Arcserve UDP on AWS Cloud

Deployment Guide
## Contents

Overview ........................................................................................................................................... 4
About the Deployment Guide .............................................................................................................. 4
Terms for Reference in the Guide ....................................................................................................... 4

### Arcserve UDP on AWS

AWS-enabled functionality in UDP .................................................................................................... 4
  - Virtual Standby of Windows in EC2 .............................................................................................. 5
  - Instant VM of Linux in EC2 ........................................................................................................... 5
  - Copy Recovery Point to S3 ........................................................................................................... 6
  - File Copy / File Archive to S3 ....................................................................................................... 6
  - Running Console in EC2, protecting EC2 instances and machines running on customer sites .............................................................................................................. 6
  - Running RPS in EC2, replicating from remote locations ............................................................... 7
  - Cost and Licenses .......................................................................................................................... 7

### Best practices

......................................................................................................................................................... 8

### Security

......................................................................................................................................................... 8

### Scenario 1 – Virtual Standby for Windows to AWS EC2 (Backup to On-Premise RPS, Replicate to RPS in EC2 and Start Virtual Standby instance in EC2)

Architecture ........................................................................................................................................ 10
Planning Deployment .......................................................................................................................... 10
Considerations ..................................................................................................................................... 11
Arcserve UDP Components required ............................................................................................... 13
Prerequisites ....................................................................................................................................... 11
Deployment Steps ............................................................................................................................... 15
Troubleshooting ................................................................................................................................ 27
  - AWS EC2 Instances Monitor ........................................................................................................ 27
  - Arcserve UDP Function Troubleshooting .................................................................................... 27

### Scenario 2 – Virtual Standby for Windows to AWS EC2 (Backup to On-Premise RPS and Start Virtual Standby instance in EC2)

Architecture ........................................................................................................................................ 31
Planning Deployment .......................................................................................................................... 31
Considerations ..................................................................................................................................... 32
Arcserve UDP Components required ............................................................................................... 32
Prerequisites ....................................................................................................................................... 34
Deployment Steps ............................................................................................................................... 36
Troubleshooting ................................................................................................................................ 47
  - AWS EC2 Instances Monitor ........................................................................................................ 47
  - Arcserve UDP Function Troubleshooting .................................................................................... 48
Scenario 3- Instant VM of Linux in AWS EC2 (Backup to On-Premise RPS, Replicate to RPS in EC2 and Start Instant VM in EC2) ........................................................................................................52
Architecture ........................................................................................................................................52
Planning Deployment ..........................................................................................................................53
Considerations .....................................................................................................................................53
Arcserve UDP Components required .................................................................................................54
Prerequisites .......................................................................................................................................56
Deployment Steps ...............................................................................................................................58
Troubleshooting ....................................................................................................................................79
AWS EC2 Instances Monitor ...............................................................................................................79
Arcserve UDP Function Troubleshooting ............................................................................................79

Scenario 4- Instant VM of Linux in AWS EC2 (Backup to Amazon S3 directly and Start Instant VM from AWS S3 in AWS EC2) ........................................................................................................82
Architecture ........................................................................................................................................82
Planning Deployment ..........................................................................................................................83
Considerations .....................................................................................................................................83
Arcserve UDP Components required .................................................................................................84
Prerequisites .......................................................................................................................................86
Deployment Steps ...............................................................................................................................87
Troubleshooting ....................................................................................................................................103
AWS EC2 Instances Monitor ...............................................................................................................103
Arcserve UDP Function Troubleshooting ............................................................................................103

Scenario 5- File Copy/File Archive to AWS S3 (Protect data files from On-Premise to AWS S3) ..............107
Architecture ........................................................................................................................................107
Planning Deployment ..........................................................................................................................108
Considerations .....................................................................................................................................108
Arcserve UDP Components required .................................................................................................108
Prerequisites .......................................................................................................................................110
Deployment Steps ...............................................................................................................................111
Troubleshooting ....................................................................................................................................124
Arcserve UDP Function Troubleshooting ............................................................................................124

Scenario 6- Copy Recovery Points to AWS S3 (Protect data from On-Premise to AWS S3) ....................125
Architecture ........................................................................................................................................125
Planning Deployment ..........................................................................................................................126
Considerations .....................................................................................................................................126
Arcserve UDP Components required .................................................................................................126
Prerequisites .......................................................................................................................................128
Deployment Steps ...............................................................................................................................129
Troubleshooting ....................................................................................................................................137
Arcserve UDP Function Troubleshooting ............................................................................................137
Overview

About the Deployment Guide

This deployment guide has been created by Arcserve team in partnership with Amazon Web Services (AWS).

This reference deployment guide provides step-by-step instructions for deploying Arcserve UDP environment on the AWS Cloud.

The guide is for IT infrastructure architects, administrators, and DevOps professionals who are planning to implement or extend their Arcserve UDP workloads on the AWS Cloud.

Terms for Reference in the Guide

The following terms used in the guide are provided here for a quick reference:

<table>
<thead>
<tr>
<th>Terms/Abbreviation</th>
<th>Description/Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arcserve UDP or UDP</td>
<td>Arcserve Unified Data Protection</td>
</tr>
<tr>
<td>Arcserve HA or HA</td>
<td>Arcserve High Availability</td>
</tr>
<tr>
<td>AWS EC2</td>
<td>Amazon (Web Services) Elastic Compute Cloud</td>
</tr>
<tr>
<td>RPS</td>
<td>Recovery Point Server</td>
</tr>
<tr>
<td>VSB</td>
<td>Virtual Standby</td>
</tr>
<tr>
<td>IVM</td>
<td>Instant Virtual Machine</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</td>
</tr>
<tr>
<td>CRP</td>
<td>Copy Recovery Point</td>
</tr>
</tbody>
</table>

Arcserve UDP on AWS

Arcserve UDP is a versatile data protection suite that allows to protect critical customer data both on-premises and in the cloud.

Key features of fast, simple, efficient next-generation data protection:

- Unified management console with simple, yet powerful plan-based data protection policies.
- Physical & agentless host-based backup for vSphere & Hyper-V.
- Global deduplication, encryption, compression & WAN-optimized replication on Source.
- Instant VM & BMR, Local & Remote Virtual Standby, Hardware Snapshots, full system High Availability & tape backup.
- Supports Windows (Inc. 10), Linux, Exchange, SQL, File Server, IIS, AD, Oracle, PSQL, vSphere, Hyper-V, and MSCS.
- Application-consistent backup & granular restores.
- Centralized reporting & alerting.
- Supports Software, appliance or cloud.
AWS-enabled functionality in UDP
This section describes UDP functionalities/features that support AWS as source/destination.

**Virtual Standby of Windows in EC2**

The Virtual Standby converts the recovery points to virtual machine formats on a specified cloud and prepares a snapshot to easily recover data when needed. This feature provides the high availability capability also and ensures that the virtual machine can take over immediately when the source machine fails. The VSB virtual machine is created by converting the recovery points to Amazon AWS EC2 virtual machine format.

**Note:** For more details, refer to [How to Create a Virtual Standby to AWS EC2 Plan](#) in Arcserve UDP Solutions Guide.

**Instant VM of Linux in EC2**

Instant virtual machine (Instant VM or IVM) supports creating a virtual machine on Amazon EC2 instantly. The IVM on Amazon EC2 provides:

- Immediate access to data and applications present in the Arcserve UDP backup sessions.
- Eliminates the downtime associated with a traditional restore or conversion of the backup session to a virtual machine.
- Provides an alternative to create virtual machine on cloud, rather than local.
- Directly provides backup to S3 and starts instant VM from S3.
Note: For more details, refer to How to Create and Manage an Instant Virtual Machine on Amazon EC2 in Arcserve UDP Solutions Guide.

Copy Recovery Point to S3

Using Arcserve UDP, you can copy the recovery points to S3 Cloud. This process helps ensure that you have an additional copy of the recovery points if your original recovery points are accidentally deleted. The copy recovery point task copies the recovery points from the backup destination to S3 Cloud.

Note: For more details, refer to How to Create a Copy Recovery Points Plan in Arcserve UDP Solutions Guide.

File Copy / File Archive to S3

The file copy task lets you copy individual files to S3 cloud. The original copy is retained. The file copy job runs on the recovery point server making it possible for Arcserve UDP to offload the task from agents.

The file archive task lets you archive individual files to S3 cloud. The original files are deleted from the source after you have copied the files to S3 cloud, providing more free space at your source.

Note: For more details, refer to How to Create a File Copy Plan and How to Create a File Archive Plan in Arcserve UDP Solutions Guide.

Running Console in EC2, protecting EC2 instances and machines running on customer sites

Running Console in EC2 can protect EC2 instance directly. You need to ensure that all related instances can communicate with private IP. To protect the machines running on customer sites utilize UDP Gateway to provide accessibility to those on-premise nodes with UDP Console in EC2.

Note: For more details, refer to How to Add and Manage a Remote Site in Arcserve UDP Solutions Guide.
Running RPS in EC2, replicating from remote locations

Being optimized for data transfer over WAN, UDP replication can efficiently replicate your recovery points from the local RPS server to the RPS servers located on EC2. Running RPS in EC2 can improve the data availability and provide the global duplication that makes the data transfer much faster and involves much lesser storage occupation when protecting large number of nodes.

Secondly, when deploying an RPS server on EC2, all data transfer for Virtual Standby and Instant VM take place at the private subnet in VPC. Such data transfer helps you have better security as only port 8014 is required for the replication from external access.

Besides, you do not need to additionally install UDP agent at another instance on EC2 as the Virtual Standby of Windows Cloud proxy when the RPS server is on EC2.

Cost and Licenses

You are responsible for the cost of the AWS services used while running Arcserve UDP product on AWS.

Primarily, your cost for deploying Arcserve UDP on AWS will consist of an Arcserve UDP license, the cost of running EC2 instances for your UDP components, and data hosting costs in Amazon S3 and EBS. For more information on running instance costs, refer to the EC2 On-Demand Pricing guide.

