Use inSync to protect Amazon WorkSpaces

Overview

Amazon WorkSpaces is an easy and secure way of providing the users in your organization access to a virtual desktop environment that is similar to that on their devices.

Data on Amazon WorkSpaces should be protected and secured so that it can be recovered in scenarios such as in case of accidental deletion. In addition, in scenarios such as a Ransomware attack, administrators can -

- Leverage the protected data in Amazon WorkSpaces for security tests
- Facilitate users by making the data available on their devices to their Amazon WorkSpace enabling them to resume their activities to support business operations

With Druva, administrators can configure and protect user data on Windows provisioned Amazon WorkSpaces and take advantage of additional Druva capabilities. Also, protected data on Windows drives or partitions can be mapped and restored enabling users to seamlessly access their data on both, their devices and Amazon WorkSpaces account.

Plan for protecting data on Amazon WorkSpaces

Choose from the following use-cases for which you plan to use Druva -

- Protect Amazon WorkSpaces assigned to users as an additional work platform - Only protect data of users working on Windows provisioned Amazon WorkSpaces.
  If you want to use Amazon WorkSpaces as an additional work platform beside a device, see Protect Amazon WorkSpaces as an additional work platform.

- Facilitate users by making their data available on Amazon WorkSpaces and later failback-
  1. Restore or migrate protected data of users on Amazon WorkSpaces and enable them to work on it.
  2. After the remote work is complete and users want to later failback to their original device with all the updated data.

If you want to facilitate users, see Facilitate users by making their protected data available on Amazon WorkSpaces.
Protect Amazon WorkSpaces as an additional work platform

Amazon WorkSpaces provides a virtual desktop interface similar to Windows OS. Administrators can install inSync Client for supported Windows OS on the user assigned Amazon WorkSpaces. Data protection for Amazon WorkSpaces works similar to other Windows OS-based devices. Any data generated on Amazon WorkSpaces is backed up based on the backup setting defined in the inSync Profile assigned to the user. For detailed instructions on installing and activating the latest inSync Client, see Install and activate inSync Client.

**Important:**

- When you activate inSync Client on Amazon WorkSpace, choose **Add a new device** option on the Activation window to add Amazon WorkSpace as an additional workspace for data protection. For more information, see Add a new device to your inSync account.

- In organizations where users are managed using Active Directory (AD) administrators can mass deploy inSync Client on Amazon WorkSpaces and activate it. For more information, see Integrated mass deployment of inSync Client.

Facilitate users by making their protected data available on Amazon WorkSpaces

This use case addresses the requirement of providing inSync users access to their protected data from their device on Amazon WorkSpaces. This is helpful in scenarios where users may not have access to their device because of situations like device loss, working from a remote location, device refresh activity in progress or lack of a VPN connection (enforced by organizations.

Administrators can resort to the provisioning of Amazon WorkSpace account for such users and enable them to resume their activities to support business operations.

However, there is a list of things that administrators need to do and fulfill this requirement using Druva.

**Some facts to consider -**

Amazon WorkSpaces provides a virtual desktop interface similar to Windows OS. However, in terms of logical partitioning of storage, there is less flexibility in Amazon WorkSpaces compared to Windows OS.

- A user device running on Windows OS may have multiple logical partitions or drives other than C:\ - for a better arrangement of data or segregation of workspace and personal data.

- An Amazon WorkSpace has only two partitions - C:\ and D:\. On Windows provisioned Amazon WorkSpaces, root volume is mapped to C: drive and user volume is mapped to D:\ drive.

Replace user device with Amazon WorkSpace account as the primary device

In order to enable users to work on their data from their Amazon WorkSpace account, you must restore the data from their device to their Amazon WorkSpace account.

https://docs.druva.com/Endpoints/030_Set_up_inSync_for_Endpoints/Protect_Amazon_WorkSpaces_using_Druva_inSync/U…

Updated: Wed, 22 Sep 2021 16:31:12 GMT

Powered by
Follow these steps to enable users to access their device data on Amazon WorkSpace -

**Step 1 - Prepare user’s device to back up all the drives**

Assume

- User’s Windows device has 4 drives, C:\, D:\, E:\, and F:\
- C:\ drive holds user’s profile data
- D:\, E:\, and F:\ drives holds user’s other data

All the drives need to be configured for backup to enable the restoration of data of these drives to the user’s D:\ drive on Amazon WorkSpace.

- As Amazon WorkSpace has C:\ and D:\ drives, the user’s data on C:\ and D:\ drive can be easily mapped and restored.
- For backing up and restoring data from E:\ and F:\ drive, create NTFS junction points.

