Setting up Windows WebDav Server for Private Cloud Backups with BackupAssist

With the release of BackupAssist v 10.3 we have added support for WebDav. This opens up a wide variety of backup destinations including Windows machines, NAS devices, and third-party hosting companies.

What is WebDAV?

WebDAV (Web-based Distributed Authoring and Versioning) is an extension of the HTTP/S protocol that allows clients to perform remote Web content authoring operations. For backups, this means it can be used to transfer data from BackupAssist to a remote server or device.

Advantages over Rsync

Why should I use WebDAV over Rsync? Using the WebDav vs the Rsync protocol results in some major improvements.

- **Ability to Resume Backup**
  Cloud Backup backs up files in chunks and keeps track of what files have been sent to the cloud destination. This means if the backup job stops or is interrupted, for example due to a network or internet outage, the backup job can resume and does not need to restart.
- **Easier to Support and Configure**
  WebDav is a common HTTP/S extension protocol that is widely available and easy to configure.(WebDAV is built into Windows and almost all NAS devices)
- **Reduced Storage Requirement** and Destination System Resources
  Deduplication on all data shrinks backups significantly 2:1 or better compression
- **Large file support** - ideal for Hyper-V guests and Exchange databases
- **Speed** - full backups are 2x and 20x faster (normal and encrypted respectively)
- No processing power is needed on the destination - it's just a file store
- **Minimal overhead** for encryption on the client, none on the destination
- **Flexible seeding** - option to use a separate portable seeding disk
- It's FREE!- if you own an existing rsync license and have upgrade cover

Want to get started?

Continue reading for instructions on how to set up your Windows system to become the WebDav destination for your backups.

Step 1 - IIS Installation

The first thing to do is enable Internet Information Server (IIS) on your Windows Server. This will allow you to run the WebDAV extension for HTTP.

1. Run the server's **Add Roles and Features** Wizard.

2. Select the **Server Roles** tab

3. Check the **Web Server (IIS)** box.

4. Expand **Web Server Role (IIS)** > **Web Server** > **Common HTTP Features**. Make sure that **WebDAV Publishing** is checked.

5. Expand **Web Server Role (IIS)** > **Web Server** > **Security**. Make sure that **Windows Authentication** is checked.

6. Expand **WebServer (IIS)** > **Web Server** > **Performance**. Check **Dynamic Content Compression.**
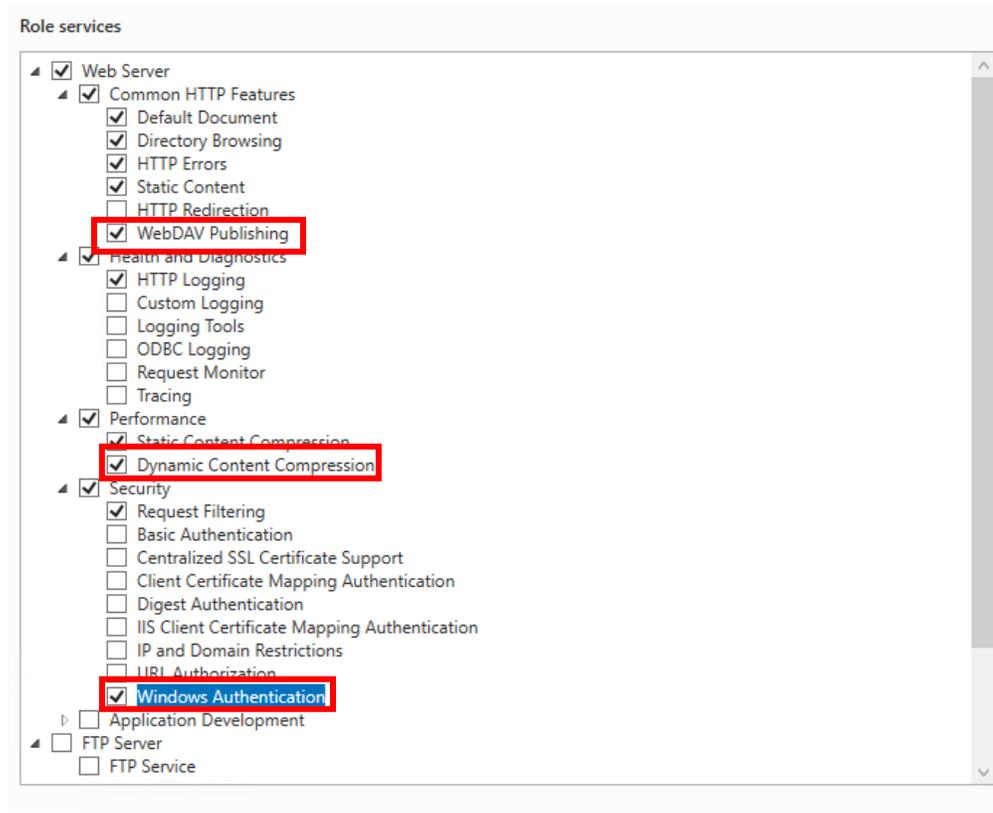
7. Complete the wizard steps by clicking **Next**.