This deployment uses a Bring Your Own License (BYOL) model for Arcserve UDP. You can obtain a 30-day free trial by completing trial request form at www.arcserve.com.
**Best practices**

- To protect the nodes in on-premise network, UDP console should be installed on the host in your on-premise network.
- Select HTTPS as protocol when installing the UDP components.
- Installing RPS server on EC2 can bring the global deduplication.
- For cost saving, back up your Linux nodes directly to S3 rather than the RPS located on EC2.
- To improve data availability, install RPS servers on different availability zones and add the replication tasks between those RPS servers.
- The inbound rules in security group should be limited to the specific ports for data transfer and monitoring. For details, see the Security section.
- All data transfer for Virtual Standby and Instant VM take place at the private subnet in VPC when deploying an RPS server on EC2. This helps restrict external access as you need to access only port 8014 from external source for the replication.
- The Virtual Standby instance must be in the same availability zone with cloud proxy. The instance can be in different subnets.

**Security**

To run properly, Arcserve UDP requires some roles for UDP service and user privileges configuration to function.

For details, refer to User Security in Arcserve UDP Solutions Guide.

**Virtual Standby of Windows in EC2**

Virtual Standby of Windows in AWS EC2 Plan requires following security prerequisites:

Configure the Security group setting on EC2 to open the related ports

- UDP Console / Recovery Point Server (RPS) (for Replication to EC2 RPS task)
  - Internet & Intranet Inbound 8014, 8015
  - Intranet Inbound 445
- UDP Windows Agent (works as Virtual Standby Proxy):
  - Internet and Intranet Inbound 8014
  - Internet and Intranet Inbound 4091

Specific AWS API permissions are required for Amazon IAM users to have control and interaction with AWS APIs for VSB to EC2.

For details, refer to How to configure IAM granular permissions for IAM users with VSB to EC2 in Arcserve UDP Solutions Guide.

For details about other prerequisites, refer to How to Create a Virtual Standby to AWS EC2 Plan in Arcserve UDP Solutions Guide.
**Instant VM of Linux in EC2**

Instant VM of Linux in AWS EC2 Plan requires following security prerequisites:

Configure the Security group setting on EC2 to open the related ports:

- UDP Console / Recovery Point Server (RPS) (for Replication to EC2 RPS task)
  - Internet & Intranet Inbound 8014, 8015
  - Intranet Inbound 445
- UDP Linux Backup Server (works as Linux Instant VM Proxy)
  - Internet and Intranet Inbound 8014
  - Intranet Inbound 8016, 8017

**Notes:** To know other prerequisites, refer to [How to Create and Manage an Instant Virtual Machine on Amazon EC2](#) in Arcserve UDP Solutions Guide.

**Copy Recovery Point to S3**

AWS API permission to perform operations on buckets and objects.

**File Copy / File Archive to S3**

AWS API permission to perform operations on buckets and objects.
Scenario 1—Virtual Standby for Windows to AWS EC2 (Backup to On-Premise RPS, Replicate to RPS in EC2 and Start Virtual Standby instance in EC2)

Virtual Standby to AWS EC2 feature supports creating a virtual standby machine on Amazon EC2 and its data based on the replicated UDP recovery points from the On-Premise backup. This feature is available in Arcserve Unified Data Protection v6.5.

Architecture
The scenario is applicable to such customers who have already deployed the data protection solution on-premise and want to set up a remote DR site in AWS cloud.

The on-premise solution comprises of UDP Console and the local RPS server. The customers can back up Windows systems to local RPS and decide whether to perform deduplication of the data. At the AWS cloud like the remote DR site. The RPS server can also provide the deduplication feature and the role of Virtual Standby Cloud proxy that will interact with EC2 and serve the Virtual Standby jobs. During the conversion of virtual standby jobs, the EBS volumes will be attached to the RPS server on EC2. The RPS server will convert the data from the recovery points and write the data to the EBS volumes. After conversion, the session snapshot will be taken to keep the original data from your volume. Then, the driver injection will be processed to make sure the machines can be launched on EC2. After that the bootable snapshot will be taken to boot up the instances.

You can plan for the Management Console to replicate the protected data from local RPS to Cloud RPS and the virtual standby task after the replication. If the production machine is down because of the hardware failure or other reasons, you can start the virtual standby instance in AWS EC2 from Cloud RPS, and then the new EC2 Instance can be ready to use within minutes as the production machine.
Planning Deployment
Planning Deployment requires the following options:

- Considerations
- Arcserve UDP Components required
- Prerequisites
- Deployment Steps

Considerations
Below are considerations for planning deployment in AWS EC2 and the On-Premise site for the scenario Virtual Standby to AWS EC2 (Backup to local RPS, replicate to RPS in AWS EC2, start VSB to EC2 task, and start Virtual Standby instance on EC2).

Important! Before deployment, refer to Arcserve UDP Release Notes and Compatibility Matrix to understand system requirements and supported Operating Systems for every component.

- Refer to Arcserve UDP v6.5 Release Notes for System Information of every component and navigate to Product Update to view the latest v6.5 level system information.
- Refer to Arcserve UDP v6.5 Compatibility Matrix for supported Operating Systems.
- Refer to Arcserve UDP v6.5 Release Notes for Supported Languages.
- Refer to Arcserve Product Download page for detailed download link. We recommend the latest version.

Arcserve UDP Components required

Arcserve UDP Components Download

Important! This scenario is supported from Arcserve UDP version 6.5. We recommend deploying the latest Update. The installed component version on AWS or On-Premise must match.

- Unified Installer

For new environment that does not have UDP installed before, we recommend utilizing unified installer to download and install the latest released update with v6.5 together.

- Unified installer download link for v6.5 is ASDownloader.exe that always publishes the latest released Arcserve Products. This link includes not only Arcserve UDP, but also Arcserve Backup and Arcserve HA.
- For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

Note:

- When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
- When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.
Product individual release download

Arcserve Product Download page: You can get all Arcserve UDP version download link for individual package. We recommend installing the latest version.

Arcserve UDP Agent (Linux) Download Links: You can get all Arcserve UDP Linux version download links and need to select matched Arcserve UDP Linux version with Arcserve UDP Console.

Note:
- For new customer, we recommend downloading the remaster build and install to get the major release with the latest Update together.
- For existing customers, we recommend downloading the individual Update package that has smaller size or select Check for Updates from Arcserve UDP Console.
- Refer to individual Update Release Notes Installation Chapter for detailed steps or download link.
- For more detailed steps, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

Auto Update

Existing v6.5 UDP customer can automatically upgrade to the latest update using the option Check for Updates from Arcserve UDP Console Help menu or wait for the scheduled time to automatically download the latest Update that is configured at Update Configuration (Default time: Sunday 3:00 AM).

Arcserve UDP Components System Requirements for AWS EC2

- Arcserve Unified Data Protection Recovery Point Server (as Replication Target RPS)
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

Arcserve UDP components System Requirements for On-Premise

- Arcserve Unified Data Protection Console
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size
Arcserve UDP on AWS Cloud: Deployment Guide

- **Arcserve Unified Data Protection Recovery Point Server (as Replication Source RPS)**
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

**Prerequisites**

Prerequisites and General Configuration for AWS EC2:

- You must have Virtual Private Cloud (VPC) and Subnet created to run RPS in AWS EC2.
  - You can find VPC settings at EC2 Management Console -> Services -> Networking & Content Delivery -> VPC
    - Access AWS EC2 Management Console
  - You can find subnet settings at EC2 Management Console -> Services -> Networking & Content Delivery -> Subnets
Arcserve UDP on AWS Cloud: Deployment Guide

- You must have a Public IP for RPS in AWS that is used for replication destination. Following are two ways to get public IP in AWS EC2:
  - Allocate **Elastic IP** and assign it to EC2 instance *(Recommended)*
  - Automatically assign when launching EC2 instance
- You must have **AWS Access** and **Secret Keys** for a user with permission to manage AWS EC2.
  - You can find Access key at **IAM -> Users -> Security Credentials**

- You must have below **Ports** enabled in **Security Group** Setting on AWS.
  - UDP Recovery Point Server (RPS):
    - Internet & Intranet Inbound 8014, 8015 *(if Console is installed in AWS)*
    - Internet Inbound 4091
- You must have specific AWS API permissions for Amazon IAM users to control and interact with AWS APIs for VSB to EC2. For details, refer to [How to configure IAM granular permissions for IAM users with VSB to EC2](#).

On-Premise Prerequisites and General Configuration:

- Prepare servers in advance to be deployed as Arcserve UDP Console, Recovery Point Server. Those servers must meet system requirements for every component.
- Servers in Arcserve UDP Console or Recovery Point Server role must be able to connect with the target instance in EC2.
Deployment Steps

Follow below steps to prepare AWS EC2 instance first and then install required Arcserve UDP components in AWS EC2.

Note: Log into AWS EC2 Management Console using your account.

Step 1. Deploy Arcserve UDP Recovery Point Server (as Replication Target RPS) in AWS EC2

1. Launch Instance at EC2 dashboard -> Instances -> Launch Instances

a) Select one Amazon Machine Image (AMI) that is provided by Amazon.

Note: Arcserve UDP RPS is supported on Windows 2008 R2 or above Windows version. Refer to the Compatibility Matrix for information about supported Operating Systems for RPS.

b) Select an Instance Type.

System requirement consideration on RPS

- Instance type m4.xlarge (13 ECU, 4 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 16 GiB memory, EBS only) is recommended.
- Instance type t2.xlarge (Variable ECU, 4 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 16 GiB memory, EBS only) is the minimal requirement.

Note: For more information, refer to the Chapter System Information for RPS in UDP Release Notes.

