Arcserve® Unified Data Protection Cloud Hybrid User Guide

Version 1.1

arcserve

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time. This Documentation is proprietary information of Arcserve and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

Contact Support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve product.

Contents

Chapter 1: Understanding Arcserve UDP Cloud Hybrid

Welcome to the Arcserve UDP Cloud Hybrid documentation. This document provides the information about setting up, accessing, and using Cloud Hybrid.

This section contains the following topics:

Introduction

Arcserve UDP Cloud Hybrid is a cloud computing service that empowers your organization to complete your data protection needs using a seamless integrated Cloud backup and Disaster Recovery (DR). Cloud Hybrid is a business continuity solution that ensures the offsite availability of your critical systems and data.

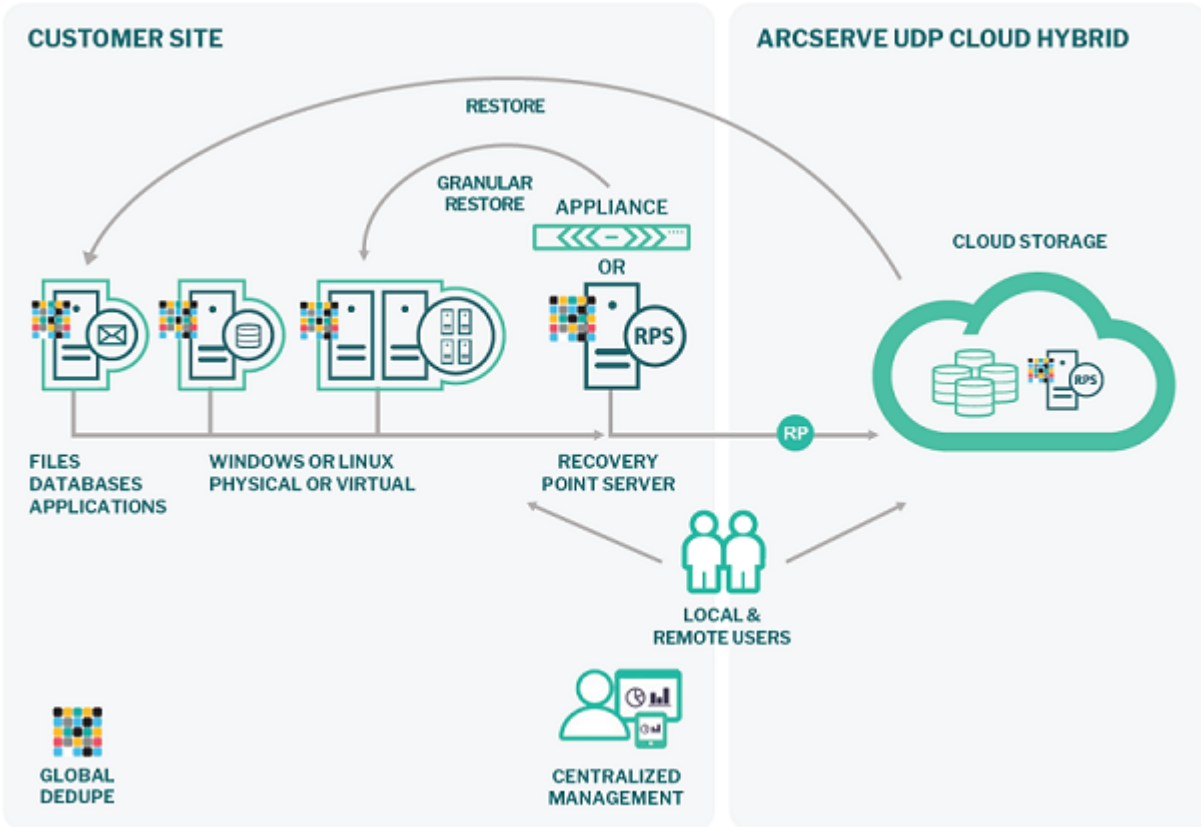
Offered as a service extension to Arcserve UDP platform, Cloud Hybrid leverages global deduplication, encryption, compression, and WAN-optimized replication for complete security and efficiency of your data protection.

With seamless integration, connect the On-premise Recovery Point Server (RPS) or Arcserve UDP Appliance to the Cloud RPS where the data is automatically replicated to manage the data in Cloud Hybrid.

Cloud Hybrid is available in the following service types:

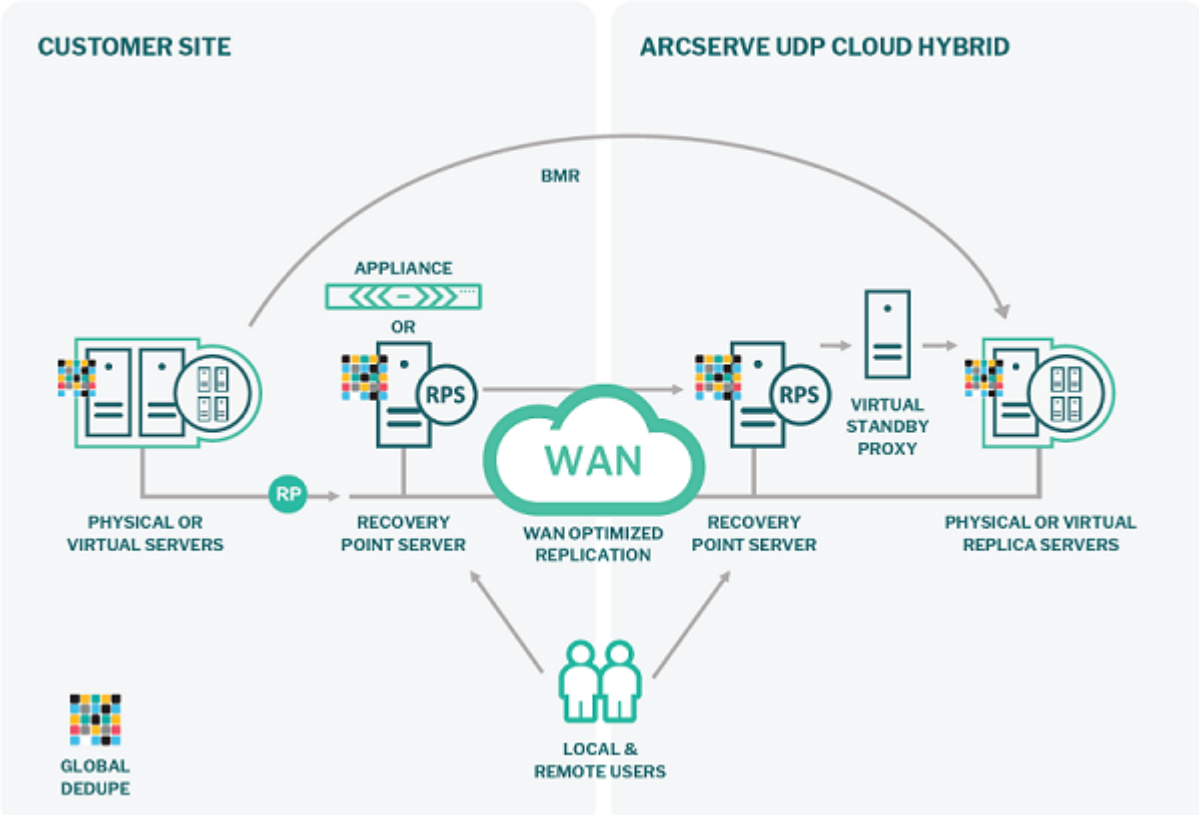
- **Backup as a Service (BaaS):** Cloud Hybrid automatically replicates your backup images from the On-premise Recovery Point Server (RPS) to a corresponding RPS in the cloud (disk to disk to cloud). You can manage the entire backup process from the Arcserve UDP Console specifying the backup source, destination, and retention.

  For more information, refer Using BaaS.



- **Disaster Recovery as a Service (DRaaS):** Cloud Hybrid goes beyond critical data asset protection and empowers organizations to complete their data protection strategy using a seamless Disaster Recovery (DR). This service is offered as an extension to the Arcserve UDP platform, a next-generation solution that leverages global deduplication, encryption, compression, and WAN-optimized replication.

  For more information, refer Using DRaaS.



Arcserve UDP Cloud Hybrid lets you replicate from one RPs to another and manually replicate the data from Cloud Hybrid.

For more information refer the following:

- Replicate from RPS to RPS
- Manual Replication from Cloud Hybrid

Simply connect your Arcserve Appliance to Cloud Hybrid and get going!

Features

Some of the key features available in Arcserve UDP Cloud Hybrid are listed below.

- **Replicate to Cloud Hybrid:** Using Arcserve UDP, you can replicate the backup sessions from On-premise Recovery Point Server to Cloud Hybrid. This process ensures that an additional copy of recovery points is available if the original recovery points are merged or accidentally deleted.

  For more information, see How to Replicate Data to the Cloud Hybrid Recovery Point Server.

- **Download file/folder from Cloud Hybrid:** Download of file/folder is available from the Cloud Hybrid replicated sessions of Windows file systems. The backup types supported are Windows Agent-based backup, Host-based agentless backup for Windows virtual machine, and UNC path. In a DRaaS environment, you can download file/folder from the Cloud Hybrid replicated sessions of Linux file systems.

  For more information, see How to Download Files and Folders from Cloud Hybrid.

- **Backing up Office 365 OneDrive to Cloud Hybrid:** OneDrive is a file store hosted on Microsoft Cloud. The OneDrive plan consists of a backup task that lets you specify the OneDrive nodes that you want to protect, the backup destination, and the backup schedule. The backup destination is a non-deduplication data store or deduplication data store where you store your backup data.

  For more information, see How to Create a Microsoft Office 365 OneDrive Node Backup Plan.

  Note: To enable this feature you require Arcserve UDP 7.0 in Cloud Hybrid.

- **Backing up Office 365 Exchange Online to Cloud Hybrid:** Exchange Online is an email application hosted on Microsoft Cloud. Create a plan to protect Exchange Online mail items such as mails, calendar items, contacts, and so on from Microsoft Cloud. The plan for Exchange Online consists of a backup task that lets you specify the Exchange Online nodes that you want to protect, the backup destination, and the backup schedule. The backup destination is a non-deduplication or deduplication data store where the backed-up data is stored.

  For more information, see How to Create an Exchange Online Plan.

- **Backing up Office 365 SharePoint Online to Cloud Hybrid:** SharePoint Online is a portal management application hosted on Microsoft Cloud. Create a SharePoint Online plan to protect SharePoint Online list items such as document library, list library, and so on from Microsoft Cloud. The SharePoint Online plan consists of a backup task that lets you specify the SharePoint Online nodes that you want to protect, the backup destination, and the backup schedule. The backup destination is a non-deduplication data store or deduplication data store where you store your backup data.

  For more information, see How to Create a SharePoint Online Plan.

- **Assured Recovery:** To verify accessibility and assured recovery of the data, create an assured recovery plan. The plan for assured recovery is based on the backup/replication plan. This recovery task adds an assured recovery task to an existing backup or replication plan that consists of a source, test settings, schedule, and advanced settings. You can also run an Assured Recovery job manually.

  For more information, see How to Create an Assured Recovery Plan.

- **Reporting in Cloud Hybrid:**

  - **RPO Reporting:** Recovery Point Objective (RPO) report is the compliance report that displays how the recovery points are distributed in the backup environment. The report helps assess, in case of a disaster, the oldest and latest point in time that the node can return to.

    For more information, see RPO Reports.

  - **RTO Reporting:** Recovery Time Objective (RTO) report is the compliance report that displays if the defined recovery time objective is met for all the executed recovery type of jobs.

    For more information, see RTO Reports.

- **Using Virtual Standby in Cloud Hybrid:** Virtual Standby converts the recovery points to virtual machine formats on specified cloud and prepares a snapshot to easily recover your data when needed. This feature is capable to provide high availability and also ensures that the virtual machine can take over immediately when the source machine fails.

  For more information, see How to Create a Virtual Standby Plan.

- **Using Instant VM in Cloud Hybrid:** Instant virtual machine (Instant VM) helps you to run the backup session inside the virtual machine without any prior conversion and create a virtual machine in the hypervisor. The Instant virtual machine provides instant access to the data and applications available in the

Arcserve UDP backup sessions. Instant VM eliminates the downtime for restore or conversion of the backup session to a physical or virtual machine.

For more information, see How to Create and Manage an Instant Virtual Machine on Hyper-V and VMware ESX Servers.

What Will a Customer Get with Cloud Hybrid?

With Cloud Hybrid, you will get the following:

- Arcserve UDP Console/RPS server.
- URL to access the Arcserve UDP Console.
- User name and password for the account used to log into the Arcserve UDP Console available in Cloud Hybrid where the same credentials are applicable to authenticate when you add the *Replicate to a remotely-managed RPS* task in the On-premise Arcserve UDP Console.

  Important! The deduplication datastore in Cloud Hybrid has a randomly generated encryption password by default. You must modify the encryption password in the first Cloud Hybrid login as Arcserve cannot restore the default password. We recommend to keep the newly created password safe as you need the password later to perform tasks such as importing the datastore and running a consistency check on the deduplication datastore. You can modify the newly created password later from datastore setting if the datastore is not deleted from Cloud Hybrid.
- A Hyper-V node if the optional Cloud Hybrid Compute subscription is purchased.
- A pre-configured Linux backup server that runs on Hyper-V.

Prerequisites to Access Cloud Hybrid

Before accessing Cloud Hybrid, verify the following prerequisites:

- You have an Arcserve UDP software or Appliance.
- You have received an email from Arcserve Support containing the following details to access Cloud Hybrid:
  - URL to the Arcserve UDP Console
  - Host name (Node name)
  - User name and Password for Cloud Hybrid.
- If the optional Cloud Hybrid Compute subscription is purchased, the following details are provided:
  - Password for root account of Linux backup server and Point to Site VPN access (same as the Cloud Hybrid password)
  - Unique configuration files for the Point to Site VPN

Backward Compatibility Support Policy

The following table lists the supported versions of Arcserve UDP for Cloud Hybrid Replication with 6.5 Update 4:

On-Premise Version	Replication supported to Cloud Hybrid (Arcserve UDP 6.5 Update 4)	Manual Reverse Replicate from Cloud Hybrid (Arcserve UDP 6.5 Update 4) to On-Premise	Requirements for Manual Reverse Replicate from Cloud Hybrid (Arcserve UDP 6.5 Update 4) to On-Premise
Arcserve UDP 7.0 Update 2	Yes	Yes	Apply patch P00001738
Arcserve UDP 7.0 Update 1	Yes	Yes	Apply patch P00001738
Arcserve UDP 7.0	Yes	Yes	Apply patch P00001738
Arcserve UDP 6.5 Update 4	Yes	Yes	-
Arcserve UDP 6.5 Update 3	Yes	Yes	-
Arcserve UDP 6.5 Update 2	Yes	Yes	-
Arcserve UDP 6.5 Update 1	Yes	Yes	-
Arcserve UDP 6.5	Yes	Yes	-
Arcserve UDP 6.0 (All Updates)	No	No	-

The following table lists the supported versions of Arcserve UDP for Cloud Hybrid Replication with 7.0:

On-Premise Version	Replication supported to Cloud Hybrid (Arcserve UDP 7.0)	Requirements for Replication supported to Cloud Hybrid (Arcserve UDP 7.0)	Manual Reverse Replicate from Cloud Hybrid (Arcserve UDP 7.0) to On-Premise
Arcserve UDP 7.0 Update 2	Yes	-	Yes

Arcserve UDP 7.0 Update 1	Yes	-	Yes
Arcserve UDP 7.0	Yes	-	Yes
Arcserve UDP 6.5 Update 4	Yes	Apply patch P00001738	Yes
Arcserve UDP 6.5 Update 3	Yes	Upgrade to 6.5 Update 4 and then apply patch P00001738	No
Arcserve UDP 6.5 Update 2	Yes		No
Arcserve UDP 6.5 Update 1	Yes		No
Arcserve UDP 6.5	Yes		No
Arcserve UDP 6.0 (All Updates)	No	-	No

Important: Verify if the version of Arcserve UDP Console is similar or higher to the version of Cloud Hybrid. For example, when the version of Cloud Hybrid is 7.0 but the Console has version 6.5, an error message appears when you create plan or modify existing plan to add or modify **Replicate to a remotely-managed RPS task** on On-Premise. The message displays: *The version of Console is lower, please upgrade your console and try again.*

To save the plan, apply Patch P00001738 on the On-Premise Console for v6.5 Update 4.

