DocAve® 6 SQL Server Data Manager

User Guide

Service Pack 3, Cumulative Update 4

Revision D 3.4

Issued August 2014

Table of Contents

About DocAve SQL Server Data Manager

SQL Server Data Manager is a recovery solution for Microsoft SharePoint. DocAve provides full fidelity analysis and restore, from an individual item to an entire SharePoint environment with all of its farm-level components.

***Note**: SQL Server Data Manager supports SharePoint 2010 and 2013 on-premises.

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 SQL Server Data Manager:

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

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. You can Submit Your Feedback on our website.

Before You Begin

Refer to the sections for system and farm requirements that must be in place prior to installing and using DocAve SQL Server Data Manager.

Configuration

In order to use DocAve SQL Server Data Manager, the DocAve 6 platform must be installed and configured properly on your farm. SQL Server Data Manager 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. DocAve Agent must be installed on a SQL Server and at least one of the Web front-end servers.

For instructions on installing the DocAve Platform, DocAve Manager, and DocAve Agents, refer to the DocAve 6 Installation Guide.

Required Permissions

To install and use SQL Server Data Manager properly, ensure that the Agent account has the following permissions.

Agent accounts configured on the SharePoint servers where DocAve Agents are installed:

- SharePoint Permissions – This permission must be manually configured prior to using DocAve 6 SQL Server Data Manager; it is not automatically configured.
    - Member of the **Farm Administrators** group

  ***Note:** For SharePoint 2013, the SQL Server Data Manager requires the Agent account to have Full Control of all zones of the Web application.

  When restoring the backed up SharePoint 2013 personal site, the Agent account used to run the Restore job must also have the following permissions:

    - Full Control to the User Profile Service Application related to the Web application where the personal site resides
    - Security account of the application pool used by the Web application where the personal site resides

- SQL Permissions – These permissions must be manually configured prior to using DocAve 6 SQL Server Data Manager; they are not automatically configured.
    - Database Role of **db_owner** for all the databases related with SharePoint, including SharePoint Content Database, Configuration Database, and Central Administration Database
    - Server Role of **public** for the SQL Server
    - Database Role of **db_owner** for the temporary databases that store the analyzed data

Users who access the databases of the staging policy:

- SQL Permissions
    - Server Role of **processadmin** for the SQL Server
    - SQL Instance Permission: Control Server
    - Server Role of **dbcreator** for the SQL Server

Agent accounts configured on the SQL Servers where DocAve Agents are installed:

- Local System Permissions
    - Member of the **Administrators** group
- SQL Permissions
    - Database Role of **db_owner** for the temporary databases that store the analyzed data
    - Server Role of **public** for the SQL Server

Local System Permissions

The following Local System Permissions are automatically configured during DocAve 6 installation. The User must be 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** have the following permissions (the group is created by DocAve automatically):
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\DocAve6
    - Full Control to the Registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\eventlog
    - Full Control to the Communication Certificate

- Permission of **Log on as a batch job** (it can be found within **Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment**)
- Full Control Permission for DocAve Agent installation directory

Getting Started

Refer to the sections below for important information on getting started with SQL Server Data Manager.

Launching SQL Server Data Manager

To launch SQL Server Data Manager and access its functionality, complete the following steps:

1. Log in to DocAve. If you are already in the software, click the **DocAve** tab.
2. From the **DocAve** tab, click **Data Protection** to view the **Data Protection** modules.
3. Click **SQL Server Data Manager** to launch this module.