Other instance type with higher performance is recommended.
c) Configure Instance Details

**Important:**

- Make sure the Arcserve UDP RPS and Linux Backup Server in AWS EC2 can connect to each other.
- Enable *Auto-assign Public IP* if you do not want to use *Elastic IP* for RPS because auto-assign public IP cannot be changed after the instance is launched.
- Enable *CloudWatch* if you want to monitor detailed information of Arcserve UDP RPS.
- Use *Dedicated Instance* if you want high performance.
Arcserve UDP on AWS Cloud: Deployment Guide

**d) Add storage for Instance.**
Storage depends on your business requirement.
- Minimum Storage: 40 GB
- Recommended Storage: 80 GB

**Notes:** Storage will depend on the source data size. Use SSD to get higher performance.

**e) Add Tag for Instance**
You can add tag for your instances to improve search. For example, use **UDP RPS** as a tag.

**f) Configure Security Group.**
Configure below **Ports** enabled for **Security Group** setting on this instance as replication target RPS in AWS EC2.
- **UDP Recovery Point Server (RPS):**
  - Internet & Intranet Inbound 8014
  - Internet & Intranet Inbound 8015 (Only where UDP Console is installed in AWS)
  - Internet Inbound 4091
Note: As the above ports are accessible to the internet, limit the source to your own IPs.

1.2 After the AWS EC2 Instance is ready, download the latest Arcserve UDP v6.5 installation package to install RPS.

- Installation by Unified Installer
  - Unified installer download link for v6.5 is ASDownloader.exe.
  - For more detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  Note:
  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- Installation by Setup Wizard
  - Access Arcserve Product Download page to get all UDP version download link for individual package and the recommend latest version to install.
  - For detailed steps, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.
Step 2. Arcserve UDP Console Installation for On-Premise

2.1 Download and Install UDP console

- **Installation by Unified Installer**
  - Unified installer download link for v6.5 is ASDownloader.exe.
  - For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**
  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration or select the Advanced Installation mode for install components separately and then you can customize the installation path and protocol.

- **Installation by Setup Wizard**
  - Access Arcserve Product Download page to get all UDP version download link for individual package and the recommend latest version to install.
  - For detailed steps, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

2.2 Launch Arcserve UDP Console after completing installation from Start menu

Arcserve UDP Console will be launched in browser like https://console_hostname:8015/. (For example, protocol and port need to match your setup configuration).
Log into Console using the correct Account name and Password.
Step 3. On-Premise side Arcserve UDP Recovery Point Server Installation and Configuration

Arcserve UDP Recovery Point Server can be deployed from Arcserve UDP Console or add it to Console after RPS Server is installed on that server. Follow these steps to add an RPS server on UDP Console and remotely deploy RPS to the server that does not have RPS server installed:

3.1 Launch Arcserve UDP Console

3.2 Add an RPS server on UDP Console -> resources -> Destination -> Add a Recovery Point Server and RPS server will be automatically deployed to the target server.

Note: For more details, refer to Add a Recovery Point Server in Arcserve UDP Solutions Guide.

The RPS server will be automatically deployed to that server according to the setting you configured. The default settings are displayed in the below screenshot.

3.3 Create a Data Store on UDP Console -> resources -> Destination -> Recovery Point Servers

Follow these steps to Create a Data Store:

Note: For details, refer to Add a Data Store in Arcserve UDP Solutions Guide.

a) Select the RPS server just added in the last step (3.2).
b) Right click the server in Centre Pane, and then click **Add a Data Store** from the drop-down menu.

<table>
<thead>
<tr>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Data Store</td>
<td>Import Data Store</td>
</tr>
<tr>
<td>RPS Jumpstart</td>
<td>Install/Upgrade Recovery Point Server</td>
</tr>
</tbody>
</table>


c) Create a Data Store.

![Create a Data Store](image)

d) After Data Store is created, verify the destination.

After completing all the procedures involved in adding an RPS, verify if the RPS is added successfully.

For more details, refer to **Verify the Destination** in Arcserve UDP Solutions Guide.
Step 4. On-Premise Arcserve UDP Console Node Management

4.1 Add RPS to Console as Replication Target RPS in AWS EC2 site.
   a) Navigate to UDP Console -> resources -> Destination -> Add a Recovery Point Server to add the RPS in AWS EC2.
   b) Follow the similar steps mentioned in Step 3.2 to add an RPS and Step 3.3 to create a data store on this RPS in AWS EC2.

   **Important!** Without adding AWS EC2 RPS before, you cannot add the replication task in the next step.

4.2 Verify if the On-Premise site RPS and Data Store created in previous Step 3 are listed correctly on UDP Console -> resources -> Destination.

4.3 Add On-Premise Windows Node as target protected node on UDP Console->resources->All Nodes->Add Nodes->Add Windows Node.

   Refer to screenshot below or Add Nodes in Arcserve UDP Solutions Guide.
Refer to the Compatibility Matrix to view supported Operating Systems for Windows Node.

4.4 Add a Cloud Account for AWS EC2 in UDP Console

Navigate to UDP Console -> resources -> Destinations -> Cloud Account -> Add a Cloud Account

**Note:** For details, refer to Add a Cloud Account in Arcserve UDP Solutions Guide.

- **Access Key ID**
  Identifies the user who is requesting access to this location.

- **Secret Access Key**
  Refers to a password that is used to verify the authenticity of the request to access this location because your Access Key is not encrypted.

  **Important!** This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials at a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over unsafe channels.

- **Proxy Settings (only when UDP Console must use Proxy to connect to AWS)**
  Specifies the proxy server settings. Select the check box of Connect using a proxy server if you want to enable this option. If selecting this option, do include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connection. You can also select this option if your proxy server requires authentication.
For proxy server, you must provide the corresponding authentication information (Domain Name/Username and Password) that is required to use the proxy server.

![Add a Cloud Account]

5. On-Premise Arcserve UDP Console Configure Plan with Backup, Replication and Virtual Standby Tasks

To enable Virtual Standby to AWS EC2 for this scenario, you need to configure a plan with backup and replication task and complete that job in advance.

5.1 Add a Plan on UDP Console->resource->All Plans->Add a Plan

Enter a name to create a plan as displayed in below screenshot.

![Add a Plan]

5.2 Add a Windows Backup Task

Follow these steps to add a Windows Backup task as the first task on this new plan:

**Note:** For more information, refer to How to Create a Windows Backup Plan in UDP Solutions Guide.
1. From Task Type, select **Backup: Agent-Based Windows**.
2. From Source, select Node by clicking **Add**.
3. From Destination, select **Arcserve UDP Recovery Point Server** as **Destination** Type (select the On-Premise RPS added in Step 3.2 and Data Store created in Step 3.3).
4. From Schedule, configure backup schedule.
5. From Advanced, configure any Pre/Post Script or Email alert.
6. Save the plan (optional).

   **Note:** You can save the plan after all tasks are configured.

**5.3 Add a Replication Task**

   After configuring the backup task, add a Replicate task. Replication lets you copy your backed-up data from one Data Store in the On-Premise RPS site to the target RPS in AWS EC2. For details, refer to **Add a Replicate Task to the Plan** in Arcserve UDP Solutions Guide.

In **Task2: Replicate**

1. To set Destination, select the RPS and Data Store in AWS that you configured in Step 4.1.
2. Set Schedule for replication.
3. Set Advanced setting to enable Email alert (optional).

<table>
<thead>
<tr>
<th>Task Type</th>
<th>Replica</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>Recovery Point Server</td>
<td></td>
</tr>
<tr>
<td>Data Store</td>
<td></td>
</tr>
<tr>
<td>When replication job fails:</td>
<td></td>
</tr>
<tr>
<td>Retry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

**5.4 Add a Virtual Standby task**

   After configuring the replication task, add a Virtual Standby task. The VSB task converts the replicated backup data to the AWS EC2 format and creates an EC2 virtual standby instance.

   For more details, refer to **Add a Virtual Standby to EC2 Task to the Plan** in Arcserve UDP Solutions Guide.

In **Task3: Virtual Standby**
4. From the virtualization server tab, select EC2 as the virtualization type.
5. Select the task2 replication as the source.
6. Select the existing AWS account created in the step 4.4.
7. Select appropriate EC2 region and the RPS server on AWS EC2 as the cloud proxy with the credentials entered below.
8. In the Virtual Machine tab, select the instance type and EBS Volume Types for the virtual standby instances.
9. Set the VPC and subnet for the virtual standby instance network.

   Note: The VPC and subnet of the virtual standby instance should be in the same available zone with the RPS server on EC2.

5.5 Save the plan with Backup, Replicate and Virtual Standby tasks that will run according to the configured schedule.

Step 6. Power on the Virtual Standby instance on AWS EC2

Prerequisites:
- Need Backup, Replicate and Virtual Standby tasks completed successfully

6.1 Configure the network of the Virtual Standby instance on EC2

You can power on the Standby VM on AWS EC2 with customized network settings.

   Note: For detailed steps, refer to How to Configure the Virtual Standby Instance on EC2 Network in Arcserve UDP Solutions Guide.

6.2 Power on the Virtual Standby Instance on EC2 from the recovery point snapshot.

You can power on virtual standby machines from recovery point snapshots manually if a source server fails, an emergency occurs, or you want to make a source node offline for maintenance.

1. From the resources tab, navigate to the Virtual Standby node group.
   The virtual standby nodes are displayed on the center pane.
2. On the center pane, select the node and click Standby VM.
   The Standby VM dialog opens.
3. On the Standby VM dialog, perform the following tasks:
   Select a date and time snapshot of the recovery point snapshot to power on the virtual machine.
   Note: If the standby virtual machine was not configured yet, the link The standby virtual machine network is not configured is displayed.
   a) Click this link to configure the network.
   b) Click Save.
      The settings are saved for the virtual standby virtual machine.
   c) Click Close and the Recovery Point Snapshot dialog appears.
4. Click Power On VM.
   The virtual machine is powered on using the data contained in the recovery point snapshot.
Note: After the virtual machine is powered on, you can be prompted to restart the machine once or multiple times due to the Amazon PV driver installed on the virtual machine.