The following table lists the supported versions of Arcserve UDP for Cloud Hybrid Replication with 7.0 Update 1:

On-Premise Version	Replication supported to Cloud Hybrid (Arcserve UDP 7.0 Update 1)	Requirements for Replication supported to Cloud Hybrid (Arcserve UDP 7.0 Update 1)	Manual Reverse Replicate from Cloud Hybrid (Arcserve UDP 7.0 Update 1) to On-Premise
Arcserve UDP 7.0 Update 2	Yes	-	Yes
Arcserve UDP 7.0 Update 1	Yes	-	Yes
Arcserve UDP 7.0	Yes	-	Yes
Arcserve UDP 6.5 Update 4	Yes	Apply patch P00001738	Yes
Arcserve UDP 6.5 Update 3	Yes	Upgrade to 6.5 Update 4 and then apply patch	No

Arcserve UDP 6.5 Update 2	Yes	P00001738	No
Arcserve UDP 6.5 Update 1	Yes		No
Arcserve UDP 6.5	Yes		No
Arcserve UDP 6.0 (All Updates)	No	-	No

Important: Verify if the version of Arcserve UDP Console is similar or higher to the version of Cloud Hybrid. For example, when the version of Cloud Hybrid is 7.0 Update 1 but the Console has version 6.5, an error message appears when you create plan or modify existing plan to add or modify **Replicate to a remotely-managed RPS** task on On-Premise. The message displays: *The version of Console is lower, please upgrade your console and try again.*

To save the plan, apply Patch P00001738 on the On-Premise Console for v6.5 Update 4.

The following table lists the supported versions of Arcserve UDP for Cloud Hybrid Replication with 7.0 Update 2:

On-Premise Version	Replication supported to Cloud Hybrid (Arcserve UDP 7.0 Update 2)	Requirements for Replication supported to Cloud Hybrid (Arcserve UDP 7.0 Update 2)	Manual Reverse Replicate from Cloud Hybrid (Arcserve UDP 7.0 Update 2) to On-Premise
Arcserve UDP 7.0 Update 2	Yes	-	Yes
Arcserve UDP 7.0 Update 1	Yes	-	Yes
Arcserve UDP 7.0	Yes	-	Yes
Arcserve UDP 6.5 Update 4	Yes	Apply patch P00001738	Yes
Arcserve UDP 6.5 Update 3	Yes	Upgrade to 6.5 Update 4 and then apply patch P00001738	No
Arcserve UDP 6.5 Update 2	Yes		No
Arcserve UDP 6.5 Update 1	Yes		No
Arcserve UDP 6.5	Yes		No
Arcserve UDP 6.0 (All Updates)	No	-	No

Important: Verify if the version of Arcserve UDP Console is similar or higher to the version of Cloud Hybrid. For example, when the version of Cloud Hybrid is 7.0 Update 2 but the Console has version 6.5, an error message appears when you

create plan or modify existing plan to add or modify **Replicate to a remotely-managed RPS** task on On-Premise. The message displays: *The version of Console is lower, please upgrade your console and try again.*

To save the plan, apply Patch P00001738 on the On-Premise Console for v6.5 Update 4.

Chapter 2: Using Cloud Hybrid as a Backup Service

Arcserve UDP Cloud Hybrid (BaaS) lets you perform the following functions:

- Replicate the backup images from the On-premise Recovery Point Server (RPS) to a corresponding RPS in the Cloud Hybrid.
- Restore and download the files/folders from Cloud Hybrid RPS to On-premise RPS.
- Create a Plan to protect Microsoft Office 365 Exchange Online, SharePoint Online or OneDrive data to Cloud Hybrid.
- Restore Office 365 Exchange Online, SharePoint Online data from Cloud Hybrid to Office 365 Server.
- Export Microsoft Office 365 OneDrive data from Arcserve UDP Cloud Hybrid to local disk.

This section contains the following topics:

Replicate Data to the Cloud Hybrid Recovery Point Server

This section contains the following topics:

How to Replicate the Protected Windows Node Data using Shared Plan

You can replicate the backup data to another recovery point server located in Cloud Hybrid managed from a different Arcserve UDP Console.

Create a new plan and move the nodes later into the replicated Cloud Hybrid plan.

Follow these steps:

1. Log into the Arcserve UDP Console available in the Cloud Hybrid using the credentials received through email.
2. Create or modify an Arcserve UDP plan on your local Arcserve UDP Appliance and add the **Replicate to a remotely-managed RPS** task after adding the Agent or Agentless Backup task.
3. In the **Destination** tab of the **Replicate to a remotely-managed RPS** task, use the information from the email you received to add the remote console, user name, and password.

   Port: 8015

   Protocol: HTTPS

   Note: The remote console located in Cloud Hybrid validates these credentials.
4. Select **Enable Proxy** if your network uses an Internet proxy and configure to your network specifications.

   Note: This information may vary and is similar to configuring a browser to access the Internet from the local network.
5. Click **Connect** to validate the connection to the RPS server in Cloud Hybrid.
6. From the Plan drop-down list, select the Replication plan from the Cloud Hybrid RPS server.

   Note: The selected plan is the Share Plan from the Cloud Hybrid RPS server for your company.
7. Click **Save** and the data is replicated after the next backup.

   By default, node replication begins after the backup is completed and the recovery points from the nodes are replicated to the Cloud Hybrid RPS server. To modify the schedule, you can add a Replication schedule.

How to Replicate the Protected Linux Node Data using Shared Plan

Arcserve UDP lets you create a plan and store your Linux backup sessions to a recovery point server. Also, Arcserve UDP allows the replication of Linux recovery points to another RPS located in Cloud Hybrid.

Follow these steps:

1. Log into the Arcserve UDP Console available in the Cloud Hybrid with the credentials provided in the email that you received.
2. Create or modify an Arcserve UDP plan on your local Arcserve UDP Appliance and add the **Replicate to a remotely-managed RPS** task after adding the Agent or Agentless Backup task.
3. In the Destination tab of the Replicate to a remotely-managed RPS task, use the information in the email received to add the remote console, user name, and password.

   Port: 8015

   Protocol: HTTPS

   Note: These credentials are validated on the remote console located in Cloud Hybrid.
4. Select **Enable Proxy** if your network uses an Internet proxy and configure to your network specifications.

   Note: This information may vary and is similar to configuring a browser to access the Internet from the local network.
5. Click **Connect** to validate the connection to the RPS server in Cloud Hybrid.
6. From the Plan drop-down list, select the Replication plan from the Cloud Hybrid RPS server.

   Note: The selected plan is the Share Plan from the Cloud Hybrid RPS server for your company.
7. Click **Save** and the data is replicated after the next backup.

   By default, node replication begins after the backup completes and the recovery points from the nodes are replicated to the Cloud Hybrid RPS server. To modify the schedule, you can add a Replication schedule.

Download/Recover Files and Folders from Cloud Hybrid

In Arcserve UDP Windows/Linux Agent browser, you can download the data from Cloud Hybrid.

This section contains the following topics:

- How to Download Files and Folders from Cloud Hybrid Using Microsoft Windows File Systems
- How to Recover Files and Folders from Cloud Hybrid

How to download Files and Folders from Cloud Hybrid Using Windows File Systems

Cloud Hybrid lets you download the files and folders from Windows File Systems using the following method:

Follow these steps:

1. Open Cloud Hybrid through the browser of Windows file system.
2. Expand **Destinations** menu available in the left pane and select the **Recovery Point Servers** option.
3. Select the recovery point server that you want to download the file/folder from.
4. Double click on the required recover point server.

   The data store list appears.
5. Right click on the specific data store and click **Browse Recovery Points**.

   The **Summary** page of the data store appears and displays the node(s) protected based on the plans assigned to the specific node.
6. Double click on the required plan and select the required node.
7. Right click on the specific plan and click **Restore**.

   The **Restore** wizard opens for the selected node.
8. Click the **Browse Recovery Points** option.

   The **Browse Recovery Points** dialog opens.
9. Select the recovery point (date and time) for the backup image that you need to download the file/folder from.
10. Expand the volume to browse the file/folder.

    Note: You need to input the session password if prompted.
11. Click the download icon.

    Note: The file is downloaded as original file and folder is downloaded as a zip file.

The selected file/folder for Windows file system is downloaded successfully.

How to Recover Files and Folders from Cloud Hybrid

Arcserve provides the ability to restore your data from Cloud Hybrid to a mounted recovery point created on your local Arcserve UDP Console using an SFTP client.

Follow these Steps:

1. Connect to the Arcserve UDP Console server SFTP client, such as FileZilla, performing the following steps:
    a. Create a new site to connect to Arcserve UDP Console server SFTP client, such as FileZilla.
    b. Specify the Arcserve UDP Console server name, user name, and password provided in your Welcome email.

    Note: Specify the default port number - 37037.
    c. Click **Connect**.
2. Perform the following steps to mount a recovery point:
    a. Minimize the SFTP client.
    b. Open Cloud Hybrid.
    c. From the **destinations** menu available in the left pane , select the **Recovery Point Servers** option.
    d. Select the required recovery point server to recover the data.
    e. Double click on the required recovery point server.

    The data store list appears.
    f. Right click on the specific data store and click **Browse Recovery Points**.

    The **Summary** page of the data store appears and displays the protected nodes based on the plans assigned to the specific node.
    g. Double click on the required plan and select the required node.
    h. Right click the selected node and click **Restore**.

    The Restore wizard appears for the selected node.
    i. Close the Restore dialog and select **Mount Recovery Point** from **Tasks** pane.

    The information about data store and node is displayed.
    j. Select the calendar date for the backup image that you want to mount.
    k. Select the recovery point that you want to mount.

l. Locate the volume or drive that you want to mount and click **Mount**.

Note: You can mount the drive to volume Z.

m. Specify the encryption password and click **OK**.

The selected volume is mounted and displayed in the list of Mounted Volumes on the **Mount Recovery Point** dialog.

3. Perform the following steps to recover files and folders from Cloud Hybrid using the recovery point mounted on volume Z:

   a. Open the SFTP client and select the site you created to connect to the mounted recovery point.

   b. Select the files or folders from Cloud Hybrid to recover by dragging them to the mounted recovery point.

The files and folders are recovered from Cloud Hybrid.

Create a Plan to protect Microsoft Office 365 data to Cloud Hybrid

The Microsoft Office 365 Exchange Protection is used to backup and restore Microsoft Exchange Online mail folders and items. To protect your Exchange online content, you need to create a Plan.

For more information, see How to Create an Exchange Online Plan.

The Microsoft Office 365 SharePoint Protection is used to backup and restore Microsoft SharePoint Online site and list item. The SharePoint Online is one of the major products in Microsoft Office 365. To protect your SharePoint content, you need to create a Plan.

For more information, see How to Create a SharePoint Online Backup Plan.

The Microsoft Office 365 OneDrive Protection is used to backup and restore Microsoft OneDrive files and folders items. The OneDrive is one of the major products in Microsoft Office 365. To protect your OneDrive content, you need to create a Plan.

For more information, see How to Create a Microsoft Office 365 OneDrive Node Backup Plan.

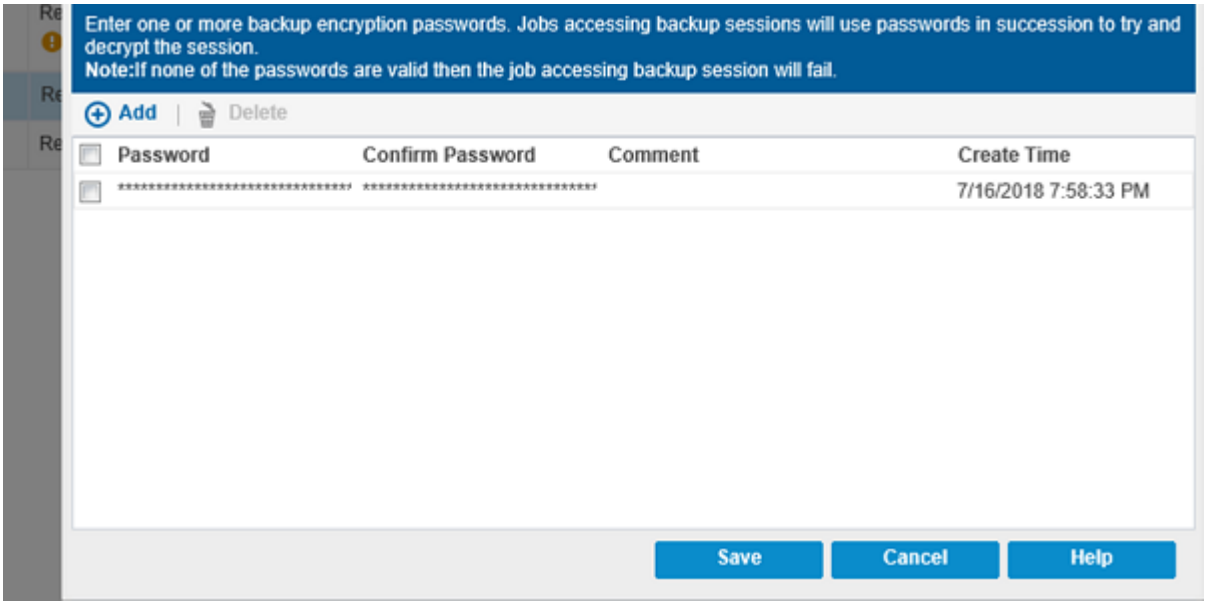
How to Perform Assured Recovery using Instant Virtual Disk

Follow these steps:

1. Log into the Arcserve UDP Console available in Cloud Hybrid and create an Assured Recovery task.
2. Navigate to the **Resources** tab, **Nodes/All Nodes** and select the node for the Assured Recovery task to set the backup password.

   Note: You must set the backup password for Virtual Standby and Restore tasks to ensure the conversion of replicated recovery points. The backup password provided is same as the session password defined in the plan used to backup the on-premise source nodes.
3. Right-click the node and from the displayed options select **Set Backup Passwords**.

   The **Set Backup Passwords for Node XXX** dialog is displayed.



