create Staging Policy** page appears. Configure the following settings:
 - **Staging Policy Name** – Enter a **Name** and optional **Description** for the staging policy.
 - **SQL Agent Name and Instance Name** – Select a **SQL agent name** (a DocAve Agent that is installed on the SQL database server). Select the **SQL instance name** (where to save the 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 the SQL database server where the DocAve Agent is installed are listed in the drop-down box.
 - **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.
3. Click **Validation Test** to verify the access to the SQL Server.
 - **Temporary Database Configuration** – Set up the configuration of the temporary database.
 - **Minimum amount of free space to leave** – Specify the minimum free space for the database file location and log file location. DocAve ensures the specified space exists in the corresponding location. If the free space exceeds the threshold, the corresponding job will fail.
 - **Temp database file location** – Specify a local path on the SQL Server to store the data (.mdf) file of the temporary database. The format of the path is **C:\data**. The default location is *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 log (.ldf) file of the temporary database. The format of the path is **C:\data**. The default location is *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. To select the content to back up:

1. Double-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.
2. 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.
3. In the screenshot below, the following SharePoint objects will be backed up by the Platform Backup plan.
 - Newly-created Web application(s) under the **Microsoft SharePoint Foundation Web Application** node (because **Include New** is selected)
 - Any content database(s) of the existing/newly-created Web application(s) under the **Microsoft SharePoint Foundation Web Application** node
 - The **Finance Web** and **HR Web** Web applications

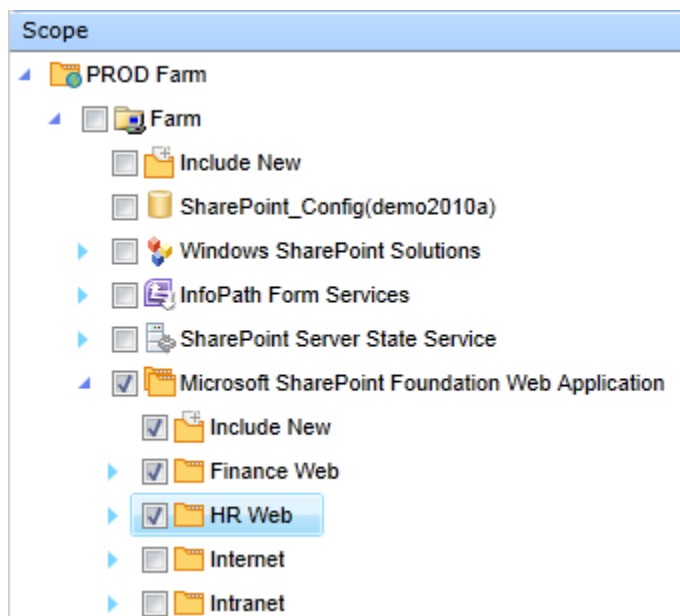


Figure 3: Selecting SharePoint farm content.

4. 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 those customized databases that are not listed. Such databases include the database of a solution, the database of a third party software, and so on.

Once the 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.

Performing a Backup

There are several ways to configure and perform a Platform Backup. Once the [content to back up is selected](#), backups can be run using the following methods:

- [Using Plan Builder \(Wizard Mode or Form Mode\)](#)
- [Running an Immediate Backup](#)

Refer to the sections below for more information.

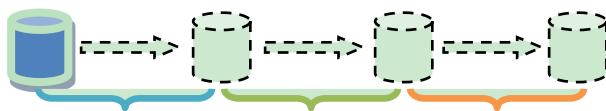
Overview of Backup Types

When configuring 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 file(s), each time a backup is performed. This option requires the most storage space because, depending upon the size of your SharePoint environment, each backup file can be substantial in size. Unlike Incremental and Differential backups, all Full backup files are independent of one another and do not have any dependencies on other back up 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 formal 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.

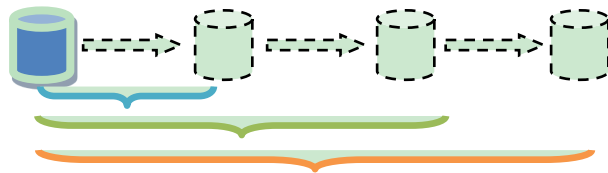
For example, if the following backups are performed in this order– Full Backup, Incremental Backup, Incremental Backup, Incremental Backup:



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:



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:** If you back up a database, and then add more data (.mdf) files and log (.ldf) files to the database, a **Full Backup** job must be run immediately to ensure data integrity.
- 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, 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 Web Service.
- SharePoint solutions – This includes any SharePoint customizations deployed to SharePoint in the form of solutions. These solutions and their deployment statuses are backed up.
- Nintex databases – This includes Nintex workflow config database, content database, and solutions.
- NewsGator – This includes NewsGator Social Platform Services (including corresponding databases), NewsGator Social Platform Services Proxy, and solutions.
***Note:** Only Social Sites (NewsGator) 1.0 is supported in DocAve 6.0.
- KnowledgeLake – This includes KnowledgeLake Imaging Data, KnowledgeLake Service Application, KnowledgeLake Proxy, and solutions.
- SharePoint front-end resources – The front-end Member Agent backs up the IIS settings (both metadata and files), SharePoint site definitions, SharePoint hive files, Global Assembly Cache files, custom features, and extra file system folders.
- FAST Search Server Farms – FAST Search Server Farms backup is supported.

