Convert an existing appliance agent to Direct-to-Cloud (D2C)

https://help.axcient.com/003-manage-d2c/1500000655082-x360Recover-Direct-to-Cloud-D2C-Convert-from-appliance-mode-to-D2C-mode

Overview

- Watch a 4 minute video: **Convert an existing appliance agent to Direct-to-Cloud (D2C)**

Why switch an agent from appliance mode to Direct-to-Cloud mode?

It is sometimes necessary or desirable to switch an existing protected system agent operating in the appliance mode to one operating in the Direct-to-Cloud mode. For example:

- You may have an aging, on-premise BDR appliance you would like to retire in order to convert a customer from appliance-based backups to Direct-to-Cloud backups. However, the existing backup history already replicated by the appliance to the Cloud vault must not be lost.
- You may have a customer who has experienced a sitewide disaster, with their server infrastructure virtualized in the Axcient cloud. To seamlessly continue backups while virtualized in the cloud, you might prefer to convert the agents on the protected systems to Direct-to-Cloud mode, and then attach them to the existing vault backup sets.

What happens during the switch from appliance to Direct-to-Cloud?

During the conversion from appliance mode to Direct-to-Cloud mode, data for the protected system may already exist from a previous appliance replication. The agent now assumes the vault instance and preserves the existing recovery point history.

Important: A full backup is required when converting an agent from appliance to Direct-to-Cloud (or vice versa.) In most cases, this full backup will be triggered automatically. If the full backup is not triggered automatically, then a full backup should be triggered manually. This is to ensure that critical recovery metadata is generated and fully synced between the server and the protected system.

Note: Although the agent will scan the full contents of the protected system disks during this backup, the data sent to the cloud will be deduplicated and only net-new and changed data will be sent to the vault over the internet. This backup is expected to take somewhat longer than a normal Incremental backup, but typically only by a few minutes.

A note about full backups in x360Recover

Unlike other backup products, x360Recover does not generate new recovery chains when performing subsequent full backups.

Instead, because of the chain-free nature of x360Recover, the additional full backup simply serves to fully synchronize the protected system with the backup server. Any data on the backup server which is not different from data on the protected system is discarded and does not cause duplication of storage consumption.

The agent sends hash data to both appliances and vaults. The hash data used by the agent to determine which blocks that have changed is stored. When a full backup is performed, the hash data from the backup server is downloaded to allow full deduplication of the data already present on the server.

When a new full backup is requested, the agent copy of the hash file is deleted and the server-side hash files are downloaded. This serves as the basis for deciding ‘what has changed’ between the last backup on the server and the current protected system.

Agent hash files are replicated to the vault along with the protected system snapshot data. When converting an endpoint from appliance-based backups to Direct-to-Cloud, the current hash data is already present on the vault.

Steps to convert an existing appliance agent to Direct-to-Cloud

Important: Do NOT remove any endpoints or customer locations in the license portal (as described in step 10) until you have completed steps 1 through 9 *first*. If the BDR appliance is no longer functional, skip steps 3 and 4.

Important: Appliance-Based protected systems using 'Storage-Based' licensing have long-term retention policies (3-year or 10-year) that are NOT inherited when the protected system is converted to Direct-to-Cloud (D2C). Please review your retention policy after the conversion to ensure it meets your client's needs.

To convert an existing appliance agent to Direct-to-Cloud, perform the following steps:

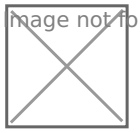
1. Verify that no backup is currently running on the appliance.

2. Uninstall the agent from the protected system.

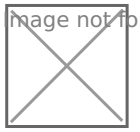
Important: Do NOT delete the agent installation directory or aristos.cfg file.

3. Verify that the appliance has completed replication of all snapshots. The date/time on the most recent snapshot on the appliance should match the most recent snapshot on the vault.