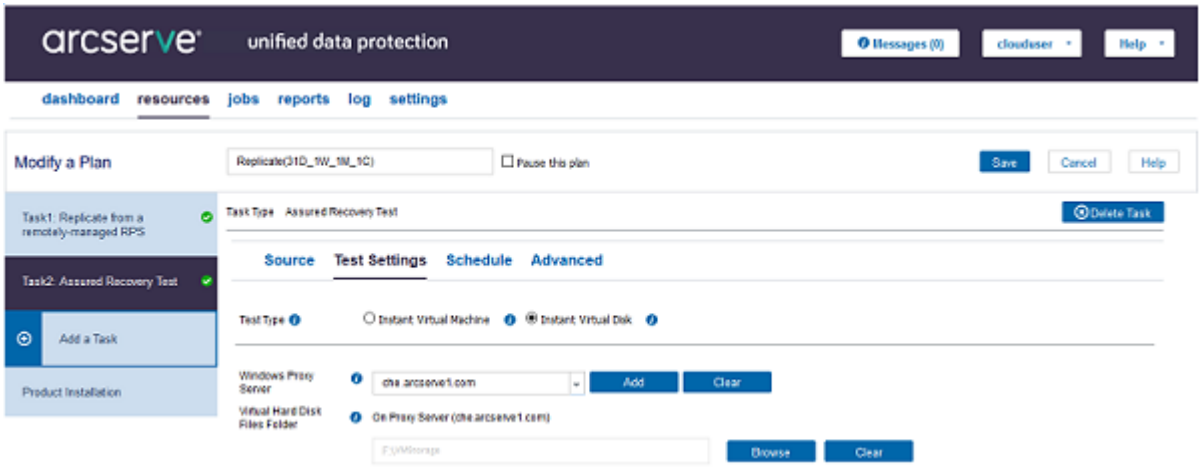
4. Add backup passwords and then click **Save**.
5. From the **Resources** tab, select **Plans/All Plans**.
6. Edit the Replication plan to add Task 2 as the Assured Recovery task.

   Note: You can add multiple backup passwords.
7. Specify the Source and select the types of Recovery Points required for Assured Recovery test.

   Note: You can select the backup types or the latest recovery points.

8. Navigate to the **Test Settings** tab.
9. Specify the Task Setting for Test Type as Instant Virtual Disk and specify the following details:
   - **Windows Proxy Server:** Enter the FQDN of Cloud Hybrid
   - **Browse the Virtual Hard Disk Files Folder:** F:\VMStorage

     Note: If the above mentioned path is not available, create the VMStorage folder manually in the F: drive.



10. Specify the **Schedule** settings required.
    Note: Custom command in advanced settings is not supported as we cannot access the proxy server.
11. Click **Save**.

The modifications are saved successfully and the Assured Recovery task is automatically deployed. After the replication job, the Assured Recovery jobs are performed automatically and are controlled using the schedule settings.

More information:

Performing Assured Recovery Test Manually for a Node

Performing Assured Recovery Test Manually for a Plan

Recover Protected Microsoft Office 365 Data from Arcserve UDP Cloud Hybrid

This section contains the following topics:

How to Restore Microsoft SharePoint Online Site Collection Data

You can restore SharePoint Online List/Library or List item in Site. The Site Collection and Site are not supported yet in Arcserve UDP v6.5. You can restore the data to original site using new name, restore the data to original location, and export to disk from the recovery points.

For more information, refer How to Restore SharePoint Online Site Collection Data.

How to Restore Microsoft Office 365 Exchange Mailbox Data

You can restore Exchange Online mailbox data such as emails, calendars, contacts, notes, tasks, and so on from the Microsoft Cloud. You can restore the data to original or alternate location.

For more information, refer How to Restore Exchange Online Mailbox Data.

How to Restore Microsoft OneDrive Data

You can export Microsoft OneDrive files and folders to local disk. You can restore using the restore option. For more information, see How to Restore Microsoft OneDrive Data.

You can also restore using the Mount Volume option from the agent user interface. For more information, see How to Recover Files and Folders from Cloud Hybrid.

Chapter 3: Using Cloud Hybrid as a Disaster Recovery Service

Important! To use Cloud Hybrid Compute Service, you need to have a backup available in the Cloud Hybrid RPS already. For more information, refer How to Replicate Data to the Cloud Hybrid Recovery Point Server.

This section contains the following topics:

How to Download Files and Folders from Cloud Hybrid Using Linux File Systems

Cloud Hybrid lets you download the files and folders from Linux File Systems.

Note: For Cloud Hybrid BaaS, the Linux file restore is possible from Cloud Hybrid through manual reverse replication.

Follow these steps:

1. Open Arcserve UDP Agent for Linux web interface in the browser of Linux file system.
2. Click **Restore** from the **Wizard** menu and select **Mount Recovery Point**.

   Restore Wizard – Mount Recovery Point opens.
3. Select the data store and node from the drop-down list.
4. Click **OK**.
5. Select the recovery point (date and time) for the backup image.
6. Select **WebDAV** option from the **Share Recovery Point Using** drop-down list.
7. Set username/password and submit the mount job.
8. Open the URL and download file.

   Your download URL will be *https://<your-cloudhybrid-FQDN>:8018/share/<username for mount>/*

The selected file/folder for Linux file system is downloaded successfully.

Run Disaster Recovery Systems in Cloud Hybrid Using Virtual Standby

This section contains the following topics:

How to Use the Hyper-V Server in Disaster Recovery System

Due to the same server configuration available for Hyper-V server and Arcserve UDP server, the following considerations helps you create the virtual machines for the Hyper-V server without affecting the Arcserve UDP server:

- Use the *F:\VMStorage* folder to store the virtual machines as the remaining drives are reserved for operating system and Cloud Hybrid. The default virtual machine path is set to *F:\VMStorage*.
- Use *Arcserve_Private_Cloud* network that helps the virtual machine to get the IP address from DHCP.
- You need to reserve memory for Arcserve UDP data store usage as the system memory is consumed for running the virtual machines. To monitor the system memory usage, navigate to the Data Store page.

How to Recover Data in the Cloud Hybrid Using Virtual Standby

Arcserve provides the ability to power on the standby virtual machines running in Cloud Hybrid using Virtual Standby task.

Note: For details about Hypervisor, contact Arcserve support.

Follow these steps:

1. Log into the Arcserve UDP cosnsole available in the Cloud Hybrid to set up your Virtual Standby task.

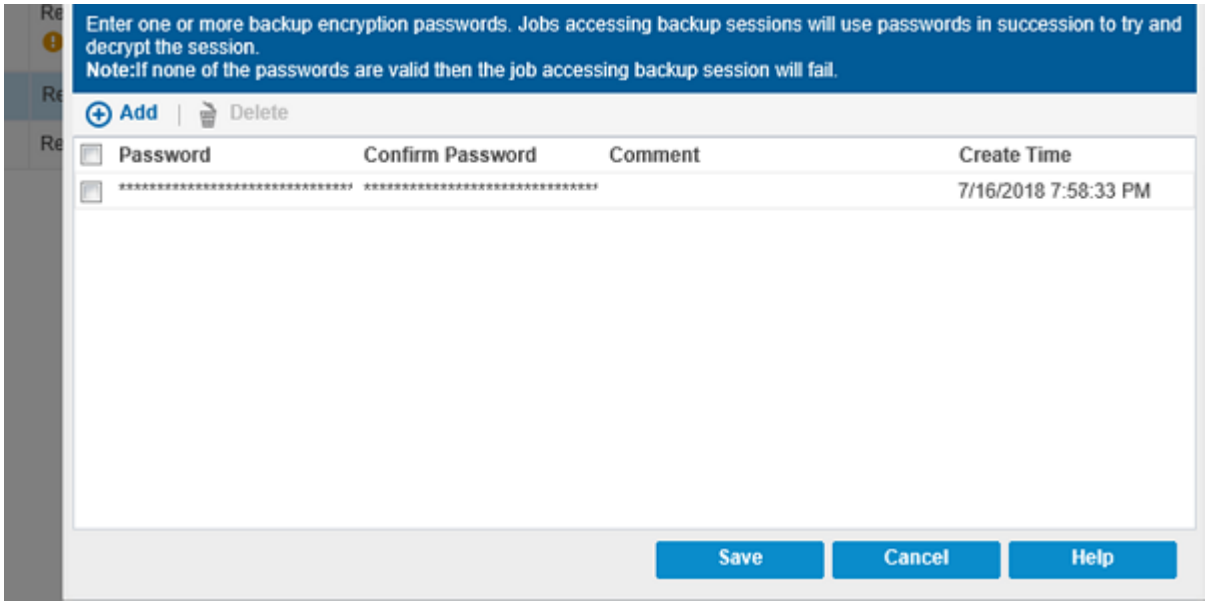
   Note: For more information related to the login of Cloud Hybrid, refer to the Welcome email.

2. Navigate to the **Resources** tab, **Nodes/All Nodes** and select the node for the Virtual Standby task to set the backup password.

   Note: You must set the backup password for Virtual Standby and Restore tasks to ensure the conversion of replicated recovery points. The backup password provided is same as the session password defined in the plan used to backup the on-premise source nodes.

3. Right-click the node and select **Set Backup Passwords**.

   The **Set Backup Passwords for Node XXX** dialog is displayed.



4. Add one or more backup passwords and then click **Save**.
5. From the **Resources** tab, select **Plans/All Plans**.
6. Edit the Replication plan to add Task 2 as the virtual standby.

7. In the **Virtualization Server** tab, enter the following details:

   Virtualization Type: Hyper-V

   Hyper-V Host Name: Enter the Cloud Hybrid FQDN/IP address

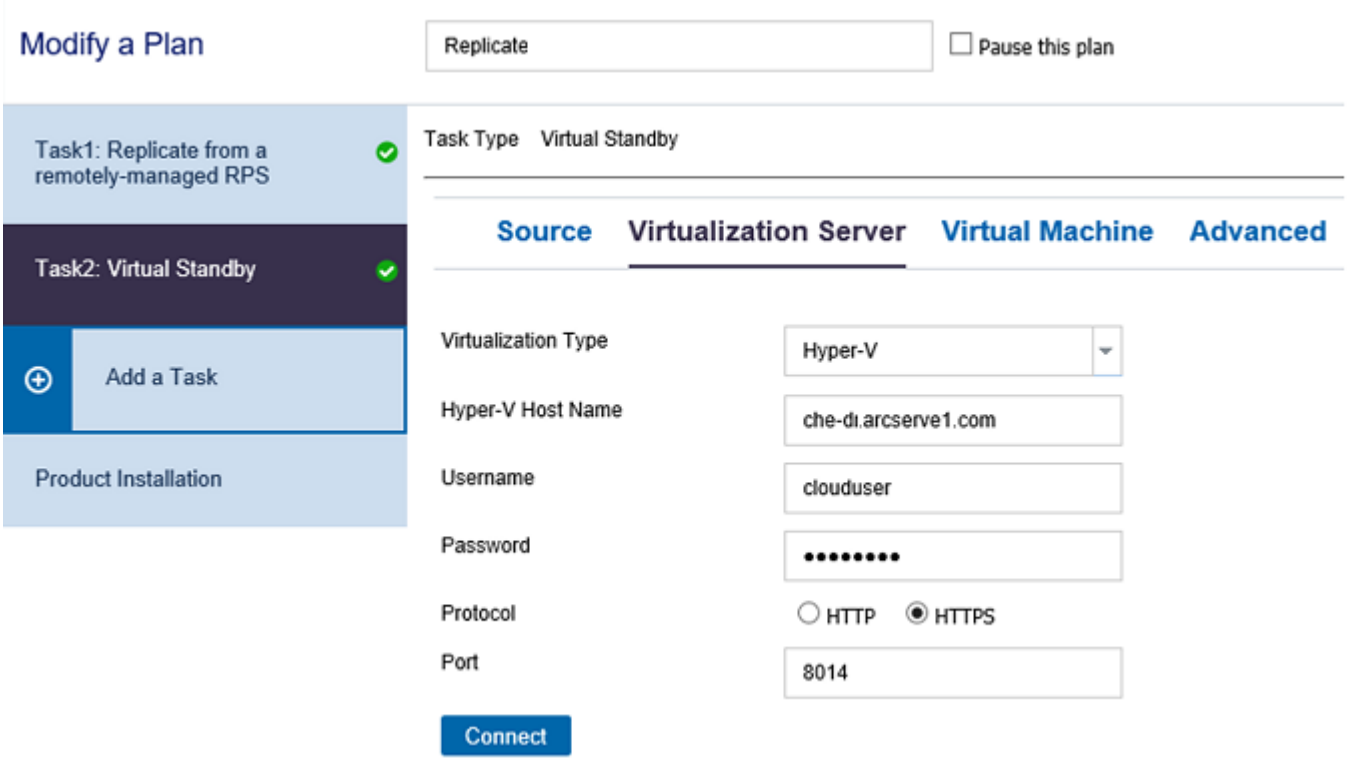
   Username: Enter the Cloud Hybrid username

   Password: Enter the Cloud Hybrid password

   Protocol: HTTPS

   Port: 8014

8. Click **Connect**.



9. In the **Virtual Machine** tab, enter the following information:

   a. Specify appropriate CPU count and memory required for the virtual standby VM.

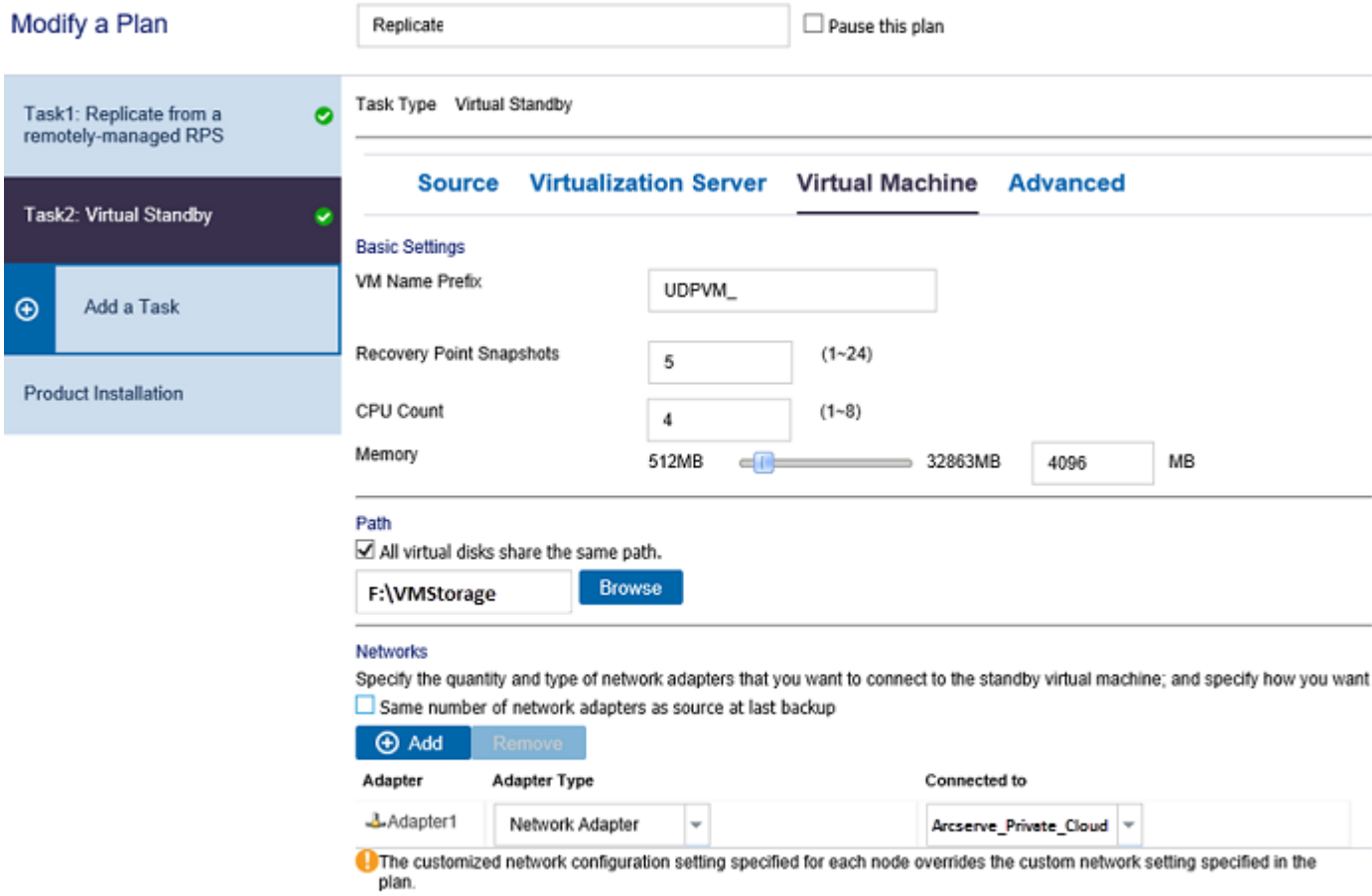
      Note: Specify the CPU count and Memory allocation based on the Cloud Hybrid Compute subscription purchased.