Note: If you are using Windows Workstation then follow the same steps in **Turn Windows features on or off**. And you can find all options under **Internet Information Services** followed by **World Wide Web Services.**
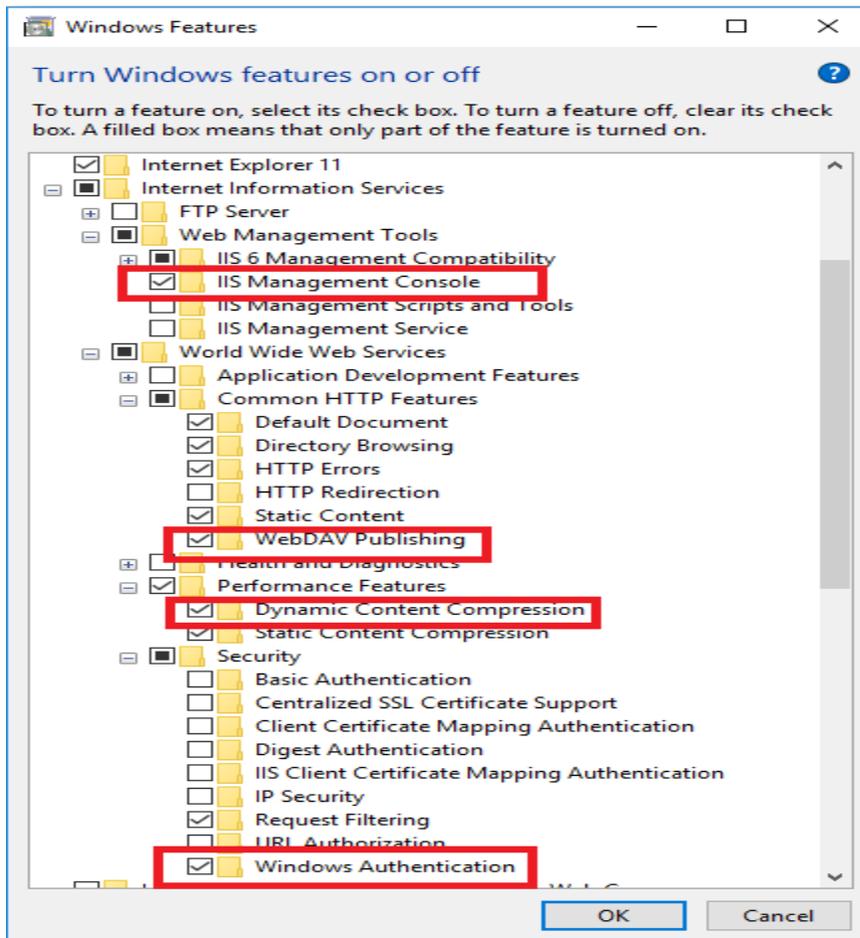

Step 2 - IIS Configuration

Next you need to configure WebDAV on IIS and assign the required permissions and access.

1. Open IIS Manager from the Server Manager Menu

2. Go to <server name> Sites > Default Web Site. In the example below, the <server name> is ROBOBAK

3. Double-Click **WebDAV Authoring Rules.**

4. In the **Actions** pane on the right, click **Enable WebDAV**. When you do this, the **Add Authoring Rule…** option will appear in the **Actions** Pane.