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

Using the Plan Builder

Both Platform Backup and Platform Restore use Microsoft Volume Shadow Copy Services (VSS) snapshot technology to protect your SharePoint farm. Use the **Plan Builder** when you wish 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

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 additional information.
 - **Use DocAve Platform Recovery 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, but does not truncate the transaction log.

If you select this option, all of the DocAve Platform Backup options can be used, making the backup 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** (recommended) (the default option) – 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 results in very large log files.

***Note:** In order to enable the [Restore Database to Most Recent State](#) function when performing the Platform Restore, the **Perform log backup after full backup** checkbox must be selected when setting up the backup plan.

- **Use DocAve Platform Recovery 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** in SQL Server: both the database's data file and log file are copied, but this option does not truncate the log, ensuring that all backups remain synchronous. 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 Recovery in addition to other existing SQL backup methods for SharePoint databases**, only Full backup is supported. Despite the fact that other backup type selections are available in the **Schedule** step, **ONLY** a Full backup will be performed regardless of which type of backup you select.

3. Click **Next**. The **Storage Policy** page appears.
4. Specify a **Storage Policy** to save the backup data from the drop-down list. 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.
5. Specify the optional operations to perform on the backup data.
 - 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.
 - 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 compression.

***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.
6. Click **Next**. The **Backup Method** page appears.
7. Choose whether or not to **Create Persistent Snapshots** of the selected objects. If you select **Yes**, DocAve saves on the corresponding hardware the snapshot taken 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, it is recommended that you use this option 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.

- Configure the **Snapshot Retention Policy**. Enter the maximum number of snapshots the current plan can take in the corresponding textbox.
- 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](#).

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

9. Choose whether or not to **Enable InstaMount 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 [Recommendations for using InstaMount](#) and [InstaMount Mapping and Restore Index](#) for more information.

***Note:** InstaMount is **only** supported for Net Share logical devices.

- If you select **Yes**, you can select the **Staging Policy** for storing the InstaMount temporary database. For more information on the staging policy, refer to [Configuring a Staging Policy](#).
- To inform specified users of the Platform Backup job, configure the email **Notification** settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.

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

11. 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.

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

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

- **Copy snapshot data to media server for last ... backup(s)** – The snapshot data of the specified latest backup(s) are sent to the storage policy selected in the [Storage Policy](#) step.
- **Generate InstaMount mapping for last ... backup(s)** – This option generates the mapping for the InstaMount function for the specified number of latest backup(s) in the storage policy selected in the [Storage Policy](#) step. The generated mapping is used in Platform granular Restore.
***Note:** If you did not enable the InstaMount granular restore in the **Advanced** step, you can generate the InstaMount mapping using this selection.
- **Generate granular restore index for last ... backup(s)** – This option generates the granular restore index for the specified number of latest backup(s) in the storage policy selected in the [Storage Policy](#) step. 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](#).

14. **Maintenance Schedule** – Define the **Schedule type selection** for the scheduled maintenance jobs.

- **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.

15. 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**. All the schedules will be displayed in the **Summary** table. Click **X** to delete a schedule.

16. **Maintenance Notification** – To inform specified users of a maintenance job, configure a notification. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.

17. When finished, click **Next**. The **Overview** screen appears.

18. 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.
 - Check the **Save current plan as plan template** check box to save the current plan as a template. Enter the template name in the textbox; after this plan template is saved, you can select it when creating a new plan.
19. On the lower-right section of the screen, 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.

Snapshot Retention Policy

If you apply a retention policy on the snapshot, both the **MaxSnapshotCount** rule in the configuration file and the rule of the snapshot threshold configured in the Plan Builder is checked when running the backup job. For information on configuring the snapshot retention rules, refer to [Setting up Snapshot Retention Rules in the Configuration File](#) and [Setting up Snapshot Retention Rules in Platform Backup and Restore Plan Builder](#).

The following information describes the logic for the retention rules in detail.

1. During the backup job, DocAve checks the retention rules twice.

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

***Note:** When checking the number of current snapshots stored on the hardware, the number of snapshots taken by the third party software will also be counted.

After the check, DocAve then performs the 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 data of the current plan's oldest snapshot is transferred to the logical device immediately and the snapshot is deleted from the hardware. A new job of 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 the jobs related to the deleted snapshot fail. Then the new job of the current plan starts.

Note the following:

- If the current snapshot number on the hardware is greater than or equal to (\geq) the **MaxSnapshotCount** configured in the configuration file, DocAve executes the policy you specified in Platform Backup and Restore Plan Builder.
 - ***Note:** DocAve will test whether there is enough space for the new snapshot after the retention. If there is not, the exceeded snapshot(s) are not deleted and the new backup job fails.
 - If you select **Policy 1** or **Policy 3**, DocAve deletes the current plan's oldest exceeded snapshot(s) 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** configured in the configuration file, DocAve runs the new backup job directly.

2. The second check occurs after backing up the desired data.

DocAve compares the number of snapshots that the current plan has taken with **The amount of snapshots you want to keep is ...** value you configured in the Plan Builder.