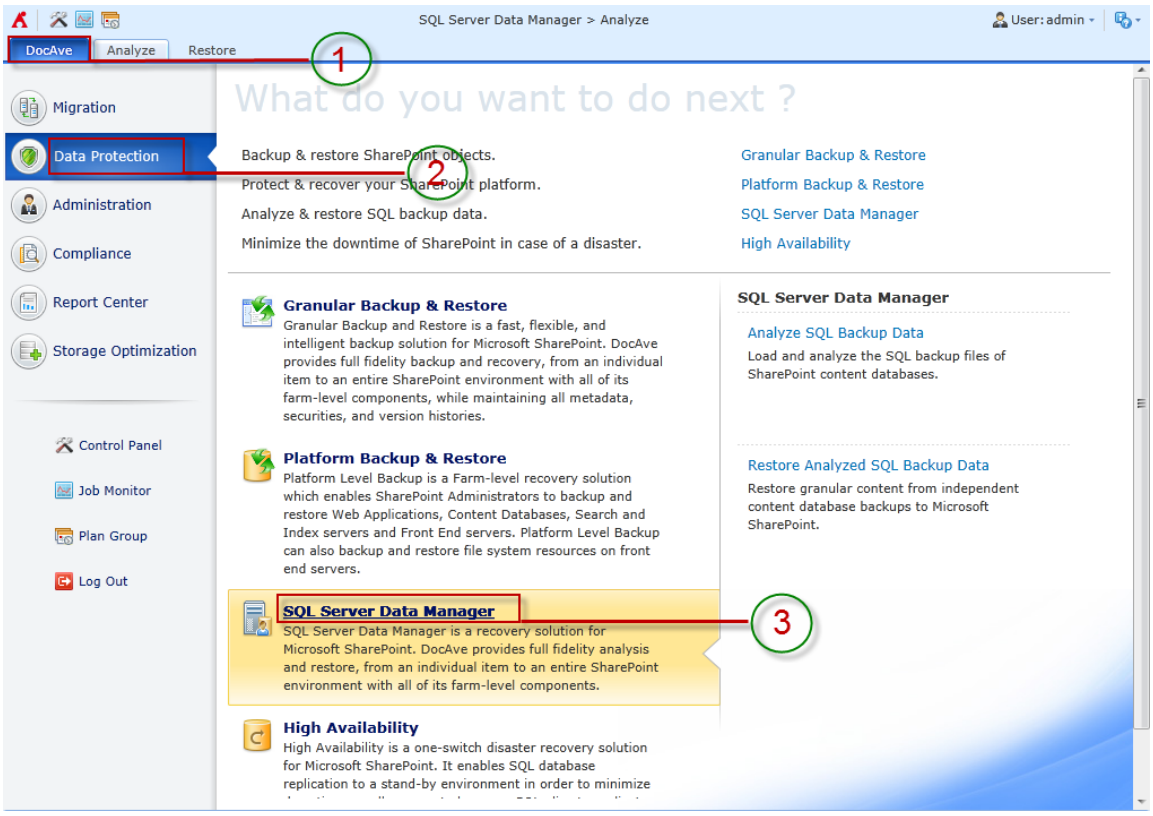

Figure 1: DocAve module launch window.

User Interface Overview

The SQL Server Data Manager interface launches with the **Analyze** tab active. This tab displays the dashboard and allows for quick access to a list of the SQL Server Data Manager features.

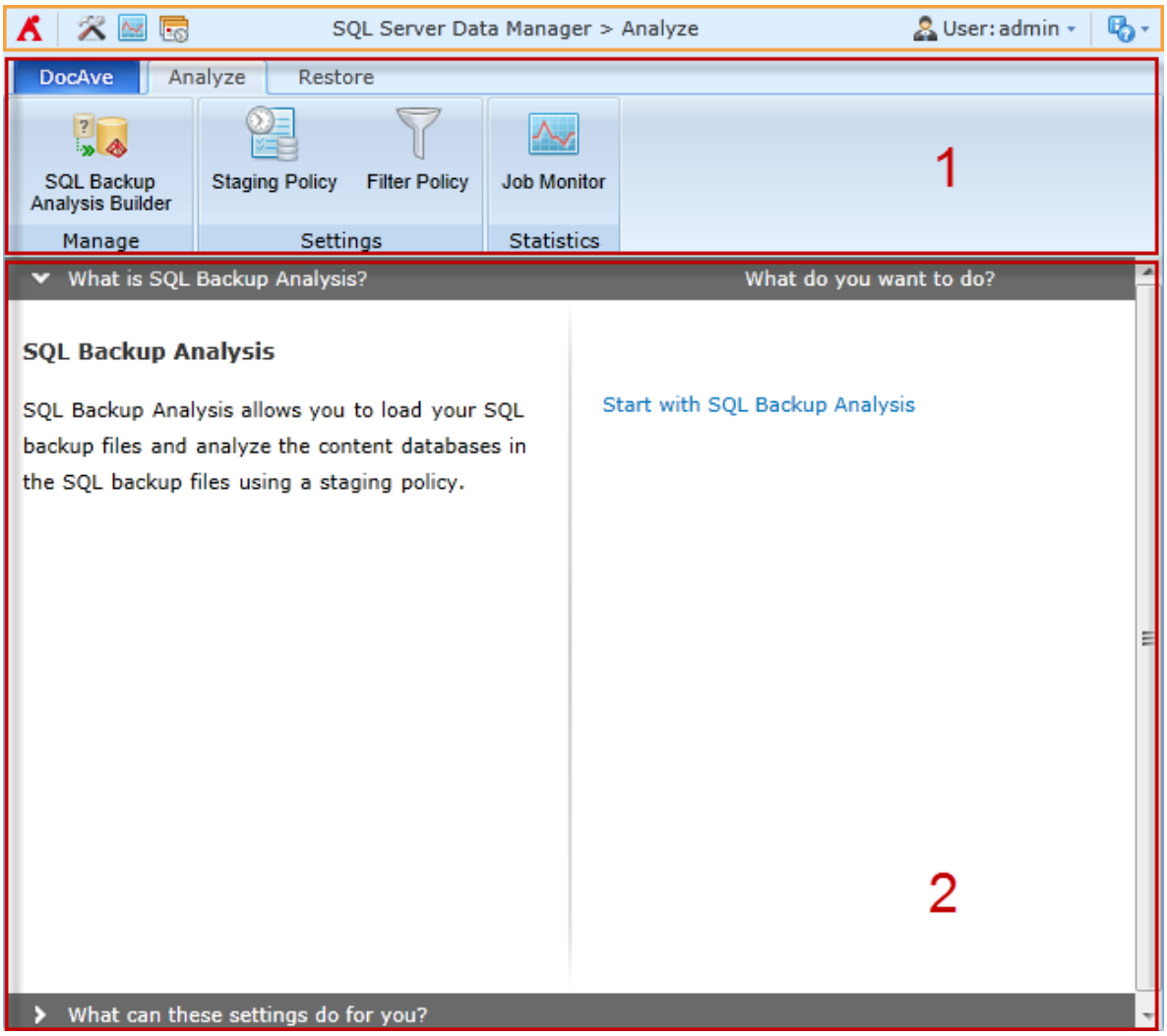

Figure 2: SQL Server Data Manager user interface.