5. In the **Actions** pane on the right, click **Add Authoring Rule...**

6. Grant **Read and Write** permissions to the appropriate group according to your usage scenarios and security requirements. For example, to grant every user permission to back up to this server, in the **Add/Edit Authoring Rule** dialog select the options **All content**, **All users,** and the **Permissions**: **Read**, **Source**, **Write**. Press **OK**.
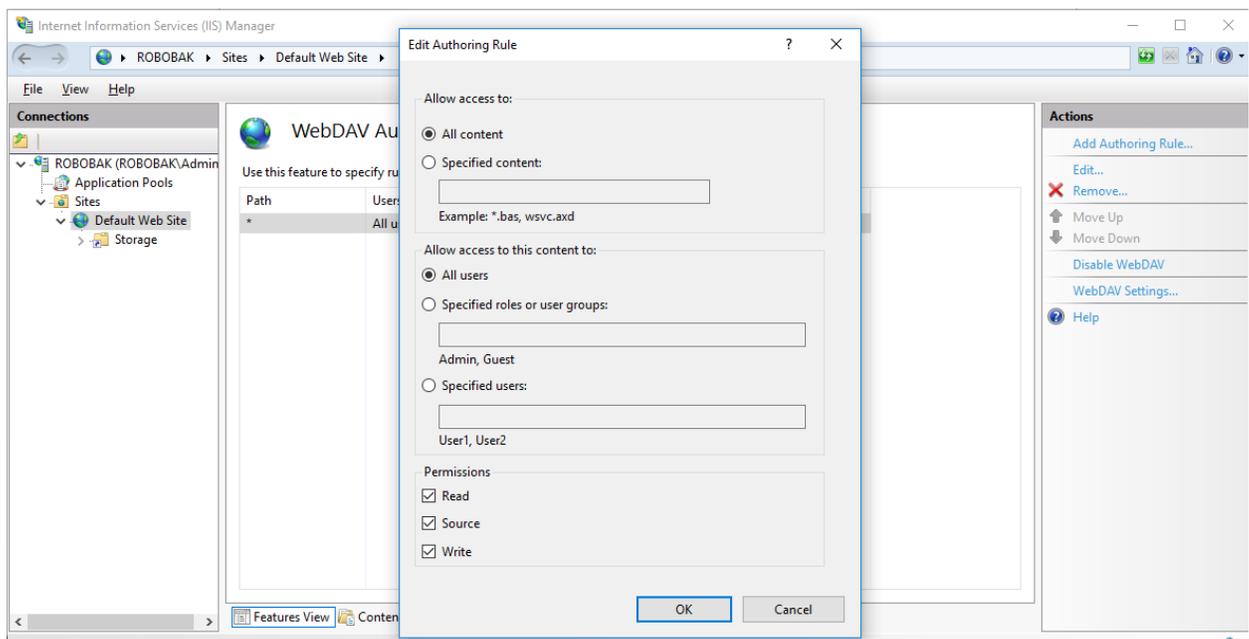
7. Go to <server name> Sites > Default Web Site.

8. Double-click on **Authentication**.

9. Enable **Windows Authentication**. We also recommend disabling anonymous authentication. Once it is enabled, you will see the **Providers…** link in the **Actions** panel.

10. Open **Providers**... and use the **Move Up** / **Move Down** buttons to move the NTLM entry to above the **Negotiate** entry. Press **OK**.
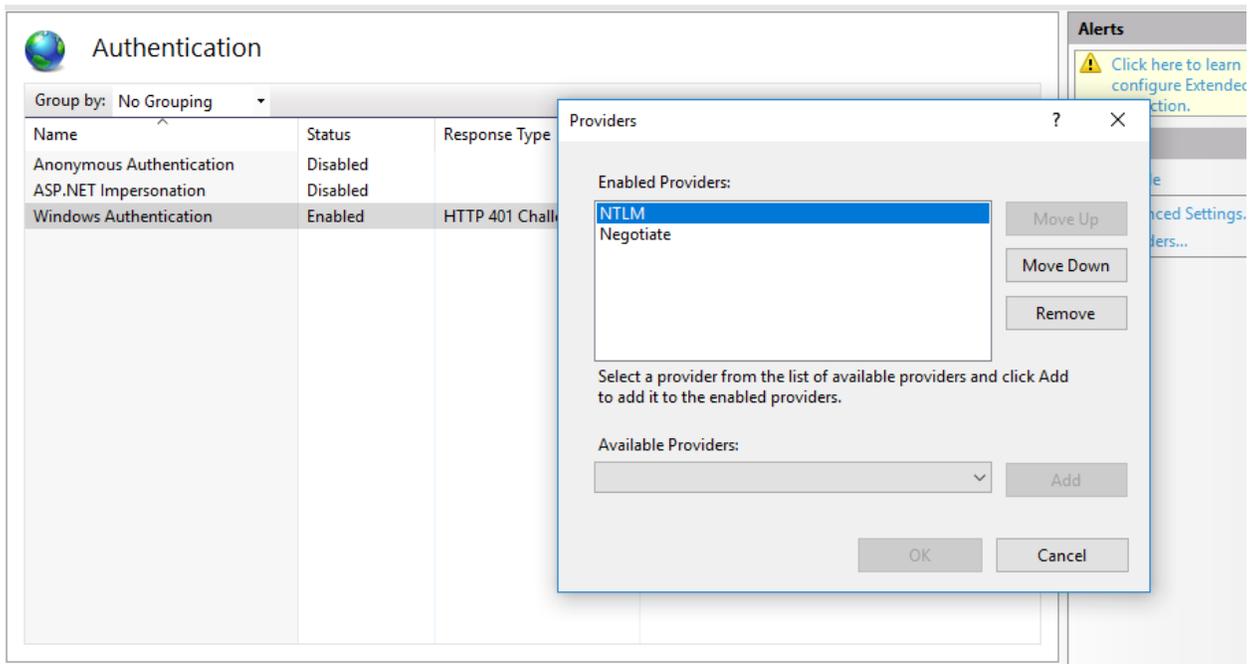
11. Go to <server name> and double-click **Default Document**. Press **Disable** from the **Action** pane.