   b. You must specify the following path for the virtual standby VM on Hyper-V:

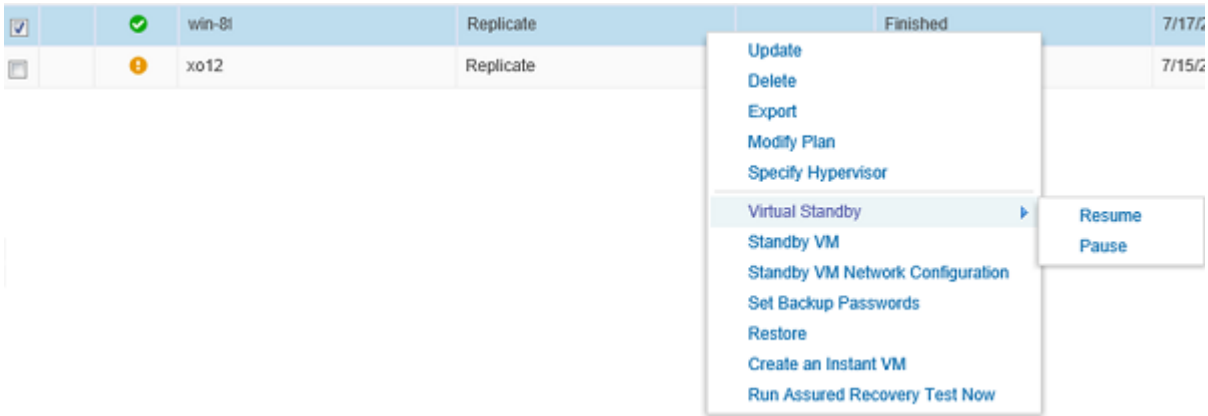
      F:\VMStorage

      Note: Do not uncheck the *All virtual disks share the same path* option as the above mentioned path is used for all the virtual disks.

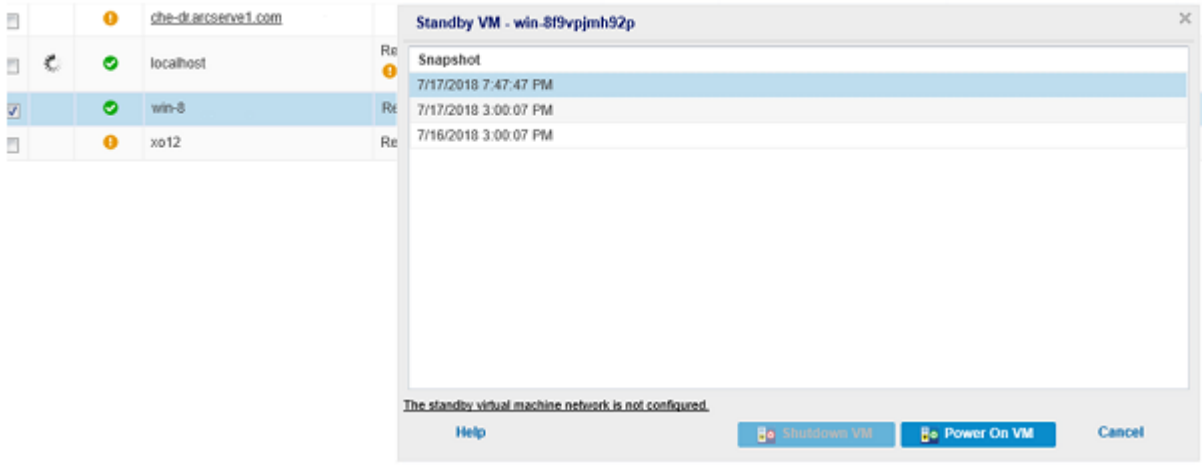
c. To specify networks, select **Network Adapter** from the *Adapter Type* drop-down list and **Arcserve_Private_Cloud** from the *Connected to* drop-down list to connect to network.



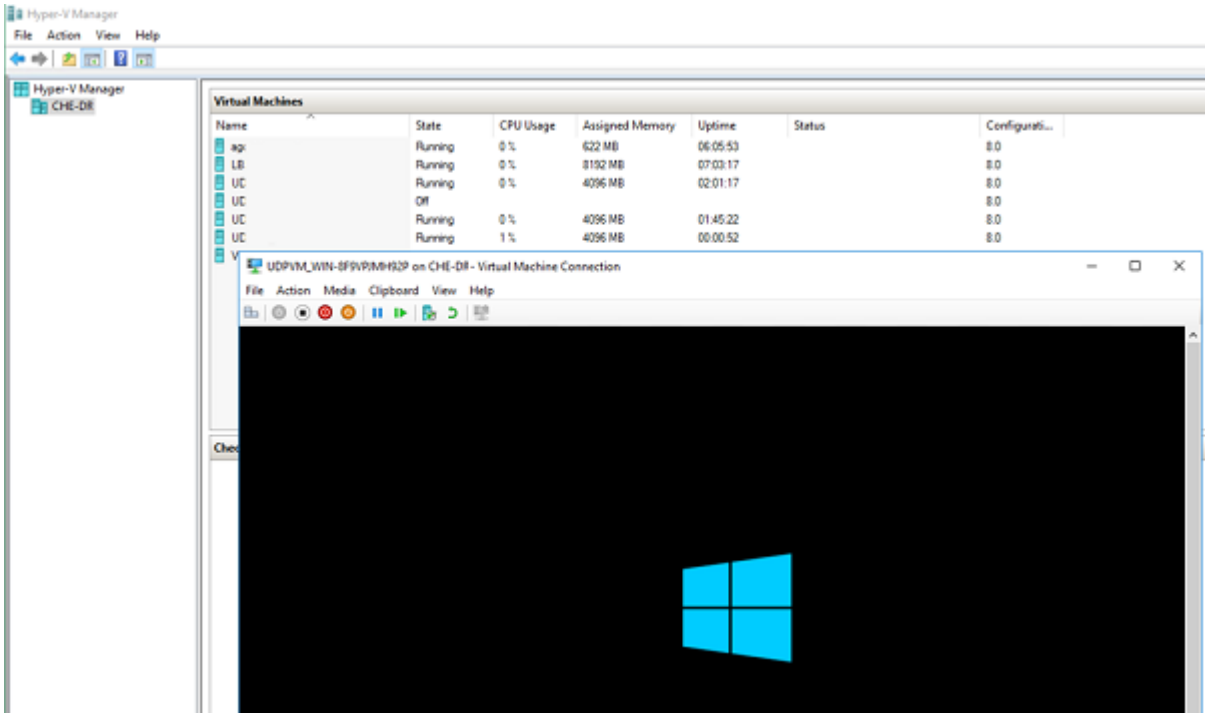
10. Right click on the replication plan and from the displayed options select **Pause and resume** to start the recovery point conversion for all nodes attached to the Hyper-visor on the recovery node.



11. After Cloud Hybrid Virtual Standby (Task 2) completes converting the recovery points to virtual machines, start or stop the Cloud Hybrid Virtual Standby VM from the Virtual Standby menu placed on the left pane of the Arcserve UDP Console and configure the virtual machine network on the Virtual Standby User Interface available in the Cloud Hybrid.



12. Click **Power On VM**.



The Virtual Standby VM is now up and running.

More information:

Protecting the Production Virtual Standby VM Running in the Cloud Hybrid

Protecting the Production Virtual Standby VM Running in Cloud Hybrid

Cloud Hybrid lets you protect the production Virtual Standby machine running in Cloud Hybrid.

Follow these steps:

1. Log into the Arcserve UDP Console available in the Cloud Hybrid.
2. Specify the IP address for the Hypervisor provided in your Welcome email to add or discover the Virtual Standby VMs or nodes.
3. Use **Task 1** to create a new plan (For example, Cloud Backup plan) using an Agentless Backup.

   Note: To avoid inadvertent recovery points, consider removing the production node from the local job.
4. Add the nodes from the Hypervisor.
5. Use the RPS data store in Cloud Hybrid as the destination.
6. Review the **Schedule** tab and other settings for the backup job.
7. Click **Save**.

   The production Virtual Standby machine is protected successfully.

Recovering the Production Virtual Standby VM Running in the Cloud Hybrid to a Local Server

You can rebuild or restore Virtual Standby machines running in Cloud Hybrid to your local environment. Replicate the Virtual Standby machines on the onsite On-premise RPS and restore from the latest/closest state with all the modifications present.

Follow these steps:

1. Perform a backup of the Virtual Standby VM to ensure data integrity.

   Note: We recommend to shut down the Virtual Standby VM till the local node is recovered.

2. Add the **Replicate task to a remotely-managed RPS** task to replicate your backup data to the On-premise RPS.
3. Perform BMR (Bare Metal Recovery) to recover the VM.
4. Add the local server back to the production backup job.

   The Virtual Standby VM is now recovered on your local server.

Run Disaster Recovery Tests in Cloud Hybrid Using Instant VM

This section contains the following topics:

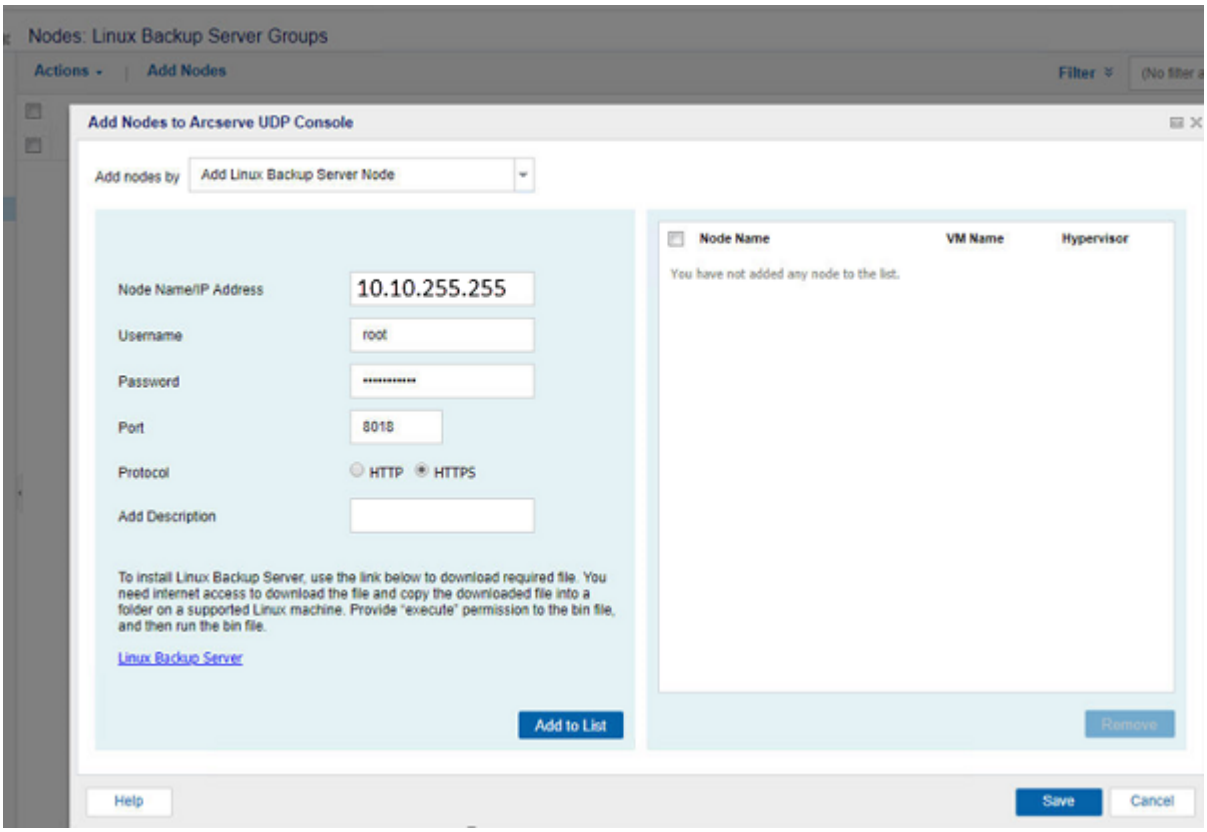
How to Add Linux Backup Server in Cloud Hybrid

Follow these steps:

1. Log into the Arcserve UDP Console available in Cloud Hybrid.
2. From the left pane, select **All Nodes**.

   The list of nodes appear on the center pane.
3. Click **Add Nodes**.

   The **Add Nodes to Arcserve UDP Console** dialog appears.
4. From the **Add nodes by** drop-down list, select **Adding Linux Backup Server Node**.



5. Enter the following Linux backup server node details:

   Node Name/IP Address : Public IP of Cloud Hybrid

   Port : 8018

   Protocol: https
6. Click **Add to List**.

   The node is added to the right pane.

7. (Optional) To remove the added node, select the node in the right pane and click **Remove**.
8. Select the nodes to add and click **Save**.
9. Navigate to **Nodes** and select **All Nodes** to view the added node.

The nodes are added successfully.

How to Create Cloud Hybrid Instant Virtual Machine

Instant virtual machine (Instant VM) creates a virtual machine in the Hypervisor and runs the backup session inside the virtual machine without any prior conversion.

Advantages of Instant virtual machine:

- Provides immediate access to data and applications available in the Arcserve UDP backup sessions.
- Eliminates the downtime associated with a traditional restore or conversion of the backup session to a physical or virtual machine.

You can create an Instant VM from the following backup sessions on the RPS server in Cloud Hybrid:

- Agent-based Windows backup
- Agent-based Linux backup
- Host-based agentless backup

To create an Instant VM:

1. Opening the Instant VM wizard in Cloud Hybrid
2. Configuring an Instant VM using the Instant VM Wizard for Windows System
3. Configuring an Instant VM using the Instant VM Wizard for Linux System
4. Creating the Instant VM

Opening the Instant VM Wizard in Cloud Hybrid

You can configure and create an Instant VM using the Instant VM wizard in Cloud Hybrid. Open the Instant VM wizard using either of the two options:

- How to Open the Instant VM Wizard Using Node Management
- How to Open the Instant VM Wizard Using Destination Management

How to Open the Instant VM Wizard Using Node Management

Using nodes available in Cloud Hybrid, you can open the Instant VM wizard.