Troubleshooting

**AWS EC2 Instances Monitor**

Monitor Console/RPS/Virtual Standby Proxy using functions provided by Amazon EC2

- Use **Status Checks** feature to verify whether Amazon EC2 has detected any problem that might prevent your instances from running applications.
  - For details, refer to [How to configure Status Checks in AWS User Guide](#).
- Use **CloudWatch** to view metrics for CPU utilization, data transfer, and disk usage activity from Amazon EC2 instances without any additional cost.
  - With an additional cost, CloudWatch provides Detailed Monitoring for EC2 instances with higher resolution and metric aggregation.
  - For details, refer to [How to use CloudWatch in AWS User Guide](#).

Log into Console/RPS/Virtual Standby Proxy to monitor the CPU/Memory/Disk usage.

When the performance is low, you can resize the instance or attach a new volume

- Resize the instance to improve the performance.
  - For details, refer to [How to resize instance in AWS User Guide](#).
- Attach new volume
  - For details, refer to [How to Attach new volume to instance in AWS User Guide](#).

**Arcserve UDP Function Troubleshooting**

Troubleshooting on AWS EC2 when Virtual Standby instance is not started or unreachable

EC2 instances do not have a physical monitor through which you can view their console output.

If the virtual standby job is complete and you power on the virtual standby instance on EC2, the Instance may sometimes

- fail to start VM or
- become unreachable

Then, you can **Get the Console Output of the Instance** or **Capture a Screenshot of the Instance** for more useful information to troubleshoot.

Open the **AWS EC2 Management Console**

**To get Console Output of the AWS EC2 Instance**

Console output is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started.
In the left navigation pane, click Instances, and select the instance.

Click Actions, Instance Settings, Get System Log.
To Capture a Screenshot of the AWS EC2 Instance

If you are unable to reach your instance through SSH or RDP, you can capture a screenshot of your instance and view it as an image. This provides visibility to the status of the instance, and allows for quicker troubleshooting. There is no data transfer cost for this screenshot. The image is generated in JPG format, not larger than 100 KB.

- In the left navigation pane, click Instances.
- Select the instance to capture.
- Click Actions, Instance Settings, Get Instance Screenshot.
- Right-click on the image to download and save.
Arcserve UDP on AWS Cloud: Deployment Guide

Note: For more details, refer to AWS User Guide.

Troubleshooting Reference for Arcserve UDP

Refer to Release Notes of each version for Limitations and Known Issues of individual feature.

Refer to Arcserve UDP Solutions Guide Troubleshooting chapter for overall Troubleshooting.

Arcserve UDP Log Collections

- Arcserve UDP Console Logs under <Install Path>|Management|logs
- Arcserve UDP RPS, Virtual Standby Proxy and Windows Agent Logs under <Install Path>|Engine|logs and <Install Path>|Engine|Configuration

assured recovery™
Scenario 2—Virtual Standby for Windows to AWS EC2 (Backup to On-Premise RPS and Start Virtual Standby instance in EC2)

Virtual Standby to AWS EC2 feature supports creating a Virtual Standby machine on Amazon EC2 and its data based on the recovery points from the On-Premise backup. This feature is available in Arcserve Unified Data Protection v6.5.

Architecture

The scenario is applicable to such customers who have already deployed the data protection solution on-premise and want to start the Virtual Standby instance in AWS cloud.

The on-premise solution comprises of UDP console and the local RPS server. The customers can back up Windows systems to local RPS and decide whether to perform deduplication of the data. At the AWS cloud, the EC2 instance installed with UDP agent will act as the role of virtual standby cloud proxy that will interact with EC2 and serve the Virtual Standby jobs. During the conversion of virtual standby jobs, the EBS volumes will be attached to the VSB cloud proxy on EC2. The cloud proxy will convert the data from the recovery points of the on-premise backup and write the data to the EBS volumes. After conversion, the session snapshot will be taken to keep the original data from customer’s volume. Then, the driver injection will be processed to make sure the machines can be launched on EC2. After that the bootable snapshot will be taken for the user to boot up the instances.

The customer can plan for the Management Console to back up the data to the local RPS and then perform the Virtual Standby task after the backup. If the production machine is down because of the hardware failure or other reasons, the customer can start the virtual standby instance on AWS EC2, and then the new EC2 Instance can be ready to use within minutes as the production machine.
Planning Deployment

Planning Deployment requires the following options:

- Considerations
- Arcserve UDP Components required
- Prerequisites
- Deployment Steps

Considerations

Below are considerations for planning deployment in AWS EC2 and On-Premise site for the scenario Virtual Standby to AWS EC2 (Backup to local RPS, VS8 task after backup and start the Virtual Standby instance).

**Important!** Before deployment, refer to Arcserve UDP Release Notes and Compatibility Matrix to understand system requirements and supported Operating Systems for each component.

- Refer to Arcserve UDP v6.5 release notes for System Information on each component, and navigate to Product Update to view the latest v6.5 level system information.
- Refer to Arcserve UDP v6.5 Compatibility Matrix for supported Operating Systems.
- Refer to Arcserve UDP v6.5 release notes for Supported Languages.
- Refer to Arcserve Product Download page for detailed download link. We recommend the latest version.

Arcserve UDP Components required

Consider the following components:

- Arcserve UDP Components Download
- Arcserve UDP Components System Requirements for AWS EC2
- On-Premise required Arcserve UDP components System Requirements

Arcserve UDP Components Download

**Important!** This scenario is supported from Arcserve UDP version 6.5. We recommend deploying the latest Update. The installed component version on AWS or On-Premise need to match.

- **Unified Installer**

  For the new environment that does not have UDP installed before, we recommend utilizing unified installer to download and install latest released update with v6.5 together.
  
  - Unified installer download link for v6.5 is ASDownloader.exe that always publishes the latest released Arcserve Products. This link includes not just Arcserve UDP, but also Arcserve Backup and Arcserve HA.
  
  - For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**
When the **Choose Components to Download** dialog opens, select **Arcserve UDP** to only download the latest package of Arcserve UDP.

When the **Installation Method** dialog opens, select **Express Installation** mode to install RPS as default configuration, or select **Advanced Installation** mode to install components separately and then you can customize the installation path and protocol.

### Product individual release download

Arcserve [Product Download page](#): You can get all Arcserve UDP version download links for individual package. We recommend installing the latest version.

Arcserve [UDP Agent (Linux) Download Links](#): You can get all Arcserve UDP Linux version download links. Select the matching Arcserve UDP Linux version with Arcserve UDP Console.

**Note:**

- For new customer, we recommend downloading the remaster build to install the major release with the latest Update together.
- For existing customer, we recommend downloading the individual Update package that has smaller size or select **Check for Updates** from Arcserve UDP Console.
- Refer to individual Update Release Notes Installation Chapter for detailed steps or download link.
- For detailed steps, refer to [Install Arcserve UDP Using the Setup Wizard](#) Arcserve UDP Solutions Guide.

### Auto Update

Existing v6.5 UDP customer can automatically upgrade to the latest update using the option **Check for Updates** from Arcserve UDP Console Help menu or wait for the scheduled time to automatically download the latest Update that is configured at **Update Configuration** (Default time: Sunday 3:00 AM).

### Arcserve UDP Components System Requirements for AWS EC2

- **Arcserve Unified Data Protection Agent (as Virtual Standby proxy)**
  - Window 2008 R2 Server or above
  - 1 GHz CPU or above
  - 40 GB (for OS installation)
  - 2 GB RAM or above

### On-Premise required Arcserve UDP components System Requirements

- **Arcserve Unified Data Protection Console**
Arcserve UDP on AWS Cloud: Deployment Guide

- Window 2008 R2 Server or above
- 1 x CPU with 4 Core (2.7 GHz) or above
- 40 GB (for OS installation)
- 8 GB RAM or above
- Backup Storage – depends on your source data size

- **Arcserve Unified Data Protection Recovery Point Server**
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

**Prerequisites**

*Prerequisites and General Configuration for AWS EC2:*

- You must have **Virtual Private Cloud (VPC)** and **Subnet** created to run RPS in AWS EC2.
  - You can find VPC settings at **EC2 Management Console -> Services -> Networking & Content Delivery -> VPC**
  
  Access **AWS EC2 Management Console**.

  ![VPC Dashboard](image)

  - You can find subnet settings at **EC2 Management Console -> Services -> Networking & Content Delivery -> VPC -> Subnets**
You must have a Public IP for RPS in AWS that is used for replication destination. Following are two ways to get public IP in AWS EC2.

- Allocate Elastic IP and assign it to EC2 instance (Recommended)
- Automatically assign when launching EC2 instance

You must have AWS Access and Secret Keys for a user with permission to manage AWS EC2. You can find Access key at IAM ->Users ->Security Credentials

You must have below Ports enabled in Security Group Setting on AWS.

- UDP Recovery Point Server (RPS):
  - Internet & Intranet Inbound 8014, 8015 (if installed Console in AWS)
  - Intranet Inbound 4091
You must have specific AWS API permissions for Amazon IAM users to control and interact with AWS APIs for VSB to EC2. For details, refer to How to configure IAM granular permissions for IAM users with VSB to EC2.

On-Premise Side Prerequisites and General Configuration:

Prepare servers in advance to be deployed as Arcserve UDP Console, Recovery Point Server and those servers must meet system requirements for each component.

Servers in Arcserve UDP Console or Recovery Point Server role must be able to connect with the target instance in EC2.