1. The **ribbon** shows the available actions for SQL Server Data Manager.
2. The **workspace** shows explanations and the content that is used during the configuration of actions performed in DocAve products.

About the Staging Policy

The staging policy determines where temporary databases generated during the analysis process. Create a staging policy to specify a temporary database location and SQL backup files locations.

Staging Policy Configuration Interface

To access Staging Policy Configuration for DocAve in the SQL Server Data Manager interface, click **Staging Policy** in the **Settings** group on the **Analyze** tab. Click **Close** on the ribbon to close the **Staging Policy Configuration** interface.

In the **Staging Policy Configuration** interface, you will see a list of previously configured staging policies. You can customize how these staging policies are displayed in the following ways:

- **Search** – Filter the staging policies displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the staging policy you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (⊕) – Manage which columns are displayed in the list so that only the information you want to see is displayed. Click the manage columns buton (⊕), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Click the hide the column button (⊖) in the column title to hide the column.

Managing Staging Policies

In Staging Policy Configuration interface, you can create a new staging policy, edit a previously configured staging policy, or delete a previously configured staging policy. For details on creating or editing a staging policy, see the Configuring Staging Policies section of this guide.

Click **Edit** on the ribbon to change the configurations for this staging policy. For details on editing configurations for staging policy, see the Configuring Staging Policies section of this guide.

To delete a staging policy for DocAve, select it from the list of previously configured staging policies, and then click **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected staging policy, or click **Cancel** to return without deleting it.

Configuring Staging Policies

To configure a staging policy, complete the following steps:

1. Click **Staging Policy** in the **Settings** group on the **Analyze** tab. The **Staging Policy Configuration** window appears.
2. Click **Create** from the **Manage** group. The **Create a New Staging Policy** page appears. Configure the following settings:
    a. **Staging Policy Name** – Enter a staging policy name and optional **Description** for the staging policy.
    b. **Platform Type** – Describe the software platform that is going to use this staging policy.
    c. **Database Access Credentials** – Choose the SQL Server that you want to use for this staging policy and specify the credentials to access the specified SQL Server.
        - **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 of the instances in the SQL Agent selected above are listed in the drop-down box.
        - **Database Authentication (for accessing database within SharePoint)**
            - **Windows authentication (recommended)** (the default option) – Use this method to confirm the user identity using Windows.
            - **SQL authentication** – SQL Server confirms the user identity according to the entered **Account** and **Password**. The specified account must be added to the **sysadmin** role in SQL Server.

        Click **Validation Test** to verify the access to the SQL Server.
    d. **Temporary Database Configuration** – Set up the configuration of the temporary database.
        - **Minimum amount of free space to leave** – Specify the minimum amount of free space to leave for the database file location and log file location. DocAve ensures that the entered amount exists in the corresponding location before starting a job. If the free space specified here does not exist in the specified location before a job starts, or if the entered amount will not exist after the temporary database is stored to the specified location, then the corresponding job will fail.
        - **Temporary database file location** – Specify a local path on the SQL Server to store the temporary database data file (.mdf). The format of the path is **C:\data**. The default location is the database data default location of SQL Server, for example, *C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data*.

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

  Click **Validation Test** to verify the access to the SQL Server.

e. **SQL Backup Data Location** – Specify the location of the SQL backup files.

   Click **Specify Location** and the **Specify Location** interface appears. For more information, see the Configuring the Specify Location Interface section of this guide.

f. **Priority Settings** – Select the action when the number threshold of temporary databases has been met or exceeds.

   - **Fail Current Job** – The restore job of the backup files will fail immediately.
   - **Fail Other Jobs** – One database of the oldest staging jobs will be deleted before staging the new temporary database.

***Note**: Make sure the **xp_cmdshell** function is enabled in the SQL instance selected in the Staging Policy, or make sure the user that logs on the SQL instance service has the **Read** and **Write** permissions to the specified UNC path in the Staging Policy.

Configuring the Specify Location Interface

Click **Specify Location** on the **Staging Policy Configuration** window in the **SQL Backup Data Location** field and the **Specify Location** interface appears. To specify the **Source Path** of the SQL backup files, configure the following settings:

1. Enter the **UNC Path**.
2. Enter the **Username**.
3. Enter the **Password**.
4. Click **Validation Test** to verify the access to the server.
5. Click **OK**.

About the Filter Policy

Filter Policy allows you to set up filter rules so you can control what objects and data within any file system level appear so that you can target content more precisely. By setting up and saving filter policies, you can apply the same filter policies to different plans without having to recreate them each time.

To access Filter Policy Configuration for DocAve in the **SQL Server Data Manager** interface, click **Filter Policy** in the **Settings** group on the **Analyze** tab. Click **Close** on the ribbon to close the **Filter Policy Configuration** interface.

In the **Filter Policy Configuration** interface, you will see a list of previously configured filter policies. You can customize how these filter policies are displayed in the following ways:

- **Search** – Filter the filter policies displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the filter policy you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** ( ) – Manage which columns are displayed in the list so that only the information you want to see is displayed. Click , and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** ( ) – Click in the column title to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Click the icon of the column you want to filter, and then check the checkbox next to the item name to have that item shown in the list. To remove all filters, click **Clear Filter**.

Managing Filter Policies

In the **Filter Policy Configuration** interface, you can create a new filter policy, view details about a filter policy, edit a previously configured filter policy, or delete a previously configured filter policy. For details on creating or editing a filter policy, see the Configuring Filter Policies section of this guide.