After the check, DocAve then performs the 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 data of 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 snapshots that the current plan has taken is greater than ($>$) **The amount of snapshots you want to keep is ...** configured in the Plan Builder, DocAve copies the data of the current plan's oldest exceeded snapshot(s) to the logical device, and then deletes it (them) from the hardware.
 - ***Note:** DocAve will test whether the snapshot(s) that the current plan has taken still exceeds the threshold (**The amount of snapshots you want to keep is ...** configured in the Plan Builder) after the retention; if it does, the exceeded snapshot(s) are not deleted. However, the new backup job completes since the new snapshot has been taken.
- If the number of snapshots that the current plan has taken is smaller than or equal to (\leq) **The amount of snapshots you want to keep is ...** configured in the Plan Builder, DocAve completes the new backup job directly.

***Note:** Snapshots taken by third party software/other plans cannot be deleted during the snapshot retention in the backup job. For example, if there are 4 snapshots on the hardware now (3 are taken by the third party software, 1 is taken by another DocAve Platform Backup and

Restore plan), and the **MaxSnapshotCount** configured in the configuration file is 3, then the backup job will fail.

***Note:** If you do not choose **Copy data from snapshot to Media server** option when running the backup job, the corresponding snapshot cannot be deleted during the snapshot retention that enables [Policy 1](#) in the Plan Builder.

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.

You must modify the value of the following attributes in the configuration file on the Agent server where the hardware is connected; otherwise, the configuration will not take effect.

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

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

```
  <DriverLetter path="c:"/>
```

```
</VolumeConfig>
```

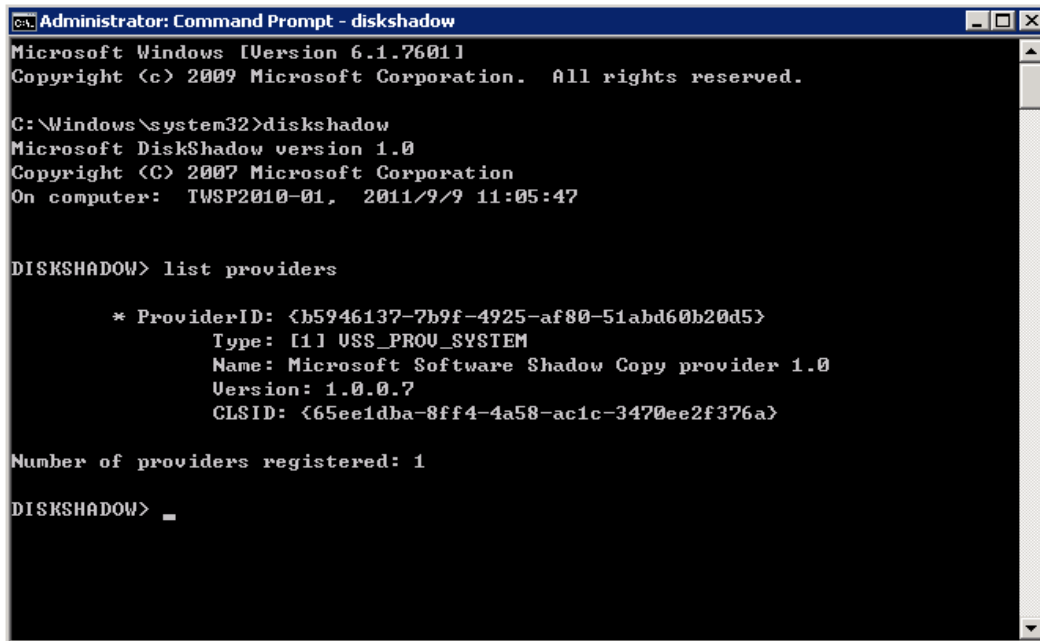
```
<HardwareProviderConfig MaxSnapshotCount="64" AlwaysSendPartialData="false">
  <!-- providerOption 0-vss default, 1-Force system provider,2-set a prefer vss provider. default to 0
  MaxSnapshotCount max snapshot can be done on the volume for the provider
  Example, NetApp H/w luns configuration
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

Figure 4: 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 the screenshot below.



```
Administrator: Command Prompt - diskshadow
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskshadow
Microsoft DiskShadow version 1.0
Copyright (C) 2007 Microsoft Corporation
On computer: TWSP2010-01, 2011/9/9 11:05:47

DISKSHADOW> list providers

    * ProviderID: {b5946137-7b9f-4925-af80-51abd60b20d5}
      Type: [1] USS_PROU_SYSTEM
      Name: Microsoft Software Shadow Copy provider 1.0
      Version: 1.0.0.7
      CLSID: {65ee1dba-8ff4-4a58-ac1c-3470ee2f376a}