Deployment Steps

Follow these steps to prepare AWS EC2 instance firstly and install required Arcserve UDP components in AWS EC2:

Log into AWS EC2 Management Console using your account

Step 1. Deploy Arcserve UDP Virtual Standby proxy in AWS EC2

1.1 Launch Instance at EC2 dashboard -> Instances -> Launch Instances

a) Select one Amazon Machine Image (AMI) that is provided by Amazon.
   Note: Arcserve UDP RPS is supported on Windows 2008 R2 or above Windows version. Refer to Compatibility Matrix for information about supported Operating Systems for RPS.
b) Select an **Instance Type**.

System requirement consideration on Virtual Standby proxy

- Instance type **m4.large** (13 ECU, 2 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 8 GiB memory, EBS only) is recommended.
- Instance type **t2.small** (Variable ECU, 1 vCPU, 12 CPU Credits/hour, Intel Broadwell E5-2686v4, 2 GiB memory, EBS only) is the minimal requirement.

**Note:** For detailed information, refer to the System Information for RPS. Other instance type with higher performance is recommended.

![Instance Type Selection](image)

**c) Configure Instance Details**

**Important!**

- Make sure the Arcserve UDP RPS and Linux Backup Server in AWS EC2 can connect to each other.
- Enable **Auto-assign Public IP** if you do not want to use Elastic IP for RPS because auto-assign public IP cannot be changed after the instance is launched.
- Enable **CloudWatch** if you want to monitor detailed information of Arcserve UDP RPS.
- Use **Dedicated instance** if you want high performance.
d) **Add storage** for Instance.

Storage 40 GB is recommended. Configure according to your business requirement.

<table>
<thead>
<tr>
<th>Step 4: Add Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Type</td>
</tr>
<tr>
<td>Root</td>
</tr>
</tbody>
</table>

**Notes:** Storage will depend on the source data size. Use SSD to get higher performance.

e) **Add Tag** for Instance.

You can add tag for your instance to make improve search possibility. For example, *UDP RPS* as a tag.
f) Configure **Security Group**. Configure below **Ports** enabled for **Security Group** setting on this instance as replication target RPS in AWS EC2.

- **UDP Recovery Point Server (RPS):**
  - Internet & Intranet Inbound 8014
  - Internet & Intranet Inbound 8015 (Only where UDP Console is installed in AWS)
  - Internet Inbound 4091

**Important!** As the above ports are opened to the internet, limit the source to your own IPs.

g) Review the instance configurations and launch it.

h) Create **Access Key ID** and **Secret Access Key** on AWS Management Console. Running Virtual Standby to EC2 job needs to use the access key for API calls. **Access Key ID** and **Secret Access Key** are required to prepare in advance under AWS Management Console for your AWS account.

You can create, rotate, disable, or delete access keys (access key IDs and secret access keys) for your AWS account root user. Anyone with an access key for your AWS account has unrestricted access to all the resources in your account, including billing information.

When you create an access key, AWS gives you an opportunity to view and download the secret access key only once. If you do not download it or if you lose it, you can delete the access key and then create a new one.

**Note:** For detailed steps, refer to Managing Access Keys for Your AWS Account.
1.2 After the AWS EC2 Instance is ready, download the latest Arcserve UDP v6.5 installation package to install UDP agent.

- **Installation by Unified Installer**
  - Unified installer download link for v6.5 is ASDownloader.exe.
  - For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**
  - When the Choose Components to Download dialog opens, select Arcserve UDP to only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Advanced Installation mode to install agent only and then you can customize the installation path and protocol.

- **Installation by Setup Wizard**
  - Arcserve Product Download page: You can get all UDP version download link for individual package. We recommend the latest version to install.
  - For detailed steps, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

**Step 2. On-Premise Arcserve UDP Console Installation**

2.1 Download and Install UDP console

- **Installation by Unified Installer**
  - Unified installer download link for v6.5 is ASDownloader.exe.
  - For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**
  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration or select the Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- **Installation by Setup Wizard**
  - Arcserve Product Download page: You can get all UDP version download link for individual package. We recommend installing the latest version.
  - For detailed steps, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.
2.2 Launch Arcserve UDP Console after completing installation from Start menu

Arcserve UDP Console will be launched in browser. For example, https://console_hostname:8015/ (protocol and port need to match your setup configuration).

Log into Console with your Account name and Password.

Step 3. On-Premise Arcserve UDP Recovery Point Server Installation and Configuration

Arcserve UDP Recovery Point Server can be deployed from Arcserve UDP Console or add it to Console after RPS Server is installed on that server.

Follow these steps to Add an RPS server on UDP Console and remotely deploy RPS to the server that do not have RPS server installed:

3.1 Launch Arcserve UDP Console

3.2 Add an RPS server on UDP Console -> resources -> Destination -> Add a Recovery Point Server and RPS server will be automatically deployed to the target server.

**Note:** For more details, refer to Add a Recovery Point Server in Arcserve UDP Solutions Guide.

RPS Server will be automatically deployed to that server according to the setting you configured. The default settings are displayed in the below screenshot.
3.3 Create a Data Store on **UDP Console->resources->Destination -> Recovery Point Servers**

Follow below steps to create a data store:

**Note:** For more details, refer to [Add a Data Store](#) in Arcserve UDP Solutions Guide.

a) Select the RPS server that you added in the last step (3.2).

b) Right click the server in Centre Pane and select **Add a Data Store** from the drop-down menu.

c) Create a Data Store.
d) After creating the data store, verify the destination. After completing all the procedures involved in adding an RPS, verify if the RPS is added successfully. For more information, refer to Verify the Destination in Arcserve UDP Solutions Guide.

Step 4. On-Premise Arcserve UDP Console Node Management

4.1 Add On-Premise Windows Node as target protected node on UDP Console->resources->All Nodes->Add Nodes->Add Windows Node

Refer to screenshot below or the Add Nodes topic in Arcserve UDP Solutions Guide.

Refer to Compatibility Matrix to view supported Operating Systems for Windows Node.
4.2 Add a Cloud Account for AWS EC2 in UDP Console

Navigate to UDP > resources > Destinations > Cloud Account > Add a Cloud Account

**Note:** For more details, refer to Add a Cloud Account in Arcserve UDP Solutions Guide.

- **Access Key ID**
  Identifies the user who is requesting access to this location.

- **Secret Access Key**
  Refers to a password that is used to verify the authenticity of the request to access this location because your Access Key is not encrypted.

  **Important!** This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials at a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

- **Proxy Settings (only when UDP Console must use Proxy to connect to AWS)**
  Specifies the proxy server settings. Select the check box of Connect using a proxy server if you want to enable this option. If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy.
server for internet connections. You can also select this option if your proxy server requires authentication. Then, you must provide the corresponding authentication information [Domain Name\Username and Password] that is required to use the proxy server.

**Step 5. On-Premise Arcserve UDP Console Configure Plan with Backup and Virtual Standby Tasks**

To enable Virtual Standby to AWS EC2 for this scenario, configure a plan with backup and complete that job in advance.

**5.1 Add a Plan on UDP Console -> resource -> All Plans -> Add a Plan**

Enter a name to create a plan.

**5.2 Add a Windows Backup Task**

Follow these steps to Add a Windows Backup task as the first task on this new plan:

*Note: For detailed steps, refer to [How to Create a Windows Backup Plan](#) in Arcserve UDP Solutions Guide.*
1. From Task Type, select **Backup: Agent-Based Windows**
2. From Source, select Node by clicking Add button
3. From Destination, select **Arcserve UDP Recovery Point Server** as Destination Type (select the On-Premise RPS added in Step 3.2 and Data Store created in Step 3.3)
4. From Schedule, config backup schedule
5. From Advanced, config any Pre/Post Script or Email alert
6. Save the plan (optional)
   
   **Note:** You can save the plan after all tasks are configured.

5.3 Add a Virtual Standby task

After configuring the backup task, add a Virtual Standby task. This task lets you convert the backup data on-premise to the AWS EC2 format and an EC2 virtual standby instance will be created.

For more information, refer to Add a Virtual Standby to EC2 Task to the Plan in Arcserve UDP Solutions Guide.

In Task 3: Virtual Standby

1. From the virtualization server tab, select EC2 as the virtualization type.
2. Select the Task 1 backup as the source.
3. Select the existing AWS account created in step 4.2.
4. Select the proper region and the virtual standby proxy on AWS EC2 as the cloud proxy with the credentials entered below.
5. In the virtual machine tab, select the instance type and EBS volume type for the virtual standby instances.
6. Set the VPC and subnet for the virtual standby instance network.

   **Note:** The VPC and subnet of the virtual standby instance should be in the same available zone with the virtual standby proxy on EC2.

5.4 Save the plan with Backup and Virtual Standby tasks that will run according to the configured schedule.
Step 6. Power on the Virtual Standby instance on AWS EC2

Prerequisites:

Need Backup, Replicate and Virtual Standby tasks completed successfully

6.1 Configure the network of the Virtual Standby instance on EC2

You can power on the Standby VM on AWS EC2 with customized network settings.

**Note:** For detailed steps, refer to How to Configure the Virtual Standby Instance on EC2 Network in Arcserve UDP Solutions Guide.

6.2 Power on the Virtual Standby Instance on EC2 from the recovery point snapshot.

You can power on virtual standby machines from recovery point snapshots manually if a source server fails, an emergency occurs, or you want to make a source node offline for maintenance.

1. From the resources tab, navigate to the Virtual Standby node group.
   The virtual standby nodes are displayed on the center pane.
2. On the center pane, select the node and click Standby VM.
   The Standby VM dialog opens.
3. On the Standby VM dialog, perform the following tasks:
   Select a date and time snapshot of the recovery point snapshot to power on the virtual machine.
   **Note:** If the standby virtual machine was not configured yet, the link "The standby virtual machine network is not configured." is displayed.
   a) Click this link to configure the network.
   b) Click Save.
      The settings are saved for the virtual standby virtual machine.
   c) Click Close.
   d) The Recovery Point Snapshot dialog appears.
4. Click Power On VM.
   The virtual machine is powered on using the data contained in the recovery point snapshot.
   **Note:** After the virtual machine is powered on, you can be prompted to restart the computer one or more times because the Amazon PV driver is installed on the virtual machine.