Follow these steps:

1. Open the Wizard from the RPS Console Node management view in Cloud Hybrid.
2. Click the **resources** tab.
3. From the left pane, select the proper site and then navigate to **Nodes** and click **All Nodes**.

   All the nodes are displayed on the center pane.
4. Right-click a node and from the displayed options select **Create an Instant VM**.

   Note: The **Create an Instant VM** option works only when the node is associated with at least one plan.

   The Instant VM wizard opens.

How to Open the Instant VM Wizard Using Destination Management

Using destinations available in Cloud Hybrid, you can open the Instant VM wizard.

Follow these steps:

1. Open the Wizard from the RPS Console Destination management view in Cloud Hybrid.
2. Navigate to **Destinations**: **Recovery Point Server**.
3. Click the **resources** tab.
4. From the left pane, select the required site, navigate to **Destinations** and click **Recovery Point Servers**.

   Previously added data stores are displayed in the center pane.
5. Click the required data store.

   If you have already backed up data to the RPS, all the source nodes are listed in the pane.
6. Right-click a node and select **Create an Instant VM**.

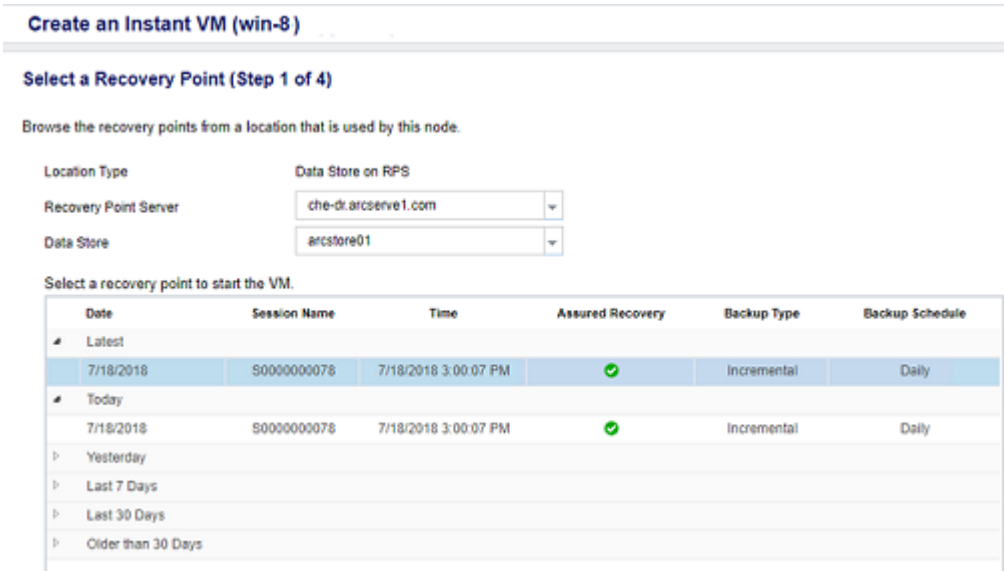
   The Instant VM wizard opens.

Configure an Instant VM using the Instant VM Wizard for Windows System

Using the Instant VM wizard, you can configure the Instant VM by entering details before creating. Follow these steps to configure the Instant VM:

1. **Select a Recovery Point**

   The Console will automatically recognize the location of the recovery point and pre-selects the Location Type, Recovery Point Server in Cloud Hybrid, and Data Store.



   Expand the Date list, select the required recovery point from the list, and click Next. The VM Location page opens.

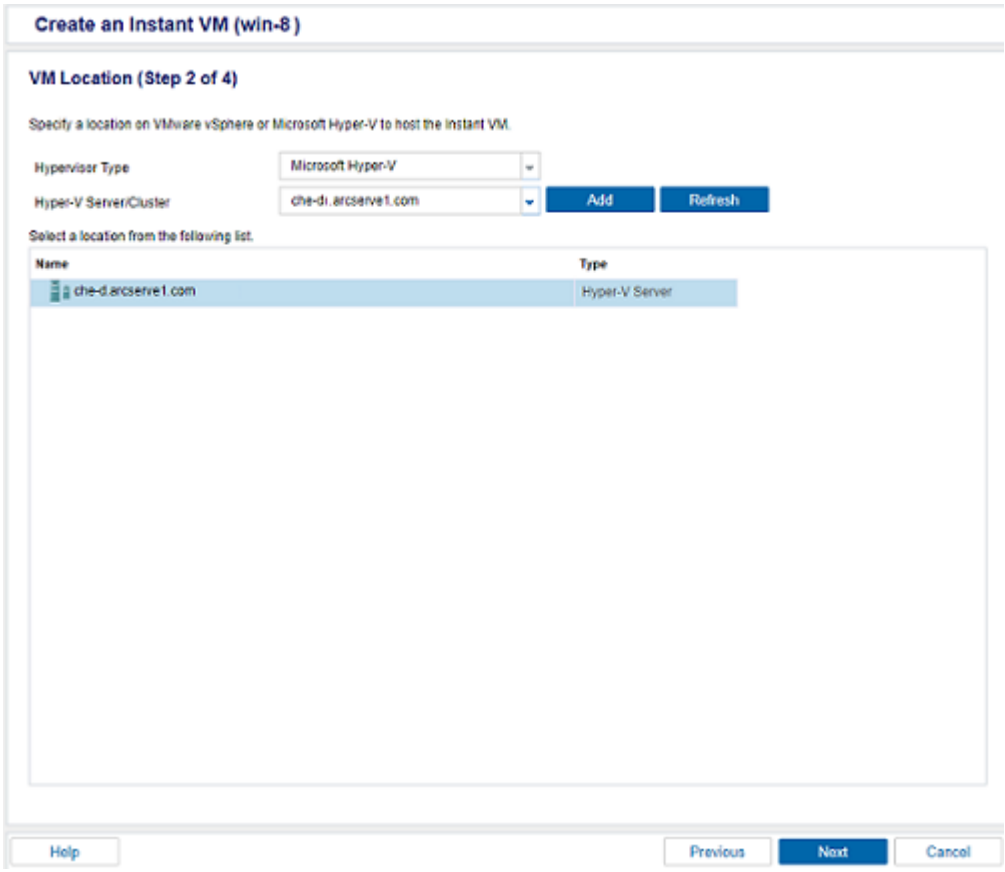
2. **Select a VM Location**

   Specify the location of the virtual machine where you want to create the Instant VM. You can specify Microsoft Hyper-V virtual machine in Cloud Hybrid.

   Follow these steps:

   a. Select Hyper-V as the Hypervisor Type and click **Add**.

   b. In Specify the VM Destination dialog, specify the Hyper-V server's IP address and credentials provided in you Welcome email and click **OK**.



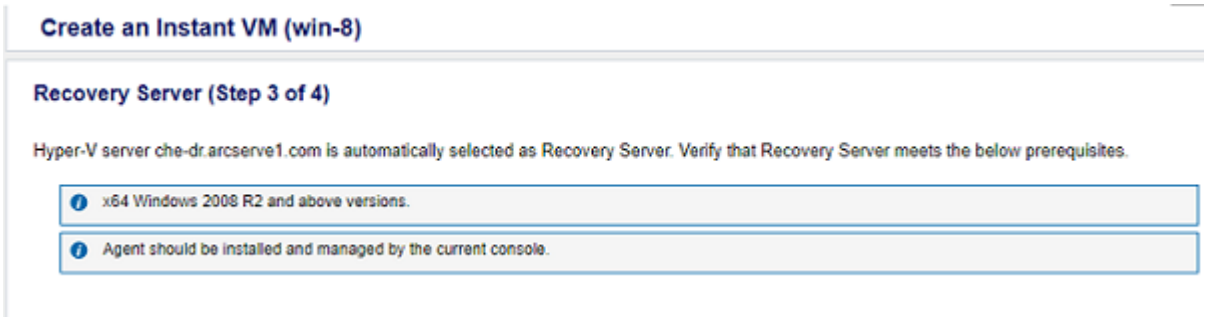
c. Click **Next**.

The Recovery Server page opens.

3. **Select a Recovery Server**

   The recovery server hosts the core module of the Instant VM. The default recovery server is the Hyper-V provided to you in Cloud Hybrid.

   For Linux backup sessions, the recovery server is the Linux Backup Server provided to you in the Arcserve Business Continuity Cloud.



   Click **Next** and The Instant VM Details page opens.

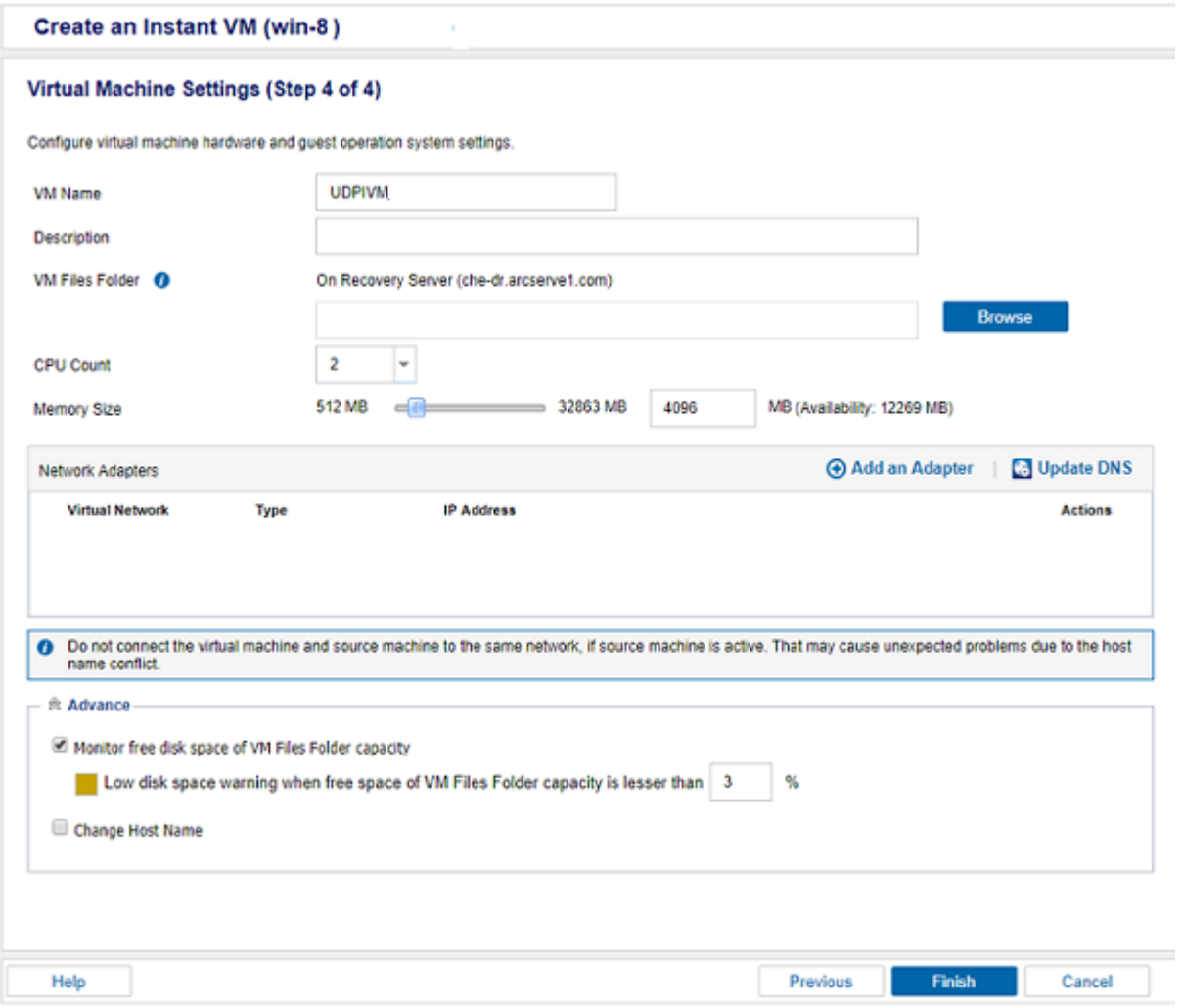
4. **Specify the Instant Virtual Machine Details**

Follow these steps:

a. Specify the name and description of the Instant VM.

b. Specify the folder location of the Instant VM on the recovery server. You must specify the following path for the Hyper-V disks location:

F:\VMStorage

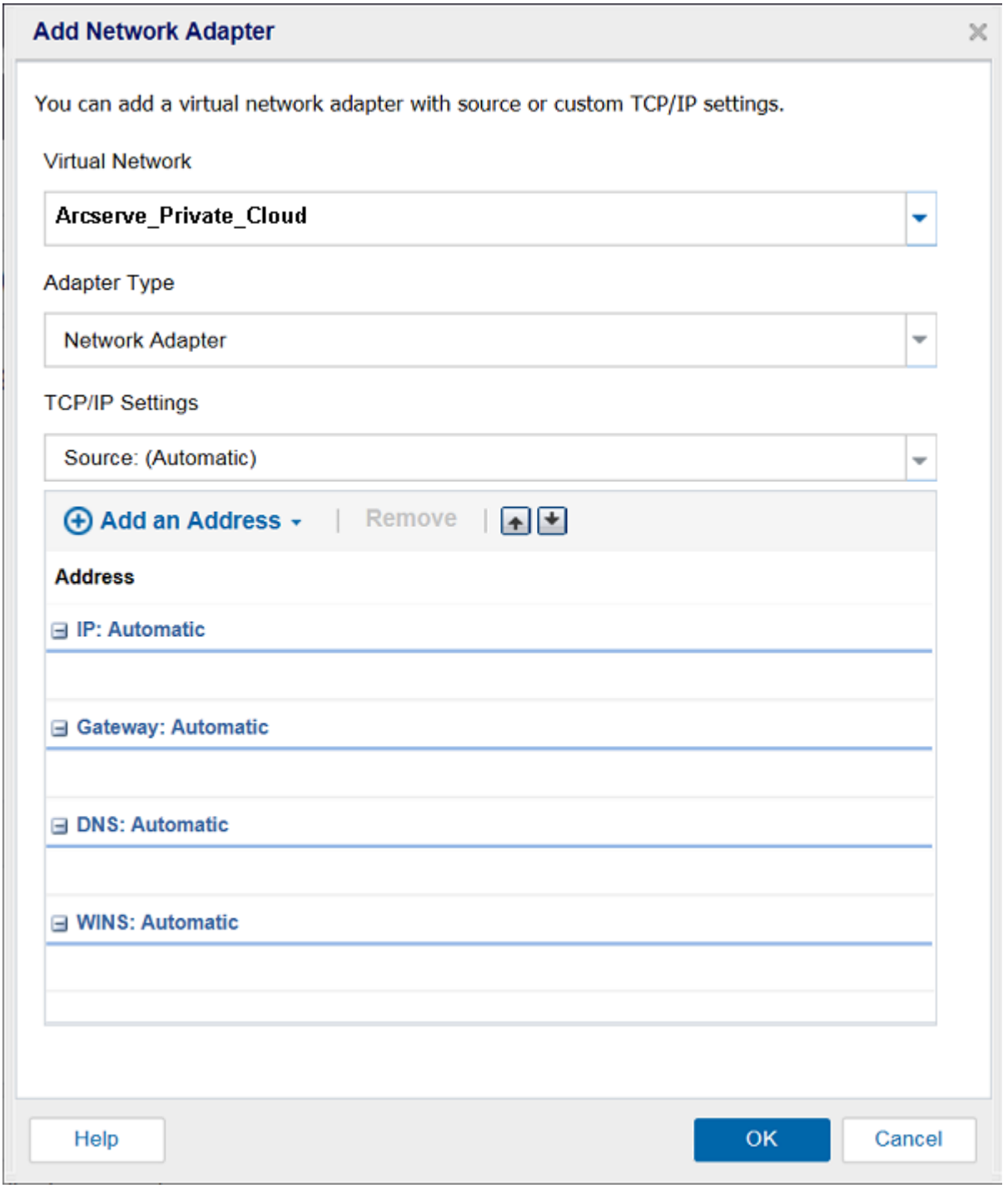


c. Specify the following Instant VM settings:

- CPU Count that specifies the number of CPU required in the Instant VM.
- Memory Size that specifies the size of memory required in the Instant VM.