Number of providers registered: 1

DISKSHADOW> _
```

- **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 the performance of the operating system.
- **path** – The name of the drive that links to the hardware.

Setting up Snapshot Retention Rules in the Plan Builder

In the Platform Backup and Restore Plan Builder, you can set the maximum amount of snapshots that the current plan can take.

The amount of snapshots you want to keep is ... – Specify the maximum number of snapshots that the backup plan can save on the hardware. Considering performance, it is not recommended that the value of this attribute be larger than 64. If the number of snapshot(s) that the current plan has taken exceeds this maximum number, the old snapshot(s) taken by the current plan are deleted when the desired data in the new job is backed up. The deletion is performed after the old snapshot(s) data is saved to the corresponding logical device so that the old snapshot(s) data can be found, if necessary.

Backup Schedule

Configure the following settings to build a new backup schedule.

1. **Backup Options** – Select the backup options for the scheduled backup job. Refer to [Overview of Backup Types](#) for additional information.

***Note:** When running the Platform Backup plan for the first time, if you choose to do an Incremental Backup or Differential Backup, DocAve performs a **Full** Backup. It is mandatory.

- **Copy data from snapshot to media server** – Copy the snapshot data from the hardware to the corresponding 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 copying 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 the scheduled/manual maintenance job 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 the scheduled/manual maintenance job after the backup job completes.
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** – Select this option to not generate the granular restore index for the backup data in the corresponding logical device. The index can be generated using the scheduled/manual maintenance job after the backup job completes.
 3. **Type** – Select the interval at which the backup occurs.
 4. **Schedule Settings** – Set up the frequency for the scheduled backup job. If you select the type as **Hourly**, **Weekly**, or **Monthly**, you can set up the advanced settings for the frequency. For more scheduling options, click the **Advanced** checkbox to reveal additional options.
 5. **Range of Recurrence** – Select the start time and end time for the schedule.

Manual Maintenance

As opposed to scheduled maintenance jobs (which can be configured in the backup plan), you can perform maintenance job manually in Job Monitor on jobs that have already completed.

- **Maintenance Notification** – If you want to inform some users of the maintenance job, configure a notification and specify the detailed settings in **Advanced Settings**.

The **Report** drop-down list displays the types of the recipients. The **Type** drop-down list displays the supported types notifications. Enter the email addresses of the recipients in the **Recipient** textbox.

- **Summary report level(s)** – Define when to send the summary report. By default, **Success**, **Failure**, and **Warning** are all selected. After the job completes, fails, or completes with an exception, a summary report is sent to the recipient.
- **Detailed report level(s)** – Define when to send the detailed report. By default, **Success**, **Failure**, and **Warning** are all selected. After the job completes, fails, or completes with an exception, a detailed report is sent to the recipient.
- **Message format** – Select the format that the message will be delivered in: **HTML** or **Plain text**.
- **Send all logs to recipient** – Select **Yes** to send all logs to recipient when the job fails, or select **No** to not send the logs.

The 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 maintenance jobs on the **Finished** backup jobs of the database(s). The backup jobs must have deferred coping data from persistent snapshot, or generated InstaMount mapping, or generated granular restore index. Once the deferred operation(s) has been performed by the maintenance job, the corresponding options/buttons will be greyed out.

Using Form Mode

Form mode is recommended for users who are familiar with building 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](#) 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 job is run immediately after the Wizard Mode plan is saved.

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

Backing Up Extended IIS Web Sites

If you back up the IIS Web site of a Web application using a **Platform Backup** job and then extend the corresponding Web application, refer to the steps below to back up the newly extended IIS Web site.

1. Reload the previously saved plan.
2. Refresh the backup tree of the plan and save the plan again.
3. Perform a **Full Backup** job of the saved plan in step 2. The newly extended IIS Web site will be backed up after successful execution of the plan.
4. After the **Full Backup** job completes, you can back up the modifications to the Web application's IIS Web site using a **Full/Incremental/Differential** backup.

About InstaMount

Refer to the sections below for information related to the InstaMount function.

InstaMount Mapping and Restore Index

The InstaMount mapping file is generated from the 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. Both the mapping file and the granular restore index can be generated during the corresponding Platform Backup and Restore job or by a maintenance job.

- When running the Platform Backup job, if **InstaMount Granular Restore** is not enabled, the index is generated from the original databases being backed up. This may occupy more resources on the corresponding SQL Server.
- When generating the granular restore index using a maintenance job, the InstaMount function is used to generate the index.

Recommendations for Using InstaMount

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

It is recommended that users enable the InstaMount function to restore the items that are small in size whose size. The following are the advantages of using InstaMount:

- The InstaMount temporary database is much smaller than the ordinary temporary database used by the ordinary restore method, so it uses less space on the SQL Server.
- The Platform granular Restore can be much faster.

However, if you are restoring large amounts of data, the advantages of using InstaMount function are not significant; it is not recommended to use InstaMount in such cases.

You can also try to use the InstaMount function to restore from the backup data which is partially damaged. If the information that Platform Restore leverages to restore content still exists in the damaged data, then the restore can be performed.

***Note:** The use of InstaMount requires minimal disk space.

Performing a Restore

Both Platform Backup and Platform Restore use Microsoft Volume Shadow Copy Services (VSS) snapshot technology to protect your SharePoint farm. A 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 A](#).