Click **Edit** on the ribbon to change the configurations for this filter policy. For details on editing configurations for filter policy, see the Configuring Filter Policies section of this guide.

To view a filter policy for DocAve, select it from the list of previously configured filter policies, and then click **View Details** on the ribbon. To delete a filter policy for DocAve, select it from the list of previously configured filter policies, and then click **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Click **OK** to delete the selected filter policy, or click **Cancel** to return without deleting it.

Configuring Filter Policies

To create a new filter policy, click **Create** from the **Manage** group. To modify a previously configured filter policy, select the filter policy, then click **Edit** on the ribbon. In the **Create Filter Policy** or **Edit Filter Policy** interface, configure the following settings:

1. **Name** and **Description** – Enter a **Name** for the filter policy. Then enter an optional **Description** for future reference.

2. **Criteria** – Select specific objects or data within each file system level (file and folder). Each level has a unique set of rules that can be applied to enhance configurations.

   ***Note:** Refer to Appendix C – Examples of Filter Policies for examples of filter policies that users can configure.

   a. Click **Add a Filter Level Group** to add a new rule of the specified level and then click **Add a Criterion** to add criteria for the new rule by completing the fields below, and click  to delete the rule that is no longer needed.

      - **Rule** – Select the new rule you want to create from the drop-down list.
      - **Condition** – Select the condition for the rule.
      - **Value** – Enter a value you want the rule to use in the text box.

   b. To add more filters to the filter policy, repeat the previous step.

      ***Note:** Depending on the filters you enter, you can change the logical relationships between the filter rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to **And**. To change the logical relationship, click on the logical relationship link. The **And** logical relationship means that the content which meets all the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

3. **Basic Filter Condition** – View the logical relationship of the filter rules in this area.

   For example, if the logical relationship is ((1 And 2) Or 3) in the Basic Filter Condition area, the contents that meet both the filter rule 1 and filter rule 2, or meet the filter rule 3, will be filtered out.

4. Click Save to save the configurations and return to the **Filter Policy** interface, or click **Cancel** to return to the **Filter Policy** interface without saving any changes.

SQL Backup Analysis Builder

Click **SQL Backup Analysis Builder** from the **Manage** group. The wizard mode page appears. Configure the following settings:

1. **Analysis Options** – Choose a staging policy, a filter policy, and a method of analysis for the job you are about to run.
    - **Staging Policy** – Determines where temporary databases generated during the analysis process. Create a staging policy to specify a temporary database location and SQL backup files locations. You may select a previously-created staging policy from the drop-down menu, or click **New Staging Policy** from the drop-down menu to create a new one. For detailed information, refer to Configuring Staging Policies.
    - **Filter Policy** – Controls what objects and data within any file system level are analyzed so that you can target content more precisely. The default filter policy is set to be none. You may select a previously-created filter policy from the drop-down menu, or click **New Filter Policy** from the drop-down menu to create a new one. For detailed information on configuring a filter policy, refer to Configuring Filter Policies.
    - **Use InstaMount for Analysis** – Select **Yes** or **No** for whether or not to use InstaMount when analyzing the SQL backups of the content databases. InstaMount makes item-level restore more efficient, as it uses a mapping file to record the relationship between the InstaMount temporary database and the backup data. Note that the user of InstaMount requires minimal disk space. Refer to About InstaMount for more information.
2. **Data Selection** – Select the SQL backup files that you want to restore data from.
    a. Click **Find SQL Backup Files** on the left pane of the interface, the **Find SQL Backup Files** window pops up.
    b. In the left pane of the pop-up window, click the SQL instance to load the tree structure.
    c. Click the node in the tree to load the corresponding backup files in the right pane of the pop-up window.
    d. Select the backup files that you want to analyze by selecting the corresponding checkboxes.
    e. Click **OK** to save the selection.
    f. In the **Analyze** tab, the paths of the selected backup files are available. Select one backup file at a time, and click it to load the corresponding content databases of the backup file.
    g. Select content databases to analyze by selecting the checkbox.
3. **Schedule** – Configure a schedule for this job.
    - **Notification** – To inform specified users of the Backup Files Analysis job, configure the **Notification** settings. Select a previously-configured notification profile from the **Select**

a profile with address only drop-down list, or choose to create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.

- **Schedule Selection** – Choose whether to run the job immediately, or configure a custom start time.
    - **No schedule** – Select this option to run the job immediately when you finish the settings of this job.
    - **Configure the schedule myself** – Select this option and the **Schedule Settings** section appears under the **Schedule Selection** section.
- **Schedule Settings** – Specify a start date and time to run this job.
- **Description** – Enter an optional description for this job.

4. **Overview** – Review and edit your configurations for this job.
5. Click **Finish** to run this job immediately or running this job at the time specified in the **Schedule Settings** section.

About InstaMount

It is recommended that you enable the InstaMount function to restore items that are small in file size. The InstaMount function can be enabled in an analysis job. The InstaMount mapping file is generated from backup data; it is used to generate the temporary files used by the InstaMount function.