Troubleshooting

AWS EC2 Instances Monitor

Monitor Console/RPS/Virtual Standby Proxy using functions provided by Amazon EC2

- Use Status Checks feature to check whether Amazon EC2 has detected any problems that might prevent your instances from running applications.
  **Note:** For details, refer to How to configure Status Checks in AWS User Guide.
- Use CloudWatch to view metrics for CPU utilization, data transfer, and disk usage activity from Amazon EC2 instances for no additional charge.
  For an additional charge, CloudWatch provides Detailed Monitoring for EC2 instances with higher resolution and metric aggregation.
  **Note:** For details, refer to How to use CloudWatch in AWS User Guide.
Log into Console/RPS/Virtual Standby Proxy to monitor the CPU/Memory/Disk usage. When the performance is low, you can resize the instance or attach a new volume:

- Resize the instance to improve the performance.
  For details, refer to How to resize instance in AWS User Guide.
- Attach new volume
  For details, refer to How to Attach new volume to instance in AWS User Guide.

**Arcserve UDP Function Troubleshooting**

*Troubleshooting on AWS EC2 when Virtual Standby instance is not started or unreachable*

EC2 instances do not have a physical monitor through which you can view their console output. If the virtual standby job is completed and you power on the virtual standby instance on EC2, sometimes the instance may:

- fail to start VM
- become unreachable

Then, you can Get the Console Output of the Instance or Capture a Screenshot of the Instance for more useful information on troubleshooting.

Open the [AWS EC2 Management Console](https://aws.amazon.com/ec2/).

**To get Console Output of the AWS EC2 Instance**

Console output is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started.

- In the left navigation pane, click Instances, and select the instance.
- Click Actions, Instance Settings, Get System Log.
To Capture a Screenshot of the AWS EC2 Instance

If you are unable to reach your instance via SSH or RDP, you can capture a screenshot of your instance and view it as an image. This provides visibility to the status of the instance, and allows for quicker troubleshooting. There is no data transfer cost for this screenshot. The image is generated in JPG format, no larger than 100 KB.

1. In the left navigation pane, click Instances.
2. Select the instance to capture.
4. Right-click on the image to download and save it.
Note: For more details, view AWS User Guide.

Troubleshooting Reference for Arcserve UDP

Refer to Release Notes of each version for Limitations and Known Issues on specific feature.

Refer to Arcserve UDP Solutions Guide Troubleshooting chapter for overall Troubleshooting.

Arcserve UDP Log Collections

- Arcserve UDP Console Logs under <Install Path>\Management\logs
- Arcserve UDP RPS, Virtual Standby Proxy and Windows Agent Logs under <Install Path>\Engine\logs and <Install Path>\Engine\Configuration
### Scenario 3- Instant VM of Linux in AWS EC2 (Backup to On-Premise RPS, Replicate to RPS in EC2 and Start Instant VM in EC2)

Instant VM of Linux in AWS EC2 feature supports creating a virtual machine on Amazon EC2 instantly based on the replicated UDP recovery points from the On-Premise backup. This feature is available in Arcserve Unified Data Protection v6.5.

#### Architecture

The scenario is applicable to the customers who have already deployed the data protection solution on-premise and want to setup a remote DR site in AWS cloud.

The on-premise solution comprises of UDP console, the local RPS and Linux Backup Server. The customers can back up Linux systems to local RPS and decide whether to perform deduplication of the data. At the AWS cloud, the Remote DR site can only have an RPS most of the time. Cloud Linux Backup Server only needs to be started when you need to run restore functions such as Linux Instant VM in cloud.

You can plan in the Management Console to replicate the protected data from local RPS to Cloud RPS. If the production machine is down because of the hardware failure or other reasons, the customer can start the Cloud Linux Backup Server to perform a Linux Instant VM in AWS EC2 from Cloud RPS, and then the new EC2 Instance can be ready to use within minutes.

With traditional BMR, you need to restore all the data first and then reboot the Instance for use. But with Linux Instant VM, you can launch an EC2 Linux Instance in minutes as the production machine instead of restoring all the data first. Linux Instant VM can help to reduce the downtime of production machines and improve the RTO to minutes.

When a Linux Instant VM job in EC2 is performed, it will create an EC2 instance, restore some data and files related to system boot first, and then reboot the EC2 Instance. The Instance can be ready to use when the system boot is finished. At the backend, it will still retrieve the data from the recovery point if the data has not been recovered, but this process is not aware of upper-level applications.

If Linux Instant VM in EC2 is for your permanent use, you can enable automatic data recovery when the EC2 Instance is ready to use. Also, reboot is not required when the recovery is finished.
Planning Deployment

Planning Deployment requires the following options:

- Considerations
- Arcserve UDP Components required
- Prerequisites
- Deployment Steps

Considerations

Below are considerations for planning deployment in AWS EC2 and On-Premise site for the scenario Instant VM of Linux in AWS EC2 (Backup to local RPS, replicate to RPS in AWS EC2, start Instant VM in AWS EC2).

**Important!** Before deployment, refer to Arcserve UDP Release Notes and Compatibility Matrix to understand system requirements and supported Operating Systems for each component.

- Refer to Arcserve UDP v6.5 release notes for System Information on every component, and navigate to Product Update to view the latest v6.5 level system information.
- Refer to Arcserve UDP v6.5 Compatibility Matrix for supported Operating Systems.
- Refer to Arcserve UDP v6.5 Release Notes for Supported Languages.
- Refer to Arcserve Product Download page for detailed download link. We recommend the latest version.
Arcserve UDP Components required

**Arcserve UDP Components Download**

**Important!** This scenario is supported from Arcserve UDP version 6.5. We recommend deploying the latest Update. The installed component version on AWS or On-Premise must match.

- **Unified Installer**
  
  For new environment that does not have UDP installed before, we recommend utilizing unified installer to download and install the latest released update with v6.5 together.

  - Unified installer download link for v6.5 is [ASDownloader.exe](#) that always publishes the latest released Arcserve Products. This link includes not just Arcserve UDP, but also Arcserve Backup and Arcserve HA.
  - For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**

  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration, or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- **Product individual release download**

  Arcserve Product Download page: You can get all Arcserve UDP version download link for individual package, we recommend the latest version to install.

  Arcserve UDP Agent (Linux) Download Links: You can get all Arcserve UDP Linux version download link, and need to select matched Arcserve UDP Linux version with Arcserve UDP Console.

  **Note:**

  - For new customer, we recommend downloading the remaster build to install and install to get the major release with the latest Update together.
  - For existing customer, we recommend downloading the individual Update package that has smaller size, or select Check for Updates from Arcserve UDP Console.
  - Refer to individual Update Release Notes Installation Chapter for detailed steps or download link
  - For more detailed steps, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

- **Auto Update**
Arcserve UDP on AWS Cloud: Deployment Guide

Existing v6.5 UDP customer can automatically upgrade to the latest update using the option **Check for Updates** from Arcserve UDP Console Help menu or wait for the scheduled time to automatically download the latest Update that is configured at **Update Configuration** (Default time: Sunday 3:00 AM).

**Note:** Arcserve UDP Linux Backup Server does not support Auto Update

---

**Arcserve UDP Components System Requirements for AWS EC2**

- **Arcserve Unified Data Protection Recovery Point Server (as Replication Target RPS)**
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

- **Arcserve Unified Data Protection Agent (Linux) Backup Server**
  - RHEL 7.x, CentOS 7.x, SuSE SLES 12.x, Ubuntu 14.04, or above recommended
  - 4 GB RAM or above
  - 2 GB disk space for /tmp folder, 6 GB disk space for /opt folder as minimum disk space (Ext 2,3,4 & Reiser FS v3 file systems)
  - **Note:** For more details about supported Operating Systems, refer to Arcserve UDP v6.5 Compatibility Matrix.

---

**Arcserve UDP Components System Requirements for On-Premise**

- **Arcserve Unified Data Protection Console**
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

- **Arcserve Unified Data Protection Recovery Point Server (as Replication Source RPS)**
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

---

assured recovery™
Arcserve UDP on AWS Cloud: Deployment Guide

- Arcserve Unified Data Protection Agent (Linux) Backup Server
  - RHEL 7.x, CentOS 7.x, SuSE SLES 12.x, Ubuntu 14.04, or above recommended
  - 4 GB RAM or above
  - 4 GB disk space for /tmp folder, 6 GB disk space for /opt folder as minimum disk space (Ext 2,3,4 & Reiser FS v3 file systems)

- (Optional) Arcserve Unified Data Protection Host-Based Agentless Backup Proxy (to protect Linux VM in Hypervisor)
  - Window 2003 R2 Server or above
  - 1 x CPU with 4 core (2.7 GHz) or above
  - 10 GB or more
  - 8 GB RAM or above

Prerequisites

Prerequisites and General Configuration of AWS EC2:

- You must have Virtual Private Cloud (VPC) and Subnet created to run RPS and Linux Backup Server in AWS EC2.
  - You can find VPC settings at EC2 Management Console -> Services -> Networking & Content Delivery -> VPC
  - You can find subnet settings at EC2 Management Console -> Services -> Networking & Content Delivery -> VPC -> Subnets
You must have a Public IP for RPS and Linux Backup Server in AWS that is used for replication destination. Following are two ways to get public IP in AWS EC2:

- Allocate Elastic IP and assign it to EC2 instance (Recommended)
- Automatically assign when launching EC2 instance

You must have AWS Access and Secret Keys for a user with permission to manage AWS EC2.

- You can find Access key at IAM -> Users -> Security Credentials

You must have below Ports enabled in Security Group Setting on AWS.