***Note:** The Platform Backup and Restore Control Agent account must be the **Administrator** of the specified site collection in order to restore the corresponding site administration level search scope.

Building a Plan

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

1. Select the **Restore** tab and click **Restore** in the **Manage** group. From the **Time-based Restore** tab, configure the following options.
2. **Job Filter** – Limit the scope of backup data to be restored by filtering out specified backup jobs.
 - **Plan Filter** – Filter the backup data by plan information.
 - **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 in the next step.
 - **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 in the next step.
 - **Job Filter** – Limit the backup jobs by job type.

- **Backup type** – Select the backup type from the drop-down list; only the backup jobs of the specified types are displayed in the next step. Select **All Types** to list the backup jobs of all three types.
 - **Restore granularity level** – Select the restore granularity level from the drop-down list; only the backup jobs of the specified restore granularity level(s) are listed in the next step. Select **All Types** to list the backup jobs of all levels.
 - **Time Range** – Filter backup data by completion time range.
 - **Entire period** – Select this option to display all Finished/Finished with Exception Platform Backup jobs in the next step.
 - **Specify time range** – Select this option to specify a time period. All of the Platform Backup jobs whose start time is in the specified time period are displayed in the next step.
3. **Backup Jobs** – All of the backup jobs that meet all the filter rules are listed in the calendar. Place the mouse cursor over the backup job, to display job information such as the Plan Name, Job ID, Backup Option, Restore Granularity Level, and Job Status. Click on **Day**, **Week**, or **Month** to change the view to see all the available jobs during that time period. Click the page turning button at the top-left corner to turn the page. Select the backup job that you want to restore.
4. Click the link applicable to your type of restore to continue with instructions on building the job:
- [In place restore job at database level](#)
 - [In place platform granular restore](#)
 - [Out of place restore at database level](#)
 - [Out of place platform granular restore](#)
 - [Restore raw database](#)

Building an In Place Restore Plan at Database Level

***Note:** To ensure data integrity and protect your farm, [a full backup](#) of the restored SharePoint object(s) must be performed after DocAve completes each in place Platform Restore job at the database level.

***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.

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** – 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.
4. **Restore Settings** – Choose the detailed settings of the restore job.

- **Restore Database to Most Recent State** – Restore a SharePoint database to its most recently-modified state. If you have made modifications to the database after it has been backed up and you want to restore the database with these changes, select **Yes** to enable this option. With this option enabled, DocAve restores the backed-up database first and then modifies the database to its most recent status using the log files backed up in the Incremental backup. The database will be recovered together with any recent modifications that were made after the latest database backup. Select **No** to restore only the backed up database.

***Note:** If you intend on performing a Platform Restore job using this option, you must first clear the **Temp** folder on the corresponding SQL Server before running the restore job. For more information, refer to [Clearing the Temp Folder before Restoring Database to Most Recent State](#).

- **Restore Database Only** – If **Yes** is selected, only the selected databases are restored with no attempt to connect them to the SharePoint environment. This is useful in the instance when a SharePoint environment has not yet been set up (for example, during a whole farm restore). This can also be used in cases where you want to perform 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 by selecting this option.

- **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 original database is deleted, and the temporary database is renamed to the original database name and then connected to the SharePoint farm. If you select **No**, the original database is deleted directly when the **Overwrite** restore job begins.

5. In the case of a **Not Overwrite** restore job at the database level, the restore job performs no action if the original database has the same name as the one in the backup.

- **Restore Option** – 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.
 - Configure the email **Notification** settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
6. When finished configuring Restore Settings, click **Next**. The **Schedule** page appears.
 7. **Schedule** – Choose whether or not to create the restore job on a schedule. If you decide to configure the schedule yourself, input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.
 8. When finished, click **Next**. The **Overview** page appears.
 9. Review and edit the job selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
 10. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Clearing the Temp Folder before Restoring Database to Most Recent State

If performing an in place Platform Restore job at the database level using the **Restore Database to Most Recent State** feature, you must first follow the steps below to clear the **Temp** folder on the SQL Server.

For SQL Cluster environment, the following steps must be performed on each SQL Cluster node.

1. Navigate to the installation path of the DocAve Agent, which is ... \AvePoint\DocAve6\Agent\temp by default.
2. Look for the **TAILLOG** folder in the **temp** folder.
 - If the **TAILLOG** folder does not exist, you can run the in place Platform Restore job at the database level using the **Restore Database to Most Recent State** feature with no further action required.
 - If the **TAILLOG** folder is in the **temp** folder, back up all of the files in the **TAILLOG** folder to a local path. Then empty the **TAILLOG** folder and proceed with the restore database job.

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 to restore. Click **View Details** link on the top right corner of the **Backup Data** pane to view the detailed backup data for the selected database.
 - **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 restore the granular content. In addition, if you do not select this option when performing an **Overwrite** restore, the newly-added content in the original site collection might be lost. Refer to [Deselecting the Restore Granular Content Feature](#) for detailed information.
 - **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.