Restore Analyzed SQL Backup Data

To run a Restore Analyzed SQL Backup job, complete the following steps:

1. Select the **Restore** tab and click **Restore** in the **Manage** group. The **Restore Analyzed SQL Backup Data** tab appears.
2. **Job Selection** – Configure the options in the **Filter By** area to limit the scope of backup data. The default filter rule is to filter the analysis jobs in the last seven days.
    - **Time Range** – Filter backup data by completion time range using the drop-down list.
        - **All jobs** – Select this option to display all Finished/Finished with Exception Backup Files Analysis jobs.
        - **Analysis jobs start within** – Select this option to specify a time period. All of the Finished/Finished with Exception Backup Files Analysis jobs whose start time is in the specified time period are displayed.
3. After **selecting** the filters, click the **Filter** button in the **Filter By** area or on the ribbon. All analysis jobs that meet the selected filter rules are listed in the calendar. If desired, click **Reset** in the **Filter By** area or click **Reset** on the ribbon to clear all filters and display all Finished/Finished with Exception analysis jobs.
4. Select the analysis job that you want to restore by clicking the job. Additional actions that can be performed:
    - Place the mouse cursor over an analysis job to display job information such as the Job ID, InstaMount Enabled, and Job Status. Click **Day**, **Week**, or **Month** to change the view to see all the available jobs during that time period.
    - Click the page turn button () on the top-left corner of the calendar to turn the page.
5. Now that you've selected an analysis job containing data you want to restore, click **Next** to continue with instructions on building the job:

Configuring a Restore Job

To configure a restore job, complete the following steps:

1. Refer to Restore Analyzed SQL Backup Data to begin building the job.
2. **Data Selection** – Select the database that includes the granular content to restore.
3. Click the **Global Setting for Restoring Content, Property and Security** link and configure the **Item Level Settings**:
    a. **Granular Content** – Select the **Restore granular content** checkbox to restore the granular content. If you do not select this checkbox, the tree in the **Backup Data** pane can only be expanded down to the site collection level and you cannot select granular content. Refer to Site Collection Level Restore for detailed information.
        - **Container Selection** – Select the **Global setting for container configuration** checkbox to enable the container's global settings.
            - **Restore container** – Restore the container and select the **Security** checkbox if you want to restore the container's security settings, and/or select the **Property** checkbox if you want to restore the container's property settings. For more information, refer to Appendix B – SharePoint Object Security and Property.
            - **Only restore security –** Only restore the container's security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security of the container in the backup to the conflict container in the destination. **Replace** will delete the security of the conflict container in the destination first, and then add the security of the container in the backup to the conflict container in the destination.

              ***Note**: Once you select **Only restore security** option, the **Container level conflict resolution** configuration field in the **Restore Settings** page will be hidden from the interface and you will not be able to configure the **Container level conflict resolution** though that page.
        - **Content Selection** – Select the **Global setting for restoring content** checkbox to enable the content's global settings.
            - **Restore content** – Restore the content. Additionally, select the **Security** checkbox if you want to restore the content's security settings along with. For more information, refer to Appendix B – SharePoint Object Security and Property.
            - **Only restore security** – Only restore the content's security settings. You can specify the **Conflict resolution** as **Merge** or **Replace**. **Merge** will add the security settings of the content in the backup into the conflict content in the destination. **Replace** will delete the security settings of the conflict content in the destination first, and then add the security of the content in the backup to the conflict content in the destination.

***Note**: Once you select **Only restore security** option, the **Content level conflict resolution** configuration field in the **Restore Settings** page will be hidden from the interface and you will not be able to configure the Content level conflict resolution though that page.

4. Expand the tree and locate the content you want to restore. The detailed information can be viewed in the **Item Browser** pop-up window. Select the objects to be restored under this node.

   When finished, click **Next**. The **Destination Settings** page appears.

5. **Destination Settings** – Choose a destination to restore the data, specify an agent to perform the restore job, select an action of how the data is restored, and configure the mapping settings to update the metadata, securities, and language while storing to an alternate location.

   ***Note:** It is not supported to restore the data backed up from SharePoint 2010 to SharePoint 2013 or to restore the data backed up from SharePoint 2013 to SharePoint 2010. Make sure that the source node and the destination node are in the same version of SharePoint. If the site within SharePoint 2013 is a SharePoint 2010 mode site, it can only be restored to the same mode site.

   a. **Destination** – Choose the destination for the restore job. You can either select an existing node on the tree or select a manually-created node. To create a node in the destination SharePoint manually, select a node with a blank text box, and then enter the URL of the destination node into the text box following the format displayed in the text box. If you are creating a new site collection, you will be asked to select one existing managed path from the drop-down list. Click **Create Container** beside the text box to create the node in the destination farm. Alternatively, click **Create Container** in the **Manage** group on the **Restore Analyzed SQL Backup Data** tab to create the corresponding node.

   b. **Agent** – Specify the Agent that will perform the restore job.

   c. **Action** – Select how the SQL backup data will be restored to the destination.

      - **Merge** – Add the backup data to the destination node.
      - **Attach** – Restore the backup data as children beneath the selected node.

   d. **Mapping Settings** (Optional) **–** Configure whether to specify the mapping settings to map the user, domain, or language to the destination.

      - **User mapping** – If desired, configure the user mapping to map the backed up user to the destination user. For specific instructions on setting up the user mapping, refer to the DocAve 6 Control Panel Reference Guide.
      - **Domain mapping** – If desired, configure the domain mapping to map the backed up domain to the destination domain. For specific instructions on setting up the domain mapping, refer to the DocAve 6 Control Panel Reference Guide.
      - **Language mapping** – If desired, configure the language mapping to display a destination node in a different language than the language of the backed-up

data. For specific instructions on setting up the language mapping, refer to the DocAve 6 Control Panel Reference Guide.