- UDP Recovery Point Server (RPS):
  - Internet & Intranet Inbound 8014, 8015 (if Console installed in AWS)
  - Intranet Inbound 445
- UDP Linux Backup Server:
  - Internet and Intranet Inbound 8014
  - Intranet Inbound 8016, 8017
On-Premise Side Prerequisites and General Configuration:

Prepare servers in advance to be deployed as Arcserve UDP Console, Recovery Point Server, Linux Backup Server and those servers must meet system requirements for each component.

Servers in Arcserve UDP Console or Recovery Point Server role must be able to connect with the target instance in EC2.

Deployment Steps

Follow these steps to prepare AWS EC2 instance first, install required Arcserve UDP components, and configure Instant VM of Linux in AWS EC2:

Log into AWS EC2 Management Console using your account.

Step 1. Deploy Arcserve UDP Recovery Point Server (as Replication Target RPS) on AWS EC2

1.1 Launch Instance at EC2 dashboard -> Instances -> Launch Instances

a) Select one Amazon Machine Image (AMI) that is provided by Amazon.

Note: Arcserve UDP RPS is supported on Windows 2008 R2 or above Windows version. Refer to the Compatibility Matrix for supported Operating Systems for RPS.

b) Select an Instance Type.

System requirement consideration on RPS
- Instance type **m4.xlarge** (13 ECUs, 4 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 16 GiB memory, EBS only) is recommended.
- Instance type **t2.xlarge** (Variable ECUs, 4 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 16 GiB memory, EBS only) is the minimal.

**Note:** For more information, refer to the System Information of RPS. Other instance type with higher performance is recommended.

c) **Configure Instance Details.**

**Important!**

- Make sure the Arcserve UDP RPS and Linux Backup Server in AWS EC2 can connect to each other.
- Enable **Auto-assign Public IP** if you do not want to use **Elastic IP** for RPS because auto-assign public IP cannot be changed after instance is launched.
- Enable **CloudWatch** if you want to monitor detailed information of Arcserve UDP RPS.
- Use **Dedicated instance** if you want high performance.
d) **Add storage for Instance**  
   Storage depends on your business requirement.  
   Minimum Storage: 40 GB  
   Recommended Storage: 80 GB

**Notes:** Storage will depend on the source data size. Use SSD to get higher performance.

e) **Add Tag for Instance**  
   You can add tag for your instance to make it easy to find, for example “UDP RPS” as a tag.

f) **Configure Security Group.**  
   Configure below Ports enabled for Security Group Setting on this instance as replication target RPS in AWS EC2.
Arcserve UDP on AWS Cloud: Deployment Guide

- UDP Recovery Point Server (RPS):
  - Internet & Intranet Inbound 8014
  - Internet & Intranet Inbound 8015 (Only where UDP Console installed in AWS)
  - Intranet Inbound 445

**Note:** As the above ports are opened to the internet, limit the source to your own IPs.

g) Review the instance configurations and launch it.

1.2 After the AWS EC2 Instance is ready, download the latest Arcserve UDP v6.5 installation package to install RPS.

- **Installation by Unified Installer**
  - Unified installer download link for v6.5 is **ASDownloader.exe**.
  - For more details, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**
  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration, or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- **Installation by Setup Wizard**
  - Arcserve Product Download page: Gets all UDP version download link for individual package, we recommend latest version to install.
  - For more details, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

**Step2. Deploy Arcserve UDP Linux Backup Server (as Instant VM Proxy) on AWS EC2**

You can launch an Arcserve UDP Agent (Linux) instance directly using Amazon Machine Image (AMI) in AWS Cloud. After launching the Arcserve UDP Agent (Linux) instance, you can open the user interface from any computer using a web browser and the server is referred as Backup Server.
For more information, refer to Install Arcserve UDP Agent (Linux) in AWS Cloud in Arcserve UDP Agent for Linux User Guide.

Launch AWS Instance at EC2 dashboard -> Instances -> Launch Instances

- Search "Arcserve_Unified_Data_Protection_Agent_Linux" in Community AMIs, and Select one AMI that match to your UDP Console version. For example, if your UDP Console version is v6.5 Update2 build number 4175.667, then you need to select AMI Arcserve_Unified_Data_Protection_Agent_Linux_6.5.4175.667.

- Select an Instance Type.
  - Instance type **t2.xlarge** (Variable ECUs, 4 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 16 GiB memory, EBS only) is recommended
  - Instance type **t2.medium** (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only) is minimal requirement

  **Note:** Refer to the System Information for Linux Backup Server for detailed information, other instance type with higher performance is recommended.
c. **Configure Instance Details.**

- **Network**
  - VPC (Virtual Private Cloud)
  - Subnet (Create new subnet)

- **Auto-assign Public IP**
  - Use IPAM (IP Address Management)

- **Domain Name**
  - None (Create new domain)

- **Security Group**
  - SSH Enabled: Port 22

- **Additional Security Options**
  - Protect against accidental termination
  - Enable CloudWatch for detailed monitoring

- **Tenancy**
  - Shared

Notes:

- Make sure the RPS and Linux backup server can connect to each other
- Enable **Auto-assign Public IP** if you do not want to use Elastic IP as auto-assign public IP cannot be changed after instance is launched.
- Enable **CloudWatch** if you want to monitor detailed information
- Use Dedicated instance if you want high performance.

d. Add Storage for Instance.

Storage depends on your business requirement.

Minimum Storage: 40 GB
Recommended Storage: 80 GB

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store-volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store-volumes. Learn more about storage options in Amazon EC2.

- Add New Volume

Minimum Storage: 40 GB
Recommended Storage: 80 GB

e. Add Tag for Instance.

You can add tag for your instance to make it easy to find.

Step 5: Add Tags

A tag consists of a tag name key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

- Add another tag

(f) Configure Security Group

UDP Linux Backup Server require below Ports opened.

- Internet and Intranet Inbound 8014
- Intranet Inbound 8016, 8017

Step 6: Configure Security Group

A security group is a list of inbound rules that control the traffic to and from your instance. For example, if you want to set up a web server and allow Internet traffic to the HTTP and HTTP ports. You can create a new security group or select an existing one. Learn more about Amazon EC2 security groups.

- [Create security group]
- [Review security group]

(g) Review the instance configurations and launch it
After the AWS EC2 Instance is launched, Arcserve UDP Linux Backup Server will be running in this instance, you can browse [https://hostname:8014](https://hostname:8014) to verify if Linux Backup Agent Console is running properly (default user is udpuser).

**Step3. On-Premise side Arcserve UDP Console Installation**

3.1 Download and Install UDP console

- Installation by Unified Installer
  - Unified installer download link for v6.5 is [ASDownloader.exe](ASDownloader.exe).
  - Refer to Arcserve UDP Solutions Guide [Install Arcserve UDP Using the Unified Installer](Install Arcserve UDP Using the Unified Installer) chapter for detailed steps.

  **Note:**
  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration, or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- Installation by Setup Wizard
  - Arcserve Product Download page: You can get all UDP version download link for individual package, we recommend latest version to install.
  - For more information, refer to [Install Arcserve UDP Using the Setup Wizard](Install Arcserve UDP Using the Setup Wizard) in Arcserve UDP Solutions Guide.

3.2 Launch Arcserve UDP Console after installation completed from Start Menu

Arcserve UDP Console will be launched in browser like [https://console_hostname:8015/](https://console_hostname:8015/) (for example, protocol and port need to match your setup configuration).

Log into Console with correct Account and Password.
Step 4. On-Premise side Arcserve UDP Recovery Point Server Installation and Configuration

Arcserve UDP Recovery Point Server can be deployed from Arcserve UDP Console, or add it to Console after RPS Server is installed on that server.

Follow these steps to add an RPS server on UDP Console and remotely deploy RPS to the server that do not have RPS server installed:

1. Launch Arcserve UDP Console.
2. Add an RPS server on UDP Console > resources > Destination > Add a Recovery Point Server and RPS server will be automatically deployed to the target server.

   **Note:** For more information, refer to Add a Recovery Point Server in Arcserve UDP Solutions Guide.

   RPS Server will be automatically deployed to that server according to the setting you configured. The default settings are displayed in the below screenshot.
3.3 Create a Data Store on UDP Console-> resources-> Destination -> Recovery Point Servers

Follow these steps to create a data store:

Note: For more information, refer to Add a Data Store in Arcserve UDP Solutions Guide.

3.3.1 Select the RPS server added in the last step.

3.3.2 Right click the server in Centre Pane, select Add a Data Store from the drop-down menu.

3.3.3 Create a Data Store.
3.3.4 After Data store is created, verify the destination.

After completing all the procedures involved in adding an RPS, verify if the RPS is added successfully.

For more information, refer to Verify the Destination in Arcserve UDP Solutions Guide.

**Step5. Arcserve UDP Linux Backup Server Installation and Configuration for On-Premise**

5.1 Download Arcserve UDP Agent (Linux) build

Open All Arcserve UDP Linux Download Links and select one Arcserve UDP Linux build that matches with Arcserve UDP console version.

5.2 Install the Arcserve UDP Agent (Linux) Backup Server on the target server by following the steps mentioned in the Install Arcserve UDP Agent (Linux) guide.

**Step6. On-Premise side Arcserve UDP Console Node Management**

6.1 Add the RPS in AWS EC2 site to Console as Replication Target RPS.

   a) Navigate to UDP Console-> resources-> Destination -> Add a Recovery Point Server to add the RPS in AWS EC2.

   b) Follow the similar steps mentioned in Step 4.2 to add an RPS and Step 4.3 to create a data store on this RPS in AWS EC2.
**Note:** Without this AWS EC2 RPS added in advance, you cannot add replication task after this step.

6.2 Verify if the On-Premise site RPS and Data Store created in previous Step4 is listed correctly on UDP Console->resources->Destination.

6.3 Add On-Premise Linux Backup Server installed in Step5 on UDP Console->resources->All Nodes->Add Nodes->Add Linux Backup Server Node.

Refer to screenshot below or Arcserve UDP Solutions Guide Add Nodes topic.