***Note:** This option can only be used when no manual/scheduled maintenance job is running on the backup data you are browsing.

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 original SQL Server which DocAve has backed up. If you want to change the location of the InstaMount temporary database, click the **Configure** link and you can select a staging policy for storing the InstaMount temporary database generated during the browsing. For more information, refer to [About the Staging Policy](#).

***Note:** If the granular restore index is not generated for the specified Platform Backup job, this option must be used when restoring the backup using Platform granular Restore.
3. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the **Item Browser** pane on the right.
 - **Container Configuration** – Specify the configuration of the container being restored.
 - **Security** – Refer to [Appendix B: SharePoint Objects Security and Property](#) for the detailed information related to security.
 - **Property** – Refer to [Appendix B: SharePoint Objects Security and Property](#) for the detailed information related to property.
4. When finished, click **Next**. The **Restore Type** page appears.
5. **Restore Type** – Choose where the content will be restored.
 - **Restore Type** – Select the location where to restore the backup data. In this case, select **In place restore** to restore the selected content to the original SharePoint location.

- **Agent Group** – Select the agent group to perform the restore job.
6. Click **Next** when finished. The **Restore Settings** page appears.
 7. **Restore Settings** – Configure how the content will be restored.
 - **Restore Option** – Specify the action to be performed on conflicts when performing the Platform granular Restore. Items with the same item ID and files with the same file name in both the backup and the original farm are considered conflicts by DocAve.
 - **Not Overwrite** – Ignore the backed-up file/item which has the same name/ID as the original one. The item in the backup will not be restored.
 - **Overwrite** – Copies the backed up file/item to the original location by overwriting the existing file/item that has the same name/ID.
 - **Append** – For the folder/site/site collection level, the original content is overwritten by the same content in the backup. For the item/item version level, a suffix (_1, _2, _3 ...) is added to the filename in the backup and it is restored to its original location. A backed-up item with a different **Modified Time** will be increased by 1 in the ID and restored to its original location with the same name. If the backed-up item has the same **Modified Time** as the original item, the original item is overwritten by the corresponding item in the backup. After the **Append** restore job, both the original file/item and the restored file/item exist in the original location.
 - **Replace** – The original content is deleted and replaced with the same content in the backup. This option can only be used at folder/site/site collection level.
 - **Include Recycle Bin Data** – Choose whether to compare the data in the backup with the data in the original SharePoint farm’s recycle bin. For example, if you run a **Not Overwrite** restore job with **Include Recycle Bin Data** enabled 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.
 - **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.
 - **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 [Recommendations for Using InstaMount](#) and [InstaMount Mapping and Restore Index](#) for more information.
 - **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 you are restoring to. For more information, refer to [About the Staging Policy](#).
 - **Workflow** – Decide how the backed-up SharePoint workflows are restored.

***Note:** Only SharePoint built-in workflows are supported in Platform Backup and Restore.

- **Include workflow definition** – Only restores the definition of the backed-up workflows.
 - **Include workflow instance** – Restore the state, history, and tasks for each item.
 - **Notification** – Configure the email **Notification** settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
8. When finished configuring Restore Settings, click **Next**. The **Schedule** page appears.
 9. **Schedule** – Choose whether or not to create the restore job on a schedule. If you decide to configure the schedule yourself, input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.
 10. When finished, click **Next**. The **Overview** page appears.
 11. Review and edit the job selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
 12. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Building an Out of Place Restore Plan at the Database Level

***Note:** If an existing Web application in the destination farm uses the same port as the one in the backup, and you want to use the backed-up Web application to overwrite the destination one, the existing destination Web application (together with the corresponding IIS Web site) must be deleted first prior to the restore. Otherwise, the backed up IIS site that serves the corresponding Web application cannot be restored.

To build and run an out of 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 the backed-up database.
3. **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 **Out of place restore** to restore the database to another SharePoint farm.
 - **Destination Farm** – Select the destination farm of the restore 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.
4. Click **Next**. The **Destination Component Options** page appears.

5. **Destination Component Options** – Specify the restore options for the destination component being restored.
 - **Detailed Information** – Display the detailed information of the database being restored, including its name and type. Click **Edit** in the **Details** column to edit the following properties.

***Note:** If you want to perform an out of place restore for a whole Web application/service application/service application proxy, the 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.
6. **Restore Settings** – Choose the detailed settings of 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.
7. 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.
 - Configure the email **Notification** settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient’s e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
8. When finished configuring Restore Settings, click **Next**. The **Schedule** page appears.
 9. **Schedule** – Choose whether or not to create the restore job on a schedule. If you decide to configure the schedule yourself, input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.
 10. When finished, click **Next**. The **Overview** page appears.
 11. Review and edit the job selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
 12. Click **Finish** to save the job’s configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job’s configuration without running it.

Building an Out of Place Platform Granular Restore Plan

To build and run an out of 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 to restore. Click **View Details** link on the top right corner of the **Backup Data** pane to view the detailed backup data for the selected database.