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

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

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

        - **Content level conflict resolution** – Sets the conflict resolution on the item level.
            - **Skip** – Ignores the source item/document that has the same item ID/document name as the destination item/document. l
            - **Overwrite** – Copies the source item/document to the destination by overwriting the destination item/document with same item ID/document name.
            - **Overwrite by Last Modified Time** – Keeps the conflict item\document which has the latest modified time and overwrites the older one.
            - **Append an Item/Document Name with a Suffix** – Keeps both of the conflict items/documents and add a suffix (_1, _2, _3…) to the name of the conflict source item/document.
            - **Append a New Version** – Adds the conflict source item/document to the destination as a new version of the conflict destination item/document.
    b. **Include Data in Recycle Bin** – Choose whether to compare the data in the backup with the data in the destination SharePoint farm's recycle bin. If you select **Skip** either at the Container level or Content level, or select **Append an Item/Document Name with a suffix** or **Append a New Version** in Content level, the **Include Recycle Bin Data** option is

available to configure. If you select **Yes** in this field, and the selected content in the backup still exists in the recycle bin of the destination SharePoint farm, then the selected content in the backup is not restored.

c. **Include Detailed Job Report for All Items** – Selecting **Yes** generates a detailed job report for all the items. Selecting **No** still generates a job report for list, site, or site collection level.

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

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

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

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

   ***Note:** If the dependent column or content type does not exist in the destination, then that column or content type will not be restored. If this is the case, use this option to restore them.

   - **Restore the item-dependent columns and content types to maintain item integrity** – Whether the item is restored and the dependent column or content type is created in the corresponding list/library are depended on the option selected below:
     - **Do not restore the columns and content types, or the corresponding items** – The columns, content types, and the corresponding items will not be restored if the columns and content types in the destination are conflicted with the backed up columns and content types.
     - **Overwrite the columns and content types** – The columns and content types will overwrite the destination conflicted columns and content types, and the corresponding items will be restored.
     - **Append the columns to the destination** – The columns and items will be restored to the destination if the columns and content types in the destination are conflicted with the backup up columns and content types.
   - **Do not restore item-dependent columns and content types** – The item dependent columns and dependent content types will not be restored. When selecting this option, make sure the dependent columns and content types exist in the destination. Otherwise, the item cannot be restored.

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

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

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

h. **Notification** – Configure the email **Notification** settings. Select a previously-configured notification profile from the **Select a profile with address only** drop-down list. You can also choose to create a new e-mail notification profile by clicking the **New Notification Profile** link. Click **View** to view the detailed configuration of the selected notification profile.

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

7. **Schedule** – Choose **whether** or not to create the restore job based on a schedule. Select **Restore at the end of the wizard** to run the job immediately after finishing the restore wizard. To configure the schedule yourself, select **Configure the schedule myself** and select a start date and time in **Schedule Settings** field. If desired, enter an optional **Description** to distinguish the restore job from others.

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

8. 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.

9. 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.

Site Collection Level Restore

Deselecting the **Restore Granular Content** checkbox disables granular content selection. This restore method can only be used for a granular restore that is performed at the site collection level. If the whole site collection needs to be restored, enable the Site Collection Level Restore feature by deselecting the **Restore Granular Content** checkbox. In this case, the restore will be similar to an STSADM site collection level restore. It is faster and can maintain internal document IDs. The restored data and its data structure are much closer to the original data and structure.

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

For a granular restore performed at the site collection level, deselecting the **Restore Granular Content** feature can be executed only when no site collection in the destination has the same URL or ID as the site collection selected in the backup data.

Checking a Job Status

SQL Server Data Manager 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.

Appendix A – Accessing Hot Key Mode

In order to work faster and improve your productivity, DocAve supports hot key mode for you to perform corresponding actions quickly by only using your keyboard. To access hot key mode from the SQL Server Data Manager interface, press the key combination of **Ctrl** +**Alt** + **Z** on your keyboard.

The following table provides a list of hot keys for the Analyze page of the SQL Server Data Manager interface. Each time you want to go back to the Home page, press **Ctrl** + **Alt** + **Z** on your keyboard. For example, continue pressing **A** to go back to the **Analyze** tab of SQL Server Data Manager.

Operation Interface	Hot Key
Analyze	A
Restore	R
DocAve Home Page	1
DocAve Online Community	2
Control Panel	3
Job Monitor	4
Plan Group	5
Account Information	9
Help and About	0

Analyze Tab

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

Operation Interface	Hot Key		
Analyze SQL Backup Builder	A	Staging Policy	S
		Filter Policy	F
		Back	B
		Next	N
		Finish	FN
		Cancel	C
Staging Policy	S		
Filter Policy	F		
Job Monitor	J		

Staging Policy Configuration Interface

The following is a list of hot keys for the Staging Policy Configuration interface functions.

Operation Interface	Hot Key		
Create	C	Save	O
		Cancel	B
Edit	E	Save	O
		Cancel	B

Operation Interface	Hot Key
Delete	D
Close	X

Filter Policy Configuration Interface

The following is a list of hot keys for the Filter Policy Configuration interface functions.