12. Go to <server name> and double-click **Output Caching** > Click **Edit Feature Settings....** from the left pane.

13. Uncheck **Enable cache** and **Enable kernel cache**.

14. Click **OK.**

Step 3 - Setting up storage Folders

The final step is to create a backup destination using IIS for Cloud Backup jobs to use if the WebDAV destination is selected.

1. Open IIS Manager.

2. Go to <server name> Sites >Default Web Site.

3. Right-click the default website and select **Add Virtual Directory**.

4. In the **Alias** field, type in "Storage". This alias, combined with the host URL, will be the value you enter in the *Server URL* field in the *Set up destination* step, when creating a BackupAssist WebDAV backup job. For this example, the Server URL value will come out to be http://robobak/Storage.

5. Specify a suitable **Physical Path**, for example: C:\\WebDAV.

6. Click **Finish**.

To get the URL required by BackupAssist, you can right-click the storage you created in IIS and select the browse button sub menu to open the storage with the URL used by IIS.

> **Note:** On WebDAV 8 and newer do not use the same name for the alias in IIS and the Container name in BackupAssist as this could cause the job to fail.

Step 4 - Create a backup to the WebDAV destination

Once you have created your storage, you can use it for private cloud backup jobs. Just create a BackupAssist Cloud Backup job and select WebDAV as the destination and configure WebDAV in the *Set up Destination* step.
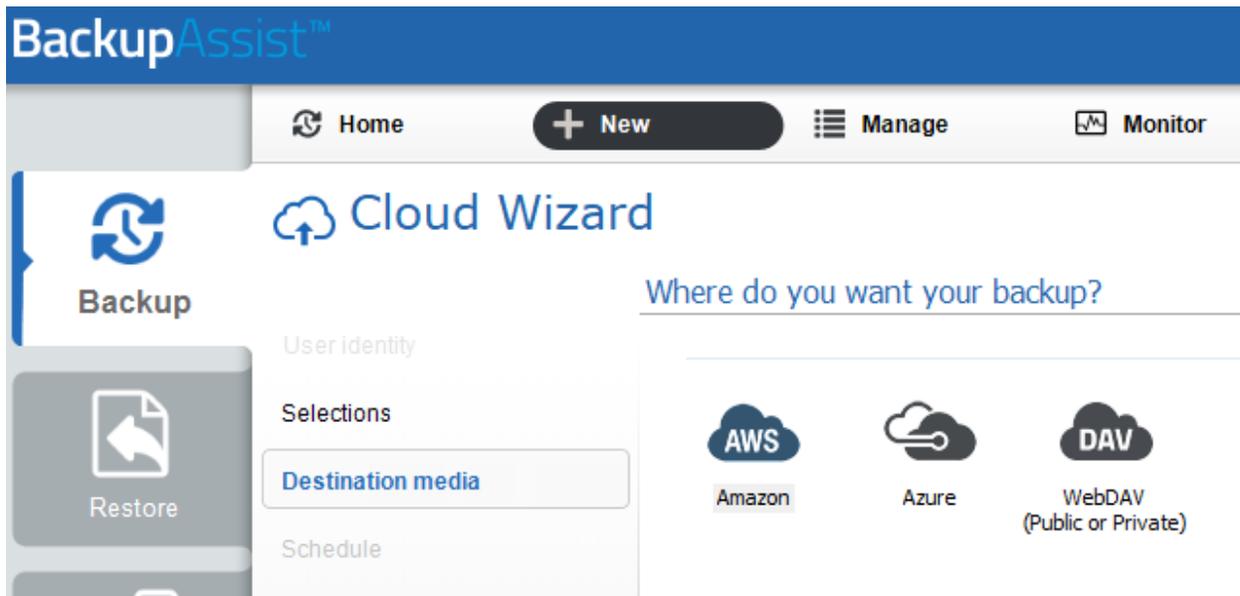
In the *Set up Destination* step you will need to fill I the following details:

- Backup Container: Provide a name for a backup destination folder. BackupAssist will create this folder in the virtual directory that you created in IIS, when you click **Check Destination**. The container name can be anything you want, for example the server name or job name.

The name can only be made of lower case letters and numbers. No capital letters, spaces or special characters allowed.

- Server URL: This will be http://server_name/alias as per the configurations you set when configuring your virtual directory.

- User Name and Password: This is what you will use to access your IIS server.

- Encryption Password: This is the password to encrypt your backup files. You will need this to do restores and the password cannot be recovered if lost.