4.1. In the *Protected System Details* page for the system being converted, click the **Replication** button as shown below:



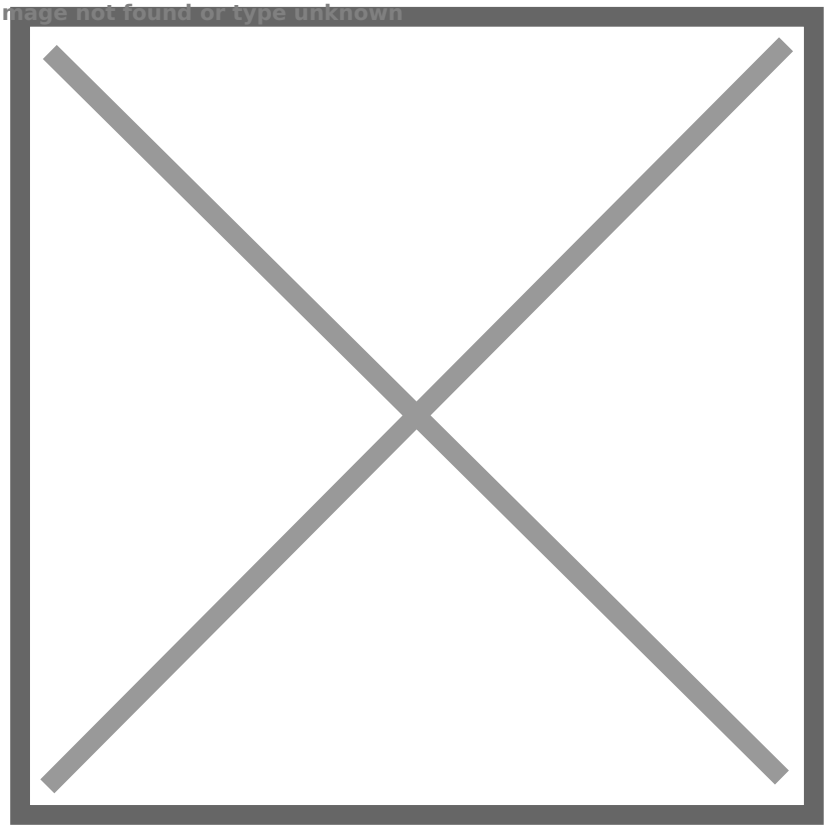
4.2. When the *Replication settings* window opens, click the **Delete** button as shown below:



4.3 When the *Delete Replication Settings* window opens, click the button marked **Delete Replication Settings but leave Protected System on Vault**, as shown in the red box below:

Important: Do **NOT** enter the hostname in the *Hostname* field and Do **NOT** click on the *Delete Settings and Vault Data* button.

Image not found or type unknown



5. Download the Direct-to-Cloud Windows agent via the vault user interface.

For Direct-to-Cloud, you can find the **Windows Agent** download link under the **Clients** tab in the vault:

Image not found or type unknown

6. Install the Direct-to-Cloud agent on the protected system. Since the Replibit Folder and Aristos.cfg file still exist, the agent installer will not present the parameter configuration screen during installation with the server field grayed out and not available to be selected. For full details on installation, see the Direct-to-Cloud Quick Start Guide.

Important: The Direct-to-Cloud agent installation file contains a specially formatted name, including an installation token that identifies which client the agent is being installed for. **Do not rename the agent installation file when downloading it from the vault.**

7. Verify that the protected system is registered in the Axcient Cloud:

- Open the *Protected Systems* page on the vault and review the **Location** column.
  1. If the protected system is on Direct-to-Cloud, it will indicate **Axcient Cloud** under *Location*
  2. Additionally, after an end point has been converted to D2C, it will display a **Schedule** section:

Image not found or type unknown

8. Verify that the next backup executed is a full backup. (If this is not the case, click **Schedule Now** and select *Full Backup from the Protected Systems Details* page.)

9. Delete the protected system from the appliance.

10. Reduce the endpoint licensing count for the customer location in the License Portal.

- **If you are decommissioning the appliance for this client:** Once the protected systems are longer showing in the Recover Manager for the appliance, you must then remove the license location in the license portal.

- **If the appliance is no longer accessible:** You must still (a) remove the endpoints on the license portal and then (b) put in a ticket with Support to have the license location removed for the appliance. (If the appliance has been assigned a storage license, you do not need to adjust the License Portal configuration.)

Billing considerations

Important: To avoid double-billing for this protected system, you must remove the protected system as described in steps 1 through 10 (above.)

If the appliance has been assigned a storage license, you do not need to adjust the License Portal configuration (as described in step 10 above). Your billing will reflect a new Direct-to-Cloud endpoint charge in the next billing cycle.

Converting a protected system to Direct-to-Cloud mode automatically triggers billing for a new Direct-to-Cloud endpoint.

For a full review of Direct-to-Cloud billing, please see Direct-to-Cloud (D2C) Billing.

Revision #1
Created 11 September 2024 13:30:54 by ColtM
Updated 11 September 2024 13:31:28 by ColtM