 - **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 restore the granular content. In addition, if you do not select this option when performing an **Overwrite** restore, the newly-added content in the original site collection might be lost. Refer to [Deselecting the Restore Granular Content Feature](#) for detailed information.
 - **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.

***Note:** This option can only be used when no manual/scheduled maintenance job is running on the backup data you are browsing.

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 original SQL Server which DocAve has backed up. If you want to change the location of the InstaMount temporary database, click the **Configure** link and you can select a staging policy for storing the InstaMount temporary database generated during the browsing. For more information, refer to [About the Staging Policy](#).

***Note:** If the granular restore index is not generated for the specified Platform Backup job, this option must be used when restoring the backup using Platform granular Restore.

3. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the **Item Browser** pane on the right.
 - **Container Configuration** – Specify the configuration of the container being restored.
 - **Security** – Refer to [Appendix B: SharePoint Objects Security and Property](#) for the detailed information related to security.
 - **Property** – Refer to [Appendix B: SharePoint Objects Security and Property](#) for the detailed information related to property.
4. When finished, click **Next**. The **Restore Type** page appears.
5. **Restore Type** – Choose where the content will be restored.
 - **Restore Type** – Select the location where to restore the backup data. In this case, select **Out of place restore** to restore the content to another SharePoint farm or a different location in the original farm.
 - **Destination** – Choose the destination of the restore job. You can either select an existing node on the tree or select a manually-created node. To create a node in the destination SharePoint manually, perform the steps below.
 - Select a node with a blank textbox.
 - Enter the URL of the destination node into the textbox following the format displayed in the textbox.
 - Click **Create Container** beside the textbox to create the node in the destination farm. Alternatively, click **Create Container** in the **Manage** group in the **Time-based Restore** tab to create the corresponding node.
 - **Agent Group** – Select the agent group to perform the restore job.
 - **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](#).
6. Click **Next** when finished. The **Restore Settings** page appears.

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

- **Restore Option** – Specify the action to be performed on conflicts when performing the Platform granular Restore. Items with the same item ID and files with the same file name in both the backup and the destination are considered conflicts by DocAve.
 - **Not Overwrite** – Ignore the backed-up file/item which has the same name/ID as the destination one. The item in the backup will not be restored.
 - **Overwrite** – Copies the backed up file/item to the destination location by overwriting the existing file/item that has the same name/ID.

***Note:** When performing the out of place Platform Restore job using the **Overwrite** option, the destination content type will be overwritten by the backed-up content type with the same name and ID. If the destination content type is in a site collection related with the corresponding **Managed Metadata service**, after the destination content type has been overwritten and published, all of the other site collections that used this content type will be affected.

- **Append** – For the folder/site/site collection level, the destination content is overwritten by the same content in the backup. For the item/item version level, a suffix (_1, _2, _3 ...) is added to the filename in the backup and it is restored to the destination. A backed-up item with a different **Modified Time** will be increased by 1 in the ID and restored to the destination with the same name. If the backed-up item has the same **Modified Time** as the destination item, the destination item is overwritten by the corresponding item in the backup. After the **Append** restore job, both the destination file/item and the restored file/item exist in the destination.
- **Replace** – The destination content is deleted and replaced with the same content in the backup. This option can only be used at folder/site/site collection level.
- **Include Recycle Bin Data** – Choose whether to compare the data in the backup with the data in the destination SharePoint farm's recycle bin. For example, if you run a **Not Overwrite** restore job with **Include Recycle Bin Data** enabled 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.
- **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.
- **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 [Recommendations for Using InstaMount](#) and [InstaMount Mapping and Restore Index](#) for more information.
- **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 you are restoring to. For more information, refer to [About the Staging Policy](#).

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

***Note:** Only SharePoint built-in workflows are supported in Platform Backup and Restore.

- **Include workflow definition** – Only restores the definition of the backed-up workflows.
 - **Include workflow instance** – Restore the state, history, and tasks for each item.
- **Notification** – Configure the email **Notification** settings. Using the drop-down boxes, select the type of report (**Summary** or **Detailed**), enter the recipient's e-mail address, and click **Add**. Repeat this procedure for any additional recipients.
8. When finished configuring Restore Settings, click **Next**. The **Schedule** page appears.
 9. **Schedule** – Choose whether or not to create the restore job on a schedule. If you decide to configure the schedule yourself, input a start time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.
 10. When finished, click **Next**. The **Overview** page appears.
 11. Review and edit the job selections. To make changes, click **Edit** in the middle of the row. This links to the corresponding setting page, allowing you to edit the configuration.
 12. Click **Finish** to save the job's configuration. If the restore job does not have a schedule, **Finish** runs the job immediately. If the restore job is set to run on a schedule, **Finish** saves the restore job's configuration without running it.

Restoring a Raw Database

This option must be used if you want 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**:

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.
 - **Database Name** – The database is 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 creates the path automatically during the restore job.

Deselecting the Restore Granular Content Feature

Deselecting the **Restore Granular Content** checkbox enables you to **not restore the granular content**.

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. This method can improve the restore speed.