  Note: Specify the CPU count and Memory allocation based on the Cloud Hybrid Compute subscription purchased.

d. To specify networks, select **Arcserve_Private_Cloud** from the *Virtual Network* drop-down list and **Network Adapter** from the *Adapter Type* drop-down list to connect IVM to network.



e. Click **OK**.

f. We recommended to select the *Monitor free disk space of VM Files Folder capacity* checkbox.

g. (Optional) Modify the Instant Virtual Machine hostname.

Now, you are ready to submit the job and create the Instant VM.

Configure an Instant VM using the Instant VM Wizard for Linux System

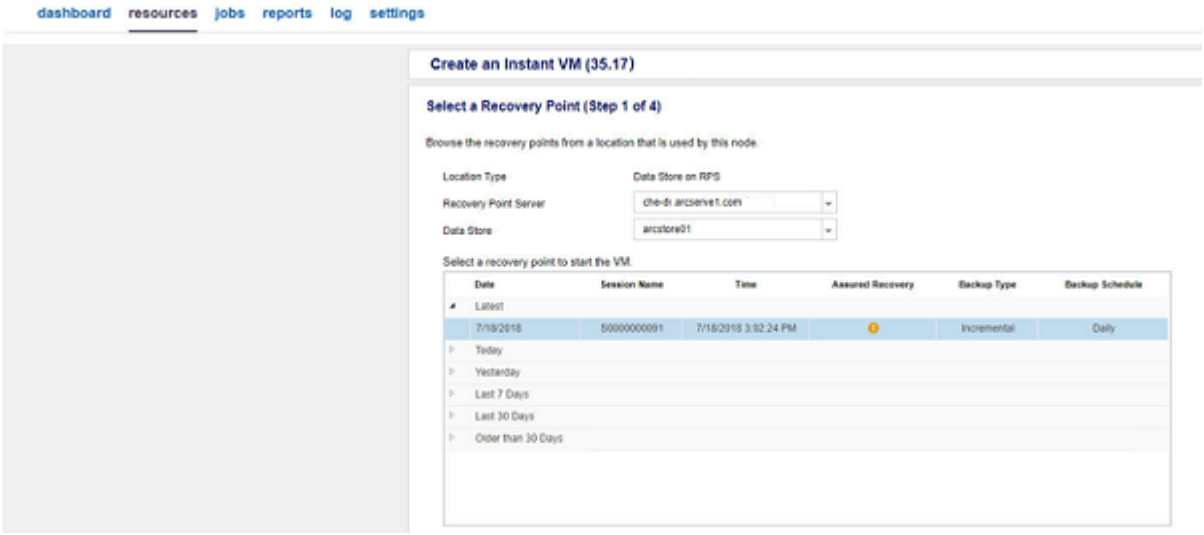
Using the Instant VM wizard, you can configure the Instant VM by entering details before creating. Follow these steps to configure the Instant VM:

1. **Add a Linux Backup Server**

   For more information, refer How to Add Linux Backup Server in Cloud Hybrid.

2. **Select a Recovery Point**

   The Console will automatically recognize the location of the recovery point and pre-selects the Location Type, Recovery Point Server in Cloud Hybrid, and Data Store.



   Expand the Date list, select the required recovery point from the list, and click Next.

   Note: If the backup session is encrypted, a password prompt appears.

   The VM Location page opens.

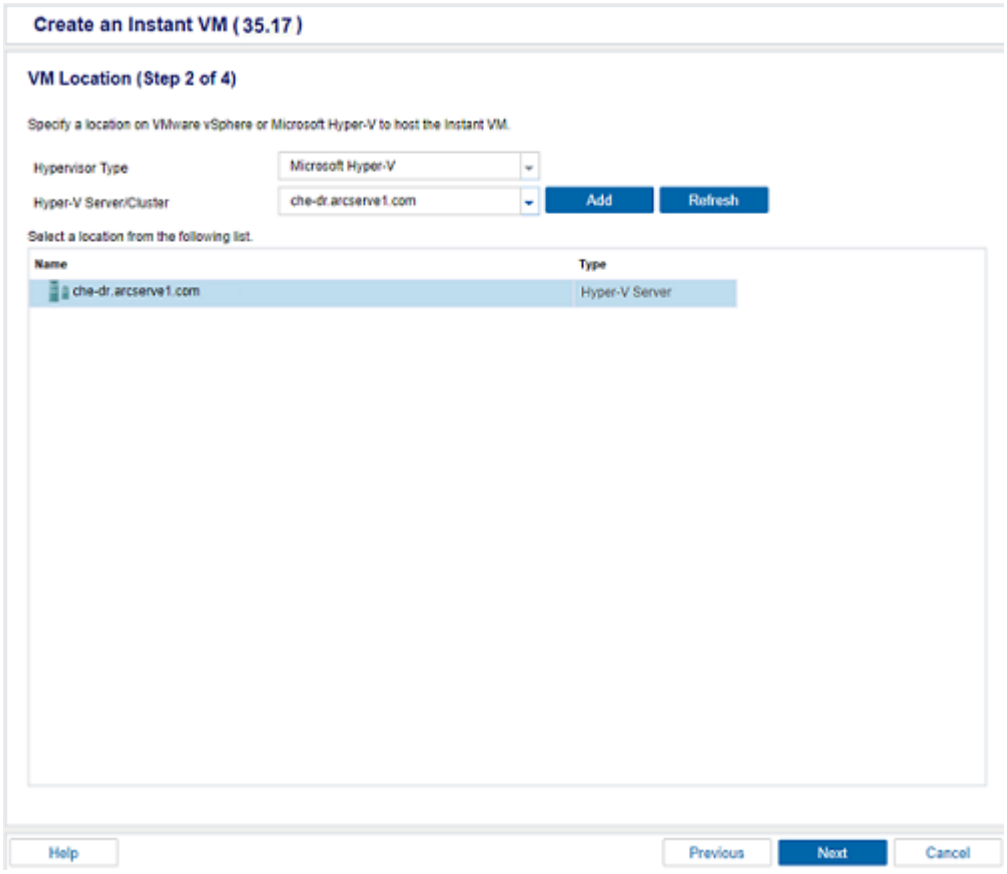
3. **Select a VM Location**

   Specify the location of the virtual machine where you want to create the Instant VM. You can specify Microsoft Hyper-V virtual machine in Cloud Hybrid.

Follow these steps:

a. Select Hyper-V as the Hypervisor Type and click Add button.

b. In Specify the VM Destination dialog, specify the Hyper-V server's IP address and credentials provided in you Welcome email and click **OK**.



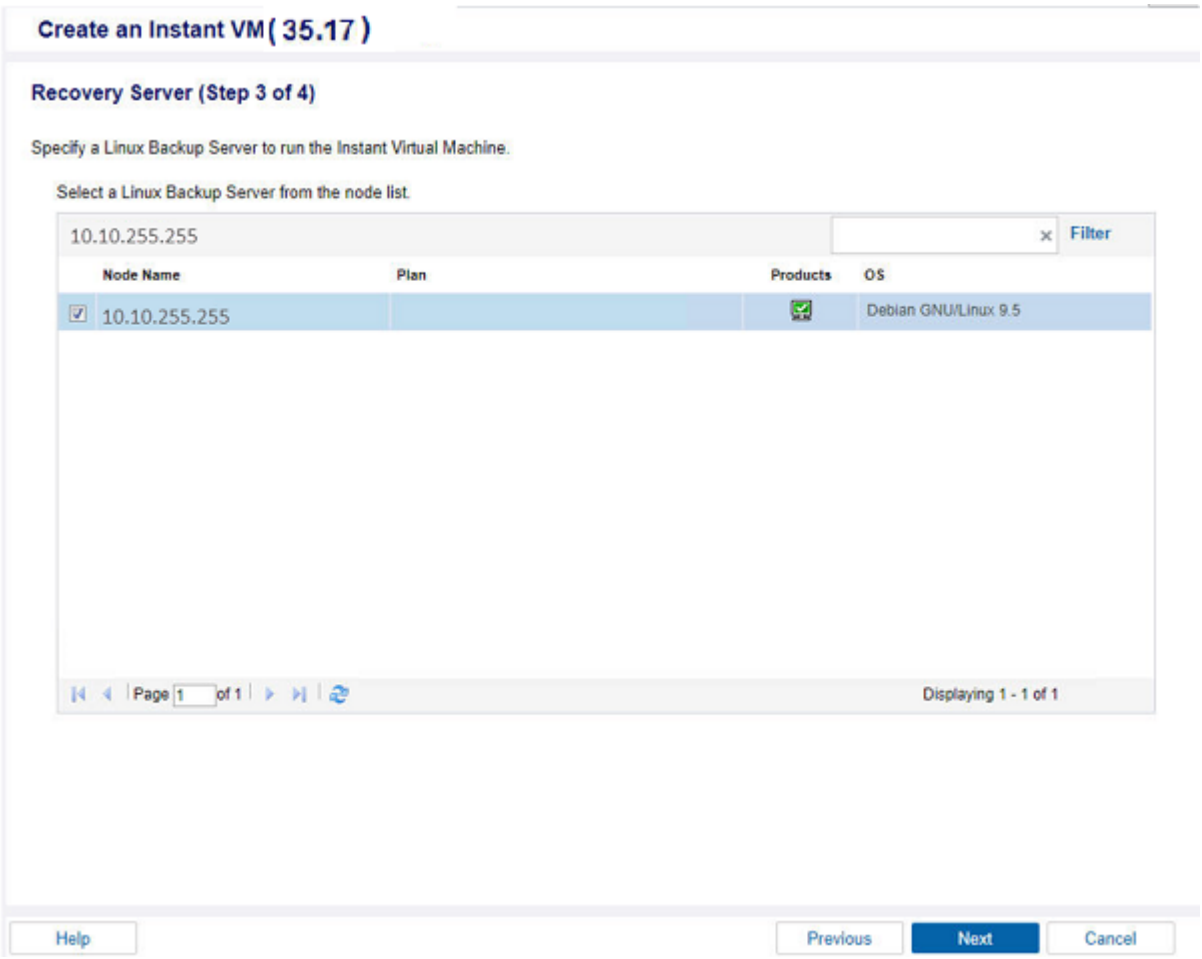
c. Click **Next**.

The Recovery Server page opens.

4. **Select a Recovery Server**

The recovery server hosts the core module of the Instant VM. The default recovery server is the Hyper-V provided to you in Cloud Hybrid.

For Linux backup sessions, the recovery server is the Linux Backup Server provided to you in the Arcserve Business Continuity Cloud.



Click **Next** and The Instant VM Details page opens.

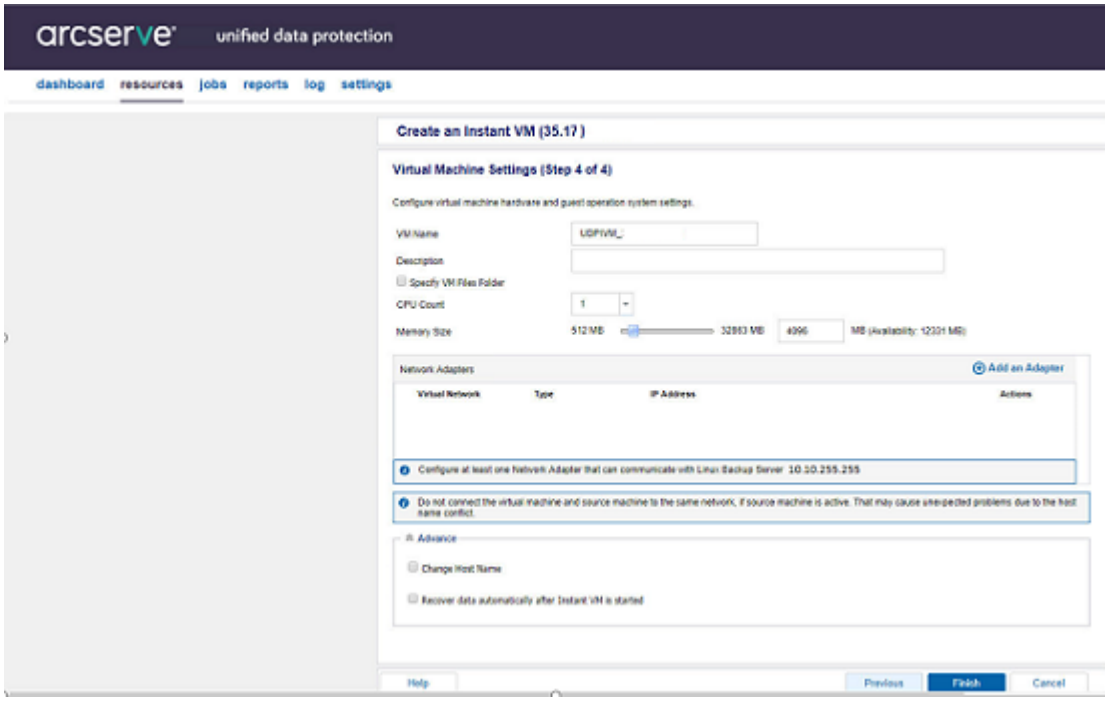
5. **Specify the Instant Virtual Machine Details**

   Follow these steps:

   a. Specify the name and description of the Instant VM.

   b. If the *Specify VM Files Folder* is selected, then specify the following path:

      F:\VMStorage

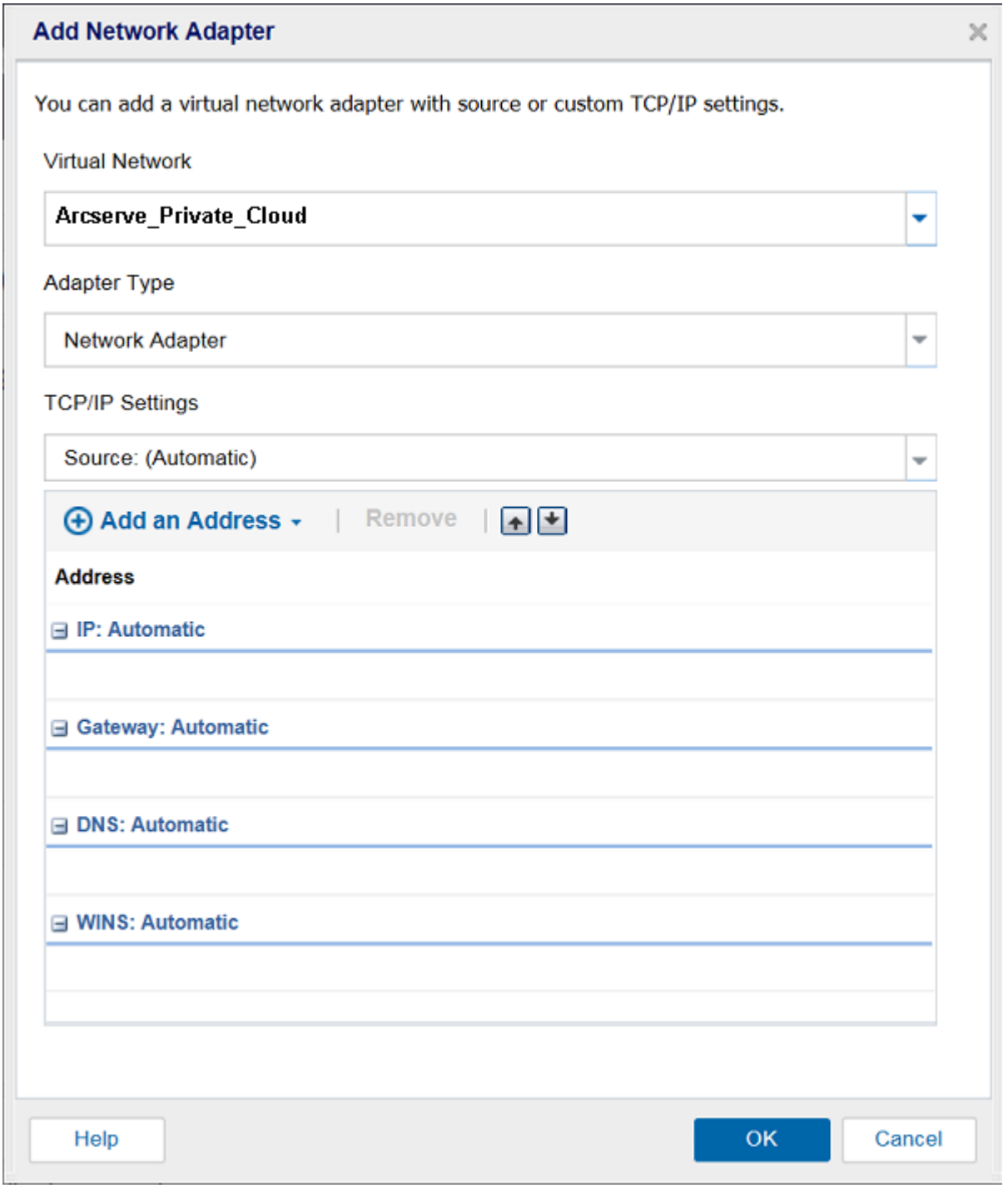


c. Specify the following Instant VM settings:

- CPU Count that specifies the number of CPU required in the Instant VM.
- Memory Size that specifies the size of memory required in the Instant VM.

  Note: Specify the CPU count and Memory allocation based on the Cloud Hybrid Compute subscription purchased.

d. To specify networks, select **Arcserve_Private_Cloud** from the *Virtual Network* drop-down list and **Network Adapter** from the *Adapter Type* drop-down list to connect IVM to network.



e. Click **OK**.

f. (Optional) Modify the Instant Virtual Machine hostname.

g. For host-based backup, we recommend to select the *Recover data automatically after Instant VM is restarted* to convert the Instant VM to an independent VM.

Now, you are ready to submit the job and create the Instant VM.

Note: The *Resume auto recovery* option for Linux Instant VM is applicable only for host based backup.

Create the Instant VM

When the configuration is complete, you can submit the created job in the previous step to create the Instant VM. After the job is complete, you can view the Instant VM at **resources**, **Infrastructure**, **Instant Virtual Machine**.

Follow these steps:

1. To submit, click **Create VM**.

   The Create VM dialog opens.

2. Select one of the following options:

   Boot Now

   Submits a job to create the Instant VM. After the VM is created, it automatically starts the VM.

   Boot Later

   Creates an Instant VM. You must manually start the VM. You can start the VM after the Instant VM job is complete.

   Cancel

   The **Create VM** dialog is closed without creating a VM and automatically redirects to the Create VM page.

   The Instant VM job is created successfully.

How to Manage Cloud Hybrid Instant Virtual Machine

You can manage the Instant VM from Cloud Hybrid. You can power-on or power-off and delete an Instant VM.

Note: Cloud Hybrid displays only the Instant VM that is created from the recovery points managed from the selected Site.

This section contains the following topics:

Start or Stop an Instant Virtual Machine

You can start or stop an Instant VM when created. The start or stop button appears according to the status of the VM.

Follow these steps:

1. From Cloud Hybrid, click **resources**.
2. Navigate to **Infrastructures** and click **Instant Virtual Machines**.
3. Select the required virtual machine from the center pane and click **Actions**.
4. Select **Power on** or **Power Off** according to the status of the virtual machine.

   The virtual machine successfully starts or stops.

Delete an Instant Virtual Machine

You can remove any Instant VM.

Follow these steps:

1. From Cloud Hybrid, click **resources**.
2. Navigate to **Infrastructures** and click **Instant Virtual Machines**.
3. Select the virtual machine from the center pane and click **Actions**.
4. Click **Delete**.

   A confirmation dialog opens.
5. Click **OK**.

   The virtual machine is successfully deleted.

Automate Disaster Recovery Tests in Cloud Hybrid Using Assured Recovery

This section contains the following topics:

How to Perform Assured Recovery of the Backup Data

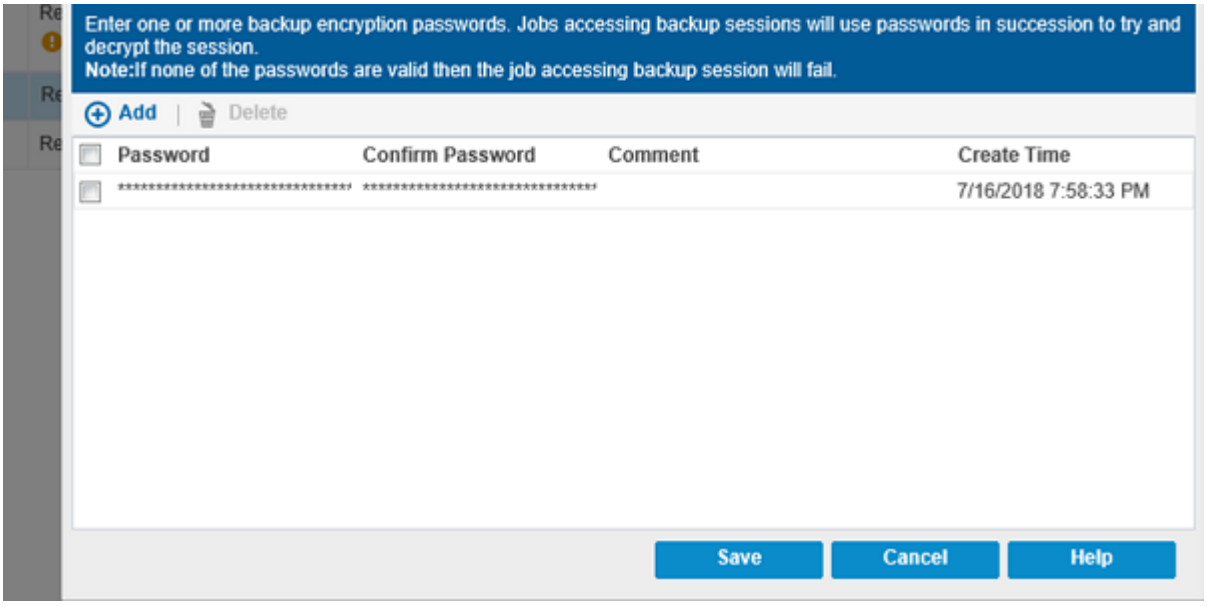
To verify accessibility and assured recovery of the data, create an assured recovery plan. The plan for assured recovery is based on the backup/replication plan.

Follow these steps:

1. Log into the Arcserve UDP Console available in Cloud Hybrid and create an Assured Recovery task.
2. Navigate to the **Resources** tab, **Nodes/All Nodes** and select the node for the Assured Recovery task to set the backup password.

   Note: You must set the backup password for Virtual Standby and Restore tasks to ensure the conversion of replicated recovery points. The backup password provided is same as the session password defined in the plan used to backup the on-premise source nodes.
3. Right-click the node and from the displayed options select **Set Backup Passwords**.

   The **Set Backup Passwords for Node XXX** dialog is displayed.



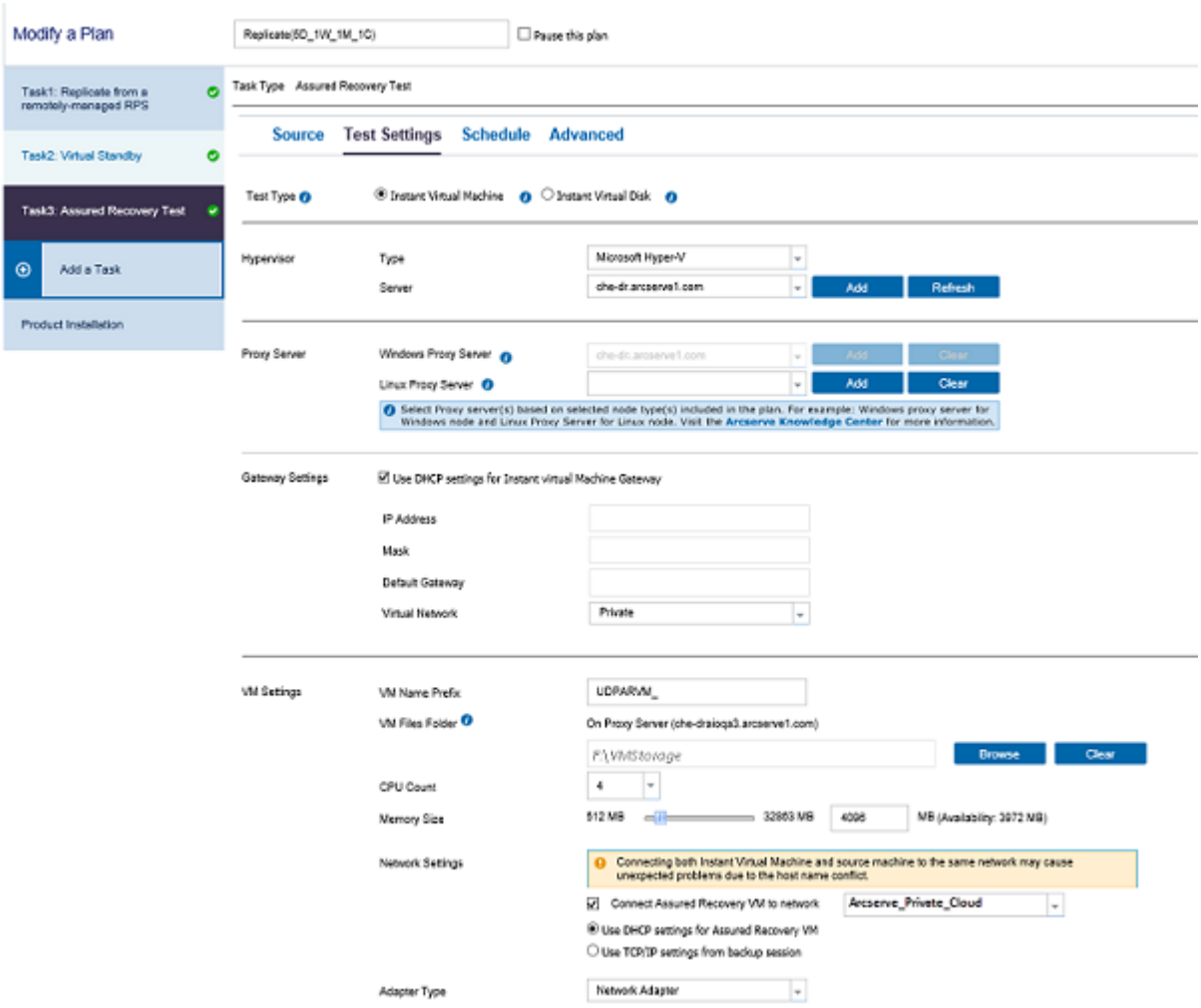
4. Add backup passwords and then click **Save**.
5. From the **Resources** tab, select **Plans/All Plans**.
6. Edit the Replication plan to add Task 2 as the Assured Recovery task.

   Note: You can add multiple backup passwords.
7. Specify the Source and select the types of Recovery Points required for Assured Recovery test.

Note: You can select the backup types or the latest recovery points.

8. Navigate to the **Test Settings** tab.
9. Specify the Task Setting for Test Type as **Instant Virtual Machine** and the Hyper-V IP address received from Arcserve support when configuring the Hyper-V.

   Note: The Gateway Settings option is applicable only for Linux nodes where you must select the **Use DHCP settings for Instant Virtual Machine Gateway** checkbox.



10. Specify the following details for the Assured Recovery VM Setatings, Schedule, and Advanced Settings:

    a. Specify appropriate CPU count and memory required for the Assured Recovery VM.

       Note: Specify the CPU count and Memory allocation based on the Cloud Hybrid Compute subscription purchased.

b. Specify the folder location of the Assured Recovery VM on the Hyper-V server. You must specify the following path for the Hyper-V disks location:

   F:\VMStorage

c. To specify networks, select **Network Adapter** from the *Adapter Type* drop-down list and **Arcserve_Private_Cloud** from the *Connect Assured Recovery VM to* drop-down list for network connectivity.

11. Click **Save**.

The modifications are saved successfully and the Assured Recovery task is automatically deployed. After the replication job, the Assured Recovery jobs are performed automatically and are controlled using the schedule settings.

More information:

(Optional) How to Run the Assured Recovery Test Job Manually

How to Run the Assured Recovery Test Job Manually

Arcserve UDP lets you perform manual Assured Recovery test for the nodes and plans besides the scheduled tests.

Notes:

- When the assured recovery task is configured after the MSP replication task for agent-based and host-based Linux machines, the ad-hoc assured recovery job fails to trigger and displays exception. However, you can manually run the scheduled assured recovery job.
- If the Assured Recovery task is configured after the MSP Replication task, the scheduled ad-hoc assured recovery job for the host-based agentless Linux machine is not supported when having a session password.

This section contains the following topics:

Performing Assured Recovery Test Manually for a Node

Important! If the Assured Recovery task is configured after the MSP Replication task, the scheduled ad-hoc assured recovery job for the Linux machine is not supported.

You can perform assured recovery test manually for a node.

Follow these steps:

1. From the Arcserve UDP Console, click the **resources** tab.
2. From the left pane, navigate to **Nodes**, and click **All Nodes**.
3. From the center pane, select the nodes having an Assured Recovery plan assigned and click **Actions**.
4. From the options displayed, click **Run Assured Recovery Test Now**.

   The Assured Recovery dialog opens.
5. Select an Assured Recovery task and a recovery point, and click **OK**.

The Assured recovery test of node is performed successfully.

Performing Assured Recovery Test Manually for a Plan

You can perform assured recovery test manually for a plan.

Follow these steps:

1. From the Arcserve UDP Console, click the **resources** tab.
2. From the left pane, navigate to **Plans**, and click **All Plans**.
3. From the center pane, select the nodes having an Assured Recovery plan assigned and click **Actions**.
4. From the options displayed, click **Run Assured Recovery Test Now**.

   The Assured Recovery dialog opens.
5. Select an Assured Recovery task and a recovery point, and click **OK**.

The Assured recovery test of plan is performed successfully.