Operation Interface	Hot Key		
Create	C	Save	O
		Cancel	C
View Details	V	Edit	E
		Cancel	C
Edit	E	Save	O
		Cancel	C
Delete	D		
Close	X		

Restore Tab

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

Operation Interface	Hot Key		
Restore	R	Create Container	CC
		Advanced Search	AS
		Filter	FL
		Reset	R
		Back	B
		Next	N
		Finish	FN
		Cancel	CX
Job Monitor	J		

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 Belonging to the Specified Type
Security	Site Collection	Users and groups of the site collection
	Site	Mappings of the users and their permissions, permission levels, groups, users
	List	Mappings of the users and their permissions, users, groups
	Folder/Item/File	Mappings of the users and their permissions, users, groups
Property	Site Collection	Basic information used to create the site collection, other information of the site collection, site features
	Site	Basic information used to create the site, other information of the site, site columns, site content types, navigation, site features, triggers for the users' actions in the site
	List	Basic information used to create the List, other information of the list, list columns, list content types, triggers for the users' actions in the list, alert
	Folder/Item/File	Properties of the folder/item/file, alert

Appendix C – Examples of Filter Policies

***Note**: The **Equals** condition is not case sensitive.

Hierarchy Level	Rule	Condition	Value	Result
File	Name	Contains	test	The file whose name contains *test* will be filtered and included in the results.
		Does Not Contain	test	The file whose name does not contain *test* will be filtered and included in the results.
		Equals	test	The file whose name is *test* will be filtered and included in the results.
		Does Not Equal	test	The file whose name is not *test* will be filtered and included in the results.
		Matches	te*t	The file whose name begins with *te* and ends with *t* will be filtered and included in the results. For example, teABct will be filtered and included in the results.
			te?t	The file whose name is the same as *te?t* except character **?** will be filtered and included in the results. For example, test will be filtered and included in the results.
		Does Not Match	te*t	All the files except those whose names begin with *te* and end with *t* will be filtered and included in the results. For example, DocAve will be filtered and included in the results.
			te?t	All the files except those whose names are the same as *te?t* except character **?** will be filtered and included in the results. For example, DocAve will be filtered and included in the results.

Hierarchy Level	Rule	Condition	Value	Result
	Size	>=	1MB	The file whose size is not smaller than 1MB will be filtered and included in the result. For example, a 2MB file will be filtered and included in the result.
		<=	1MB	The file whose size is not bigger than 5 will be filtered and included in the result. For example, a 500KB file will be filtered and included in the result.
	Modified Time	Before	2011-11-11 12:15:50	The file which is modified before *12:15:50 11/11/2011* will be filtered and included in the result.
		After	2011-11-11 12:15:50	The file which is modified after *12:15:50 11/11/2011* will be filtered and included in the result.
		On	2011-11-11 12:15:50	The file which is modified on *12:15:50 11/11/2011* will be filtered and included in the result.
		Within	5 Days	The file which is modified in last *5 days* will be filtered and included in the result.
		Older Than	5 Days	The file which is modified *5 days* ago will be filtered and included in the result.
	Created Time	Before	2011-11-11 12:15:50	The file which is created before *12:15:50 11/11/2011* will be filtered and included in the result.
		After	2011-11-11 12:15:50	The file which is created after *12:15:50 11/11/2011* will be filtered and included in the result.
		On	2011-11-11 12:15:50	The file which is created on *12:15:50 11/11/2011* will be filtered and included in the result.

Hierarchy Level	Rule	Condition	Value	Result
		Within	5 Days	The file which is created in last *5 days* will be filtered and included in the result.
		Older Than	5 Days	The file which is created *5 days* ago will be filtered and included in the result.
	Last Accessed Time	Before	2011-11-11 12:15:50	The file whose last accessed time is before *12:15:50 11/11/2011* will be filtered and included in the result.
		After	2011-11-11 12:15:50	The file whose last accessed time is after *12:15:50 11/11/2011* will be filtered and included in the result.
		On	2011-11-11 12:15:50	The file whose last accessed time is on *12:15:50 11/11/2011* will be filtered and included in the result.
		Within	5 Days	The file whose last accessed time is in last *5 days* will be filtered and included in the result.
		Older Than	5 Days	The file whose last accessed time is *5 days* ago will be filtered and included in the result.
Folder	Name	Contains	test	The folder whose name contains test will be filtered and included in the results.
		Does Not Contain	test	The folder whose name does not contain test will be filtered and included in the results.
		Equals	test	The folder whose name is test will be filtered and included in the results.
		Does Not Equal	test	The folder whose name is not test will be filtered and included in the results.

Hierarchy Level	Rule	Condition	Value	Result
		Matches	te*t	The folder whose name begins with te and ends with t will be filtered and included in the results. For example, teABct will be filtered and included in the results.
			te?t	The folder whose name is the same as te?t except character ? will be filtered and included in the results. For example, test will be filtered and included in the results.
		Does Not Match	te*t	All the folders except those whose names begin with te and end with t will be filtered and included in the results. For example, DocAve will be filtered and included in the results.
			te?t	All the folders except those whose names are the same as te?t except character ? will be filtered and included in the results. For example, DocAve will be filtered and included in the results.
	Modified Time	Before	2011-11-11 12:15:50	The folder which is modified before 12:15:50 11/11/2011 will be filtered and included in the result.
		After	2011-11-11 12:15:50	The folder which is modified after 12:15:50 11/11/2011 will be filtered and included in the result.
		On	2011-11-11 12:15:50	The folder which is modified on 12:15:50 11/11/2011 will be filtered and included in the result.
		Within	5 Days	The folder which is modified in last 5 days will be filtered and included in the result.