Run the following commands to create NTFS junction points on D:\ drive -

**Create Junction point for E:\ drive**

C:\> mklink /J D:\E_Data E:\

**Create Junction point for F:\ drive**

C:\> mklink /J D:\F_Data F:\

**Important:**

- Create the NTFS junction points in D:\ because it maps to the user volume on Amazon WorkSpace.
- *E_Data* and *F_Data* are sample names that we have used for demonstration purposes. You can provide any names as per your guidelines.
- Create junction points for every drive of which data you want to migrate to Amazon WorkSpace using the command.

**Step 2 - Update inSync profile associated with the users**

As an administrator, update the profile assigned to the users to backup all the drives.

To edit a profile

1. On the inSync Management Console menu bar, click **Profiles**.
2. On the Manage Profile page, select the profile that you want to update.
3. Configure the following for backup from a user’s device -
1. Configure %userprofile% as a custom folder for backup.
This takes care of moving data from C:\ drive i.e. User profile to user profile (D:\ drive) on Amazon Workspace. For detailed instructions, see Configure custom folders for backup.

2. Configure D:\ drive for backup

3. Configure the NTFS junction points that we created earlier, for backup
   - D:\F_Data
   - D:\E_Data
   Also, add any additional NTFS junction points if you have created.

Important: When you are configuring custom folders for backup, ensure all the devices of the users associated with the profile have these custom folders. Else, the inSync Client on those devices generates a ‘Misconfigured folder’ alert.

**Step 3 - Backup user devices**

After configuring user devices and adding folders for backup in inSync profile, trigger backup on the user devices. After the backup is complete, proceed to step 4.

**Step 4 - Install inSync and migrate protected data to Amazon WorkSpace account**

1. Install inSync Client in the user’s Amazon WorkSpace account. For detailed instructions, see Install the inSync Client on Windows.

Important:
- In organizations where users are managed using Active Directory (AD) administrators can mass deploy inSync Client on Amazon WorkSpaces and activate it. For more information, see Integrated mass deployment of inSync Client.

2. Activate inSync Client and select Replace an Existing Device option during activation. Also, select Restore Now to restore the protected data from the user device to their Amazon WorkSpace account. For detailed instructions, see Replace a device linked with your inSync account.

Important:
- Druva recommends activating Amazon WorkSpace using the Replace an Existing Device option.
- After activation of inSync Client on Amazon WorkSpace using the ‘Replace an Existing Device’ option, inSync Client on the user device is deactivated. Hence, any changes made to the data on the original device after inSync Client deactivation are not updated on inSync Cloud.

After you select the Restore Now option, inSync restores the following data in the user’s Amazon WorkSpace account.
• Restores USERPROFILE on user volume (D: drive)
• Restores contents of D:\ drive on D:\D_Data folder on Amazon Workspace.
• Restore contents of E:\ drive on D:\E_Data folder on Amazon Workspace.
• Restore contents of F:\ drive on D:\F_Data folder on Amazon Workspace.
• If you have configured other drives, restores contents in a folder in D:\ on Amazon Workspace.

After the restoration of data is complete, users can start working on their desired data by accessing it. inSync Client ensures newly created and any updated data is backed up to inSync Cloud.

Failback to user’s original device from their Amazon WorkSpace account

After the requirement of working on Amazon WorkSpace account is over, in scenarios such as inSync users gaining access to their device after overcoming situations like getting a new device from IT after device loss, device refresh activity, or gaining access to VPN network and so on.

Administrators can move the data from the user’s Amazon WorkSpace account to the mapped device drives on user’s device.

Follow these steps to again make a user's original device as the primary device and restore the latest data on all the drives.

**Important**: The following steps assume NTFS junction points created earlier are available on the device.

**Step 1 - Uninstall the inSync Client from the user device**

As an Administrator, uninstall the inSync Client, which is already in the deactivated state from the user device. For detailed instructions, see [Uninstall inSync Client](#).

**Important**: Ensure you perform a clean uninstall, that is, remove the configuration details from the device.

**Step 2 - Install the latest inSync Client on the device.**

For detailed instructions, see [Install the inSync Client on Windows](#).

**Step 3 - Activate the inSync Client on the device**

Select Replace an Existing Device option during activation. After prompted to restore data, select Restore Now to restore the protected data on the user device from their Amazon WorkSpace account. For detailed instructions, see [Replace a device linked with your inSync account](#).

After you select Restore Now option, inSync restores the following data on the user’s device -
• Data for USERPROFILE is restored to the C:\Users\<username> on the user device.
• Data on D: drive on Amazon WorkSpace is restored to D: to the user device.