Connect to Disaster Recovery System in Cloud Hybrid

This section contains the following topics:

How to Use Network Configurations in Disaster Recovery System

Access the running virtual machines and use as part of a scheduled disaster recovery test or if you want to use these machines as part of production network.

Note: To use test network configuration options to Cloud Hybrid, contact Arcserve Support.

Connect the running virtual machine using Point to Site VPN Configuration.

Point to Site VPN Configuration:

A *Point to Site* connection enables a secure virtual private network (VPN) connection between a single client machine and the virtual private data center in Cloud Hybrid. Such a connection enables an end user at a coffee shop to establish a secure private connection to the recovered environment in the cloud. It is important to note that a separate connection is needed if the end user also required access to systems that were still available in the On-premises environment. The On-premises systems fail to communicate with the recovered systems in the cloud through the “Point to Site” connection.

Follow these steps:

1. Download and install the OpenVPN client from the link.
2. Get the VPN configuration files and password from the email received as part of the onboarding process.
3. Copy the VPN configuration file content to the following path:

   <c:\program files\openvpn\config>
4. Open the *OpenVPN* Console, right click on the tray icon and click **Connect**.
5. Enter the login password.

   The IP address is assigned automatically in the range from *192.168.x.242* to *192.168.x.254*. The Subnet Mask is *255.255.255.240*.

   Note: In the IP address range mentioned above, *x* is the last octet of the public IP address of the Cloud instance. To get the public IP address, ping FQDN (Fully Qualified Domain Name) of the Cloud instance.

How to Connect to Hyper-V Server in the Disaster Recovery System

Arcserve UDP Cloud Hybrid lets the Hyper-V role available in Arcserve UDP server run Virtual Standby, Instant VM, and Assured Recovery tasks of replicated sessions. You can install the Hyper-V Manager on the local system and connect the Hyper-V server available in Cloud Hybrid using Point-to-Site VPN or Site-to-Site VPN to monitor and manage the recovered virtual machines.

Note: The Cloud Hybrid Hyper-V Server has Windows 2016 OS. As a result, use a machine that has Windows 2016 or Windows 10 (Professional or Enterprise edition) installed to connect to the Cloud Hybrid Hyper-V Server.

Follow these steps:

1. Open notepad as administrator.
2. Open C:\Windows\System32\drivers\etc\hosts and add the following line:

   <internal_server_ip> < ch*****.arcserve1.com >
3. From the client machine, open PowerShell as administrator.
4. Add the Hyper-V feature based on the installed operating system using the following command:

   For Windows 2016:

   Add-WindowsFeature Hyper-V-Tools, Hyper-V-PowerShell

   For Windows 10:

   Enable-WindowsOptionalFeature -Online -FeatureName "Microsoft-Hyper-V-Tools-All"
5. Enable the Windows PowerShell remoting using the following command:

   enable-psremoting
6. Enable Credential Security Support Provider (CredSSP) authentication on a client or on a server machine using the following command:

   enable-wsmancredssp -role client -delegatecomputer “ch*****.arcserve1.com
7. Add the Cloud Hybrid user using the following command:

   cmdkey /add:"< ch*****.arcserve1.com >" /user:clouduser /pass

8. Follow the prompt to enter the password of Cloud Hybrid user that you receive in the Welcome email.
9. Set the configuration for Windows Remote Management using the following command:

   winrm set winrm/config/client '@{TrustedHosts="<hostname.arcserve1.com>"}'

10. Launch the *Local Group Policy Editor* tab using the following command:

    Launch gpedit.msc

11. Navigate to Computer Configuration, Administrative Templates, System , Credentials Delegation and double click the **Allow delegating fresh credentials with NTLM-only server authentication** option.

    The **Allow delegating fresh credentials with NTLM-only server authentication** tab appears.

12. Select the **Enabled** option.
13. Click **Show** from the Options tab.

    The **Show Contents** tab appears.

14. Enter the following command in the *Value* tab:

    *wsman/< ch*****.arcserve1.com>*

15. Open the Hyper-V Manager.
16. Select the **Connect as another user** checkbox and connect to the server (ch*****.arcserve1.com) using the following credentials:

    Username: < ch*****.arcserve1.com >\clouduser

    Password: <Cloud user password>

    Note: Do not modify the default LBS and VPN settings for the VMs.

    The VMs available in the Cloud Hybrid are displayed.

The Hyper-V server in the Disaster Recovery system is connected successfully.

How to access your DRaaS instance using a Site to Site VPN

If you are a customer with a DRaaS subscription, please fill up the form with the help of your network team and contact Arcserve Support to initiate the setting up of site to site VPN process.

We might require the assistance of your Network Administrators to complete this activity.

Chapter 4: Configuring the Reverse Replication to a New or Empty Recovery Point Server Manually

Important! When replicating data from Cloud Hybrid to On-premise RPS server, do not select the source data store as your replication destination. To avoid data corruption, we recommend to use a new or empty data store.

The following table explains the Manual Reverse Replication scenarios in Cloud Hybrid:

Scenario	Description	Steps
Scenario 1	If the data on On-premise server, production servers, and Recovery Point Server (RPS) is lost for Cloud Hybrid BaaS.	link
Scenario 2	If the data on On-premise server, production servers, and Recovery Point Server (RPS) is lost for Cloud Hybrid DRaaS.	link
Scenario 3	If an error or data corruption occurs in the On-premise Arcserve UDP Console or RPS data store. However, the On -premise production servers are working properly.	link
Scenario 4	To get the historic data, when the retention set for local On-premise RPS is lesser than the Cloud Hybrid RPS.	link

How to Configure Manually Using Scenario 1 and Scenario 2

Follow these steps:

1. Set up a new server and install Arcserve UDP Console and RPS server.

   Verify that the RPS server is accessible in public network or is NAT configured.

   Notes:

   - Arcserve UDP Console and Agent ports are open and accessible from Internet that helps to establish the connection to Cloud Hybrid and RPS.
   - Default Ports: 8014/8015
   - For better security, we recommend to install using HTTPS protocol.

2. Create a deduplication data store and set the deduplication block size to 64KB for better performance.

   Note: The data store should not contain the same replication node(s). We recommend to create a new data store.

3. Create a local non-administrator user and a shared replication plan.

   For more information, refer link.

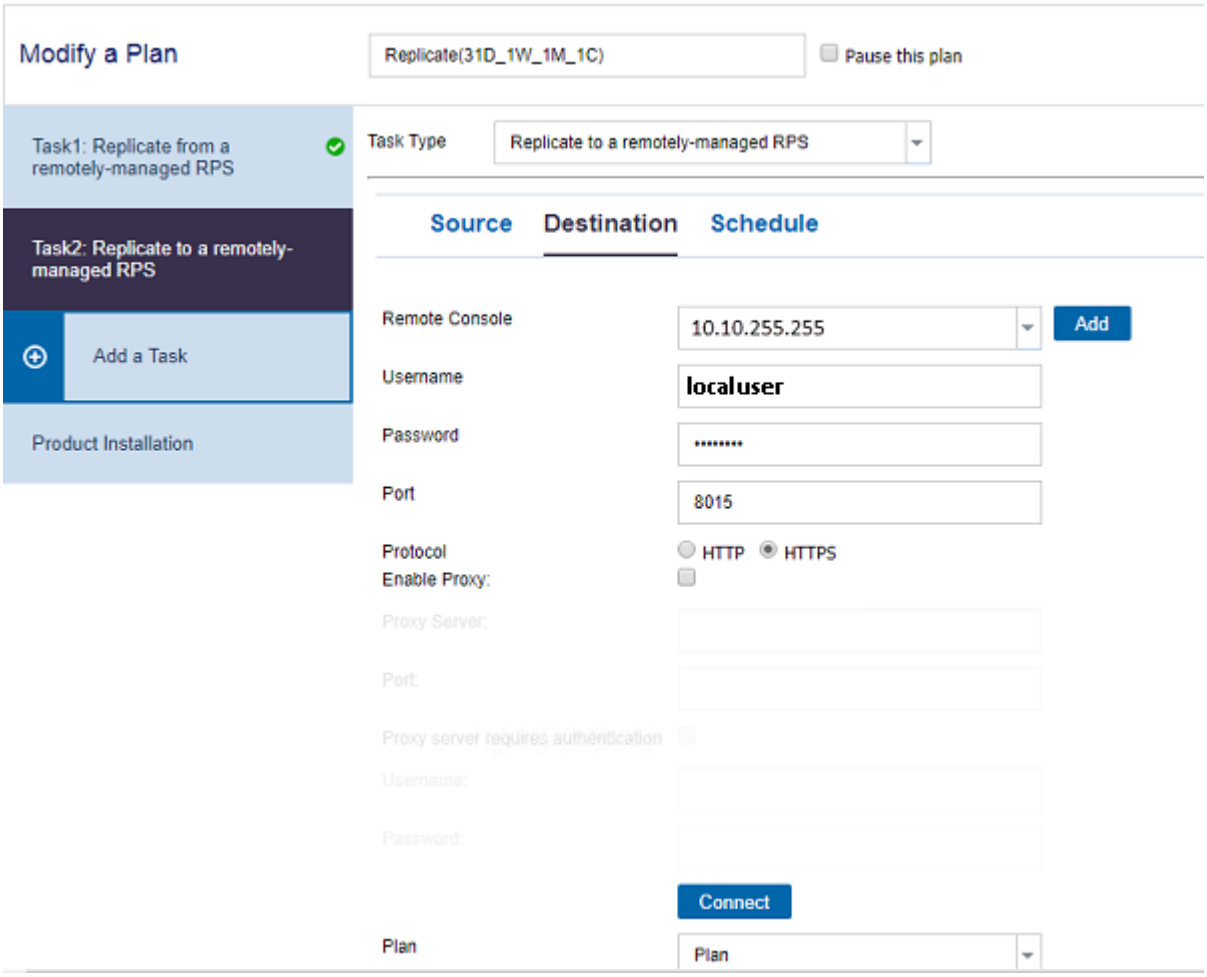
4. Log into the Arcserve UDP Console available in Cloud Hybrid using the credentials received from Arcserve.

5. Select the node(s) where you need to perform reverse replication, modify the corresponding plan, and add a **Replicate to a remotely-managed RPS** task.

6. In the **destination** tab, provide the newly deployed Arcserve UDP Console access information.

7. Click **Save**.

   The plan is saved.



8. Perform the manual replication job in Cloud Hybrid.

   For more information, refer link.

9. Perform the restore job such as BMR, VM recovery, IVM as required in the Arcserve UDP Console.

For more scenarios, click link.

How to Configure Manually Using Scenario 3 and Scenario 4

Follow these steps:

1. Log into the Arcserve UDP Console and RPS server.

   Verify that the RPS server is accessible in public network or is NAT configured.

   Notes:

   - Arcserve UDP Console and Agent ports are open and accessible from Internet that helps to establish the connection to the Cloud Hybrid and RPS.
   - Default Ports: 8014/8015
   - For better security, we recommend to install using HTTPS protocol.

2. Create a deduplication data store and set the deduplication block size to 16KB for better performance.

   Note: The data store should not contain the same replication node(s). We recommend to create a new data store.

3. Create a local non-administrator user and a shared replication plan.

   For more information, refer link.

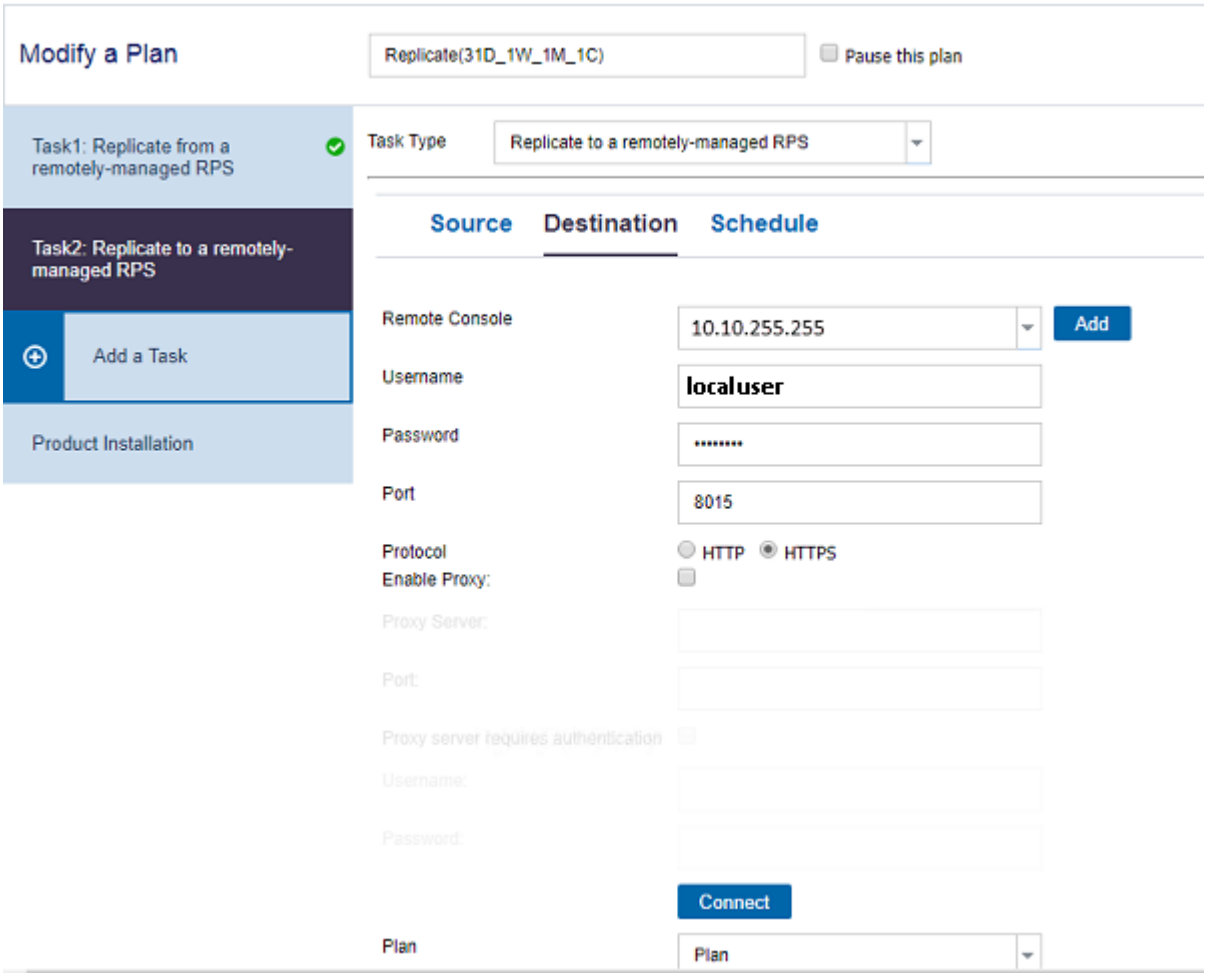
4. Log into the Arcserve UDP Console available in Cloud Hybrid using the credentials received from Arcserve.

5. Select the node(s) where you need to perform reverse replication, modify the corresponding plan, and add a **Replicate to a remotely-managed RPS** task.

6. In the destination tab, provide the newly deployed Arcserve UDP Console access information.

7. Click **Save**.

   The plan is saved.



8. Perform the manual replication job in Cloud Hybrid.

   For more information, refer link.

9. Perform the restore job such as BMR, VM recovery, IVM as required in the Arcserve UDP Console.

For more scenarios, click link.