Hierarchy Level	Rule	Condition	Value	Result
		Older Than	5 Days	The folder which is modified 5 days ago will be filtered and included in the result.
	Created Time	Before	2011-11-11 12:15:50	The folder which is created before 12:15:50 11/11/2011 will be filtered and included in the result.
		After	2011-11-11 12:15:50	The folder which is created after 12:15:50 11/11/2011 will be filtered and included in the result.
		On	2011-11-11 12:15:50	The folder which is created on 12:15:50 11/11/2011 will be filtered and included in the result.
		Within	5 Days	The folder which is created in last 5 days will be filtered and included in the result.
		Older Than	5 Days	The folder which is created 5 days ago will be filtered and included in the result.
	Last Accessed Time	Before	2011-11-11 12:15:50	The folder whose last accessed time is before 12:15:50 11/11/2011 will be filtered and included in the result.
		After	2011-11-11 12:15:50	The folder whose last accessed time is after 12:15:50 11/11/2011 will be filtered and included in the result.
		On	2011-11-11 12:15:50	The folder whose last accessed time is on 12:15:50 11/11/2011 will be filtered and included in the result.
		Within	5 Days	The folder whose last accessed time is in last 5 days will be filtered and included in the result.
		Older Than	5 Days	The folder whose last accessed time is 5 days ago will be filtered and included in the result.

Appendix D – Advanced Settings in Configuration Files

Configure the **SP2010PlatformConfiguration.xml** file to specify the maximum number of the temporary databases can be created and specify the Web application URL for the backup data analysis.

1. Go to the machines with DocAve Agent installed and open the *…\AvePoint\DocAve6\Agent\data\SP2010\Platform* directory to find the **SP2010PlatformConfiguration.xml** file.
2. Open the **SP2010PlatformConfiguration.xml** file with Notepad.
3. Find the **</SDMConfig>** node.

   For detailed information, refer to the screen shot below:

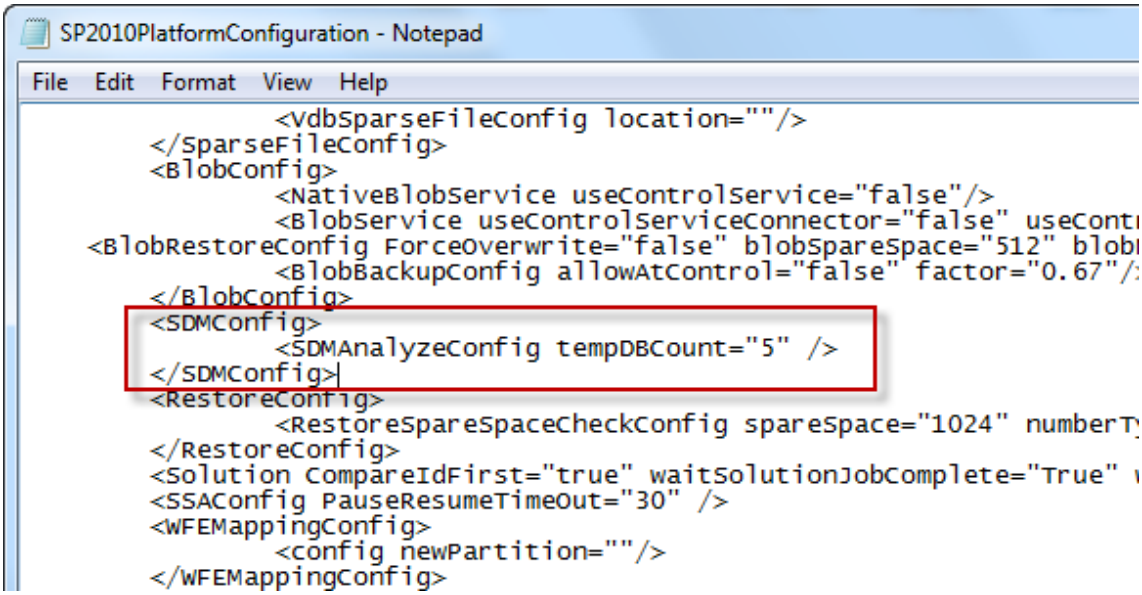

Figure 3: Finding the </SDMConfig> node in the SP2010PlatformConfiguration.xml file.

<SDMAnalyzeConfig tempDBCount=" " /> – Specify the maximum number of temporary databases. The default value is **5**. When the number of temporary databases is larger than **5**, the action will be taken according to the settings in the **Priority Settings** section. For more information on Priority Settings section, see the Configuring Staging Policies section of this guide.

4. Find the **<PlatformItemRestore ContentTypeFieldLinksOption="merge" >** node, and insert the parameter **SDMSourceWebAppUrl=" "** to this node.

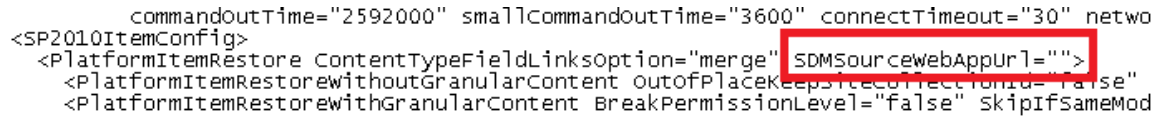

Figure 4: Inserting the SDMSourceWebAppUrl parameter.

5. Enter the desired Web application URL.

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

Trademarks

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

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