For in place Platform granular Restore at the site collection level, deselect **Restore Granular Content** checkbox in the **Backup Data** pane to enable this restore method. If you do not select this option, the tree in the **Backup Data** pane can only be expanded down to the site collection level, so you cannot restore the granular content. In addition, if you do not select this option when performing an **Overwrite** restore, the newly-added content in the original site collection might be lost.

For out of place Platform granular Restore performed at the site collection level, deselecting the **Restore Granular Content** feature can be executed only when both of the following conditions are met:

- Only one site collection is selected on the backup data tree when selecting the scope of the restore job.
- There is not a site collection in the destination with the same ID as the site collection selected in the backup data.

Perform the steps below to enable this restore method:

1. Navigate to the default installation path of DocAve
Agent: ...*AvePoint\DocAve6\Agent\data\SP2010\Platform*.
2. Locate the **SP2010PlatformConfiguration.xml** file. Right-click the file and open it with Notepad.
3. Locate the **UseCopyTableOutOfPlaceRestore** attribute and change its value to **true**.

***Note:** The default value of this attribute is **false** and the **not restore the granular content** restore method is not enabled.

4. Uncheck the **Restore Granular Content** checkbox in the **Backup Data** pane and continue with building the plan as normal.

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 [Restore 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, including the settings and associated IIS sites. Content databases under the 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, it is deployed to the related Web applications with the same status that existed during backup. 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 by restoring those files. 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 back up and restore them.

***Note:** Front-end resources cannot be restored together with other farm components. They need to be restored separately after any other farm components are restored.


Selecting the Tree to Restore the Whole Site Collection








Select the tree as shown below to restore the whole site collection. Either of the following two selections can be used.

Selection 1


 http://vdi-ibtca-001:19001/sites/FB


Selection 2

 http://vdi-ibtca-001:19001/sites/FB

-  top-level site{sites/FB}
-  Lists
-  Sites
 -  Select All
 -  sites/FB/DB{sites/FB/DB}
 -  sites/FB/IB{sites/FB/IB}
 -  sites/FB/subsite 1{sites/FB/subsite 1}

If you select the tree as below, only the top-level site of the selected site collection will be restored.

 http://vdi-ibtca-001:19001/sites/FB

-  top-level site{sites/FB}

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.

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

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 Recovery 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 name(s) 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, Shared Services Providers for SharePoint 2007 or Shared Services Applications for 2010, Single Sign-On, etc.

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

Appendix A: 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	√	

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

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	Database(s) 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	√	x
State Service	StateService_Database(State Service Database Settings)	√	x
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_Reporting DB(Web Analytics Warehouse Database)	√	√
Word Automation Services(Word Conversion Service)	WordAutomationServices_Database(Microsoft.Office.Word.Server.Service.QueueDatabase)	√	√
Lotus Notes Connector	–	x	x
Usage and Health data collection	WSS_Logging	√	x

Word Viewing Service	-	x	x
PowerPoint Service Application	-	x	x
Project Service Application	-	v	x
SQL Server PowerPivot Service Application	-	x	x
Subscription Settings Service Application	Subscription Settings Database	v	v

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	√	×	
Central Admin Web Application	√	×	
Admin Content Database	√	×	
Web Application	√	√	
Content Database	√	√	
Global Search Settings	√	√	Farm-level search settings and Crawler impact rules are supported.
SharePoint Help Search	√	×	
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	√	√	<ul style="list-style-type: none"> • For in place restore, restoring the uploaded solution and its status in the Solution Management is supported. • For out of place restore, restoring the uploaded solution in the Solution Management is supported. Restoring the solution's status in the Solution Management is not supported.
FAST Search Server 2010 for SharePoint	√	×	<p>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:</p> <p>http://technet.microsoft.com/en-us/library/ff460221.aspx</p>
Knowledge Lake Imaging	√	×	
NewsGator	√	×	Only Social Site (NewsGator) 1.0 is supported in DocAve 6.0.
Nintex Workflow	√	×	
Farm Level Backup and Item Level Restore	√	√	<ul style="list-style-type: none"> • If you want to do Platform granular Restore, the Platform granular Restore index must be generated. • InstaMount function is supported.

Front-end Web 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 B: 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

Index

Backup Method, 19
Backup tab, 9
Browse the index in InstaMount, 38
Browse the stored index, 38
Copy data from snapshot to media server, 26
Copy snapshot data to media server for last ... backup(s), 21
Create, 12
Customize Database, 14
Data Compression, 19
Database Access Credentials, 12
Defer copying data from persistent snapshot, 26
Defer generating granular restore index, 26
Defer generating InstaMount mapping, 26
Destination Component Options, 36
Differential Backup, 20
Enable InstaMount Granular Restore, 20
Encryption, 19
Failover Database Server, 37
Form Mode, 27
Full Backup, 20
Generate granular restore index for last ... backup(s), 21
Generate InstaMount mapping for last ... backup(s), 21
In place restore, 30
Incremental Backup, 20
InstaMount Granular Restore, 29
Job Filter, 30
Maintenance Options, 21
Manage, 12
MaxSnapshotCount, 22
Minimum amount of free space to leave, 12
Out of place restore, 30
Parent Web Application URL, 37
Perform log backup after full backup, 18
Plan Builder, 18
Range of Recurrence, 26
Refresh, 13
Restore Database Only, 32
Restore Database to Most Recent State, 32
Restore Granularity Level, 26
Restore raw database, 32
Restore Raw Database, 41
Restore SharePoint farm components, 32
Schedule, 20
Snapshot Retention Policy, 20
SQL Agent Name and Instance Name, 12

Staging Policy, 12
Staging Policy Name, 12
Temp database file location, 12
Temp log file location, 12
Temporary Database Configuration, 12
The amount of snapshots you want to keep is ..., 25
Use DocAve Platform Recovery as the only backup method for SharePoint databases, 18
Use DocAve Platform Recovery in addition to other existing SQL backup methods for SharePoint databases, 19

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 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, 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