Refer to the Compatibility Matrix for supported Operating Systems for Linux Backup Server.
6.4 Add On-Premise Linux Node as target protected node on UDP Console\,
\rightarrow resources\rightarrow All Nodes\rightarrow Add Nodes\rightarrow Add Linux Node.

Refer to screenshot below or Arcserve UDP Solutions Guide Add Nodes topic;

All target protected Linux nodes need to be added one by one to have those added into Plan to protect in the next step.

Refer to the Compatibility Matrix for supported Operating Systems for Linux Node.

---

Step 7. On-Premise Arcserve UDP Console Configure Plan with Backup and Replication Tasks

To enable Linux IVM to AWS EC2 for this scenario, configure a plan with backup and replication task and complete that job in advance.

7.1 Add a Plan on UDP Console\rightarrow resource\rightarrow All Plans\rightarrow Add a Plan

Create a plan and name it, as displayed in below screenshot.

7.2 Add a Linux Backup Task

Follow these steps to Add a Linux Backup task as the first task on this new plan.
Note: For more information, refer to How to Create a Linux Backup Plan in Arcserve UDP Solutions Guide.

a. From Task Type, select **Backup: Agent-Based Linux**

b. From Source, select Linux Backup Server (Select the On-Premise side Linux Backup Server added in Step 6.3)

c. From Source, select Node by clicking **Add** (Select the On-Premise Linux node added in Step 6.4)

d. From Destination, select **Arcserve UDP Recovery Point Server** as **Destination** Type (select the On-Premise RPS added in Step 4.2 and Data Store created in Step 4.3)

e. From Schedule, config backup schedule

f. From Advanced, config any Pre/Post Script or Email alert

g. Save the plan (optional)

**Note:** You can click Save the plan after all tasks are configured.
7.3 Add a Replication Task

After configuring the backup task, add a Replicate task that will copy your backup data from one Data Store in On-Premise RPS site to the target RPS in AWS EC2.

Arcserve UDP Solutions Guide Add a Replicate Task to the Plan Arcserve UDP Solutions Guide.

In Task2: Replicate

1. Set Destination, Select the RPS and Data Store in AWS that you configured in Step 6.1.
2. Set Schedule for replication.
3. Set Advanced setting for enable Email alert (optional).

7.4 Save the plan with Backup and Replicate task that will run according to the configured schedule.

Step8: Create and Manage Instant Virtual Machine on AWS EC2

Prerequisites:

- Create Access Key ID and Secret Access Key on AWS Management Console

Launch Instant VM needs to use the access key for API calls, Access Key ID and Secret Access Key are required to prepare in advance under AWS Management Console for your AWS account.

You can create, rotate, disable, or delete access keys (access key IDs and secret access keys) for your AWS account root user. Anyone who has an access key for your AWS account has unrestricted access to all the resources in your account, including the billing information.

When you create an access key, AWS gives an opportunity to view and download the secret access key only once. If you do not download it or lose it, you can delete the access key and then create a new one.

Note: For more information, refer to Managing Access Keys for Your AWS Account topic in AWS Documentation.
• **Add a Cloud Account for AWS EC2 in UDP Console**

  Navigate to UDP Console -> resources -> Destinations -> Cloud Account -> Add a Cloud Account

  Note: For more information, refer to [Add a Cloud Account](#) in Arcserve UDP Solutions Guide.

  - **Access Key ID**
    
    Identifies the user who is requesting access to this location.

  - **Secret Access Key**
    
    Refers to a password that is used to verify the authenticity of the request to access this location because your Access Key is not encrypted.

    **Important!** This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials at a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

  - **Proxy Settings (only when UDP Console must use Proxy to connect to AWS)**

    Specifies the proxy server settings. Select the check box of [Connect using a proxy server](#) if you want to enable this option. If selecting this option, do include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections. You can also select this option if your proxy server requires authentication.

    For proxy server, you must provide the corresponding authentication information (Domain Name\Username and Password) that is required to use the proxy server.
Add the Linux Backup Server in AWS EC2 to UDP Console as Linux IVM proxy

Navigate to UDP Console->resources->All Nodes->Add Nodes->Add Linux Backup Server Node to add this Linux Backup server, similar as in Step 6.3.

Note: The default user is udpuser for the Linux Backup Server in AWS.

Need Backup and Replicate task completed successfully

Create an Instant VM on Node Management View or Destination Management View.

Creating an Instant VM involves the following five major steps:

Note: For detailed steps, refer to How to Create and Manage an Instant Virtual Machine on Amazon EC2 in Arcserve UDP Solutions Guide.

1. Open the Instant VM Wizard from UDP Console.
   Instant VM Wizard can be launched for specified Linux node from Node Management View or Destination Management View by selecting 'Create an Instant VM' after a right click on the Linux Node.
   Note: For more information, refer to Open the Instant VM wizard in Arcserve UDP Solutions Guide.

2. Select a Recovery Point that stored in the AWS Replication Target RPS
   Note: For more information, refer to Select the recovery point in Arcserve UDP Solutions Guide.
3. Select VM Location to launch Instant VM.

Specify **Cloud Type** as Amazon EC2 and the **Account Name** that you prepared in advance to create the Instant VM.

**Note:** For more information, refer to **Select the VM location** in Arcserve UDP Solutions Guide.

4. Select a Recovery Server to run Instant VM.

Specify the Linux Backup Server in AWS EC2 as proxy to run Instant VM.

**Note:** For more information, refer to **Select the recovery server** in Arcserve UDP Solutions Guide.
5. Specify the Instant VM machine details for AWS EC2 Cloud Instance.

   **VM Name**
   Specifies the name of the Instant VM. The name of the source node prefixed with “UDPIVM_” becomes the default name of the Instant VM. You can modify the name. Some special characters, such as '@', '/' and so on, are not allowed in the name.

   **Description**
   (Optional) Specifies the description for the Instant VM.

   **Region**
   Specifies the region of your Amazon EC2 account.

   **Instance Type**
   Specifies the supported instance type.

   **Volume Type**
   Specifies the type of volume.

   **Network**
   Specifies the network existing on the Amazon EC2 account.

   **Subnet**
   Specifies the subnet existing on the Amazon EC2 account.

   **Auto-assign Public IP**
   Specifies the public IP assigned to the VM.

   **Primary IP**
   Specifies the primary IP of VM. Specifies automatically if you do not specify.
Select a Security Group
Specifies the security group. You can select multiple groups. If you do not select, automatically creates a new security group.

Advance: Change Host Name
Specifies the host name of new VM.

Advance: Recover data automatically after Instant VM is started
Specifies if data recovery takes place automatically, after creating the Instant VM.

Note: For more information, refer to Specify the Instant VM details in Arcserve UDP Solutions Guide.

6. Submit the Instant VM job.

After Virtual Machine Settings configuration, click Finish.

When Boot VM dialog opens, select Boot Now, Boot Later option.

Boot Now: Automatically starts the VM after the VM is created; Boot Later: You can start the VM manually after the Instant VM job is complete.

The Instant VM job is successfully created.

After the job is complete, you can view the Instant VM in resources, Infrastructure, Instant Virtual Machine.

Note: For more information, refer to Submit the Instant VM job in Arcserve UDP Solutions Guide.
Manage an Instant Virtual Machine

You can manage the Instant VM from Console. You can power-on or power-off an Instant VM from the UDP Console. Also, you can delete any Instant VM.

Note: The UDP Console displays only those Instant VM that are created from the recovery points managed from the selected Site.

For more details, refer to the following topics in Arcserve UDP Solutions Guide:

- Start or Stop an Instant Virtual Machine
- Restart an Instant Virtual Machine
- Delete an Instant Virtual Machine
- Convert the Linux Instant Virtual Machine to an Independent Virtual Machine
- Migrate the Linux Instant Virtual Machine from Amazon EC2 to a Physical Machine
Troubleshooting

AWS EC2 Instances Monitor

Monitor Console/RPS/Proxy using functions provided by Amazon EC2

- Use Status Checks feature to check whether Amazon EC2 has detected any problem that might prevent your instances from running applications.  
  Note: For details, refer to How to configure Status Checks in AWS User Guide.
- Use CloudWatch to view metrics for CPU utilization, data transfer, and disk usage activity from Amazon EC2 instances for no additional cost. 
  For an additional cost, CloudWatch provides Detailed Monitoring for EC2 instances with higher resolution and metric aggregation.  
  Note: For details, refer to How to use CloudWatch in AWS User Guide.

Log into Console/RPS/Proxy to monitor the CPU/Memory/Disk usage. 
When the performance is low, you can resize the instance or attach a new volume

- Resize the instance to improve the performance. 
  For more details, refer to How to resize instance in AWS User Guide
- Attach new volume. 
  For more details, refer to How to Attach new volume to instance in AWS User Guide.

Arcserve UDP Function Troubleshooting

Troubleshooting on AWS EC2 when Linux Instant VM not started or unreachable

EC2 instances do not have a physical monitor through which you can view their console output. 

If you perform an Instant VM job to an AWS EC2 Instance, sometimes the Instance may:

- fail to start VM after the Instant VM job 
- become unreachable after the Instant VM job

Then, you can Get the Console Output of the Instance or Capture a Screenshot of the Instance for more useful information for troubleshooting.

Open the AWS EC2 Management Console

To get Console Output of the AWS EC2 Instance

Console output is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started.

- In the left navigation pane, select Instances, and then select the instance. 
- Select Actions, Instance Settings, Get System Log.
To Capture a Screenshot of the AWS EC2 Instance

If you are unable to reach your instance through SSH or RDP, you can capture a screenshot of your instance and view it as an image. This provides visibility to the status of the instance and allows quicker troubleshooting. There is no data transfer cost for this screenshot. The image is generated in JPG format, no larger than 100 KB.

1. In the left navigation pane, select Instances.
2. Select the instance to capture.
4. Right-click on the image to download and save it.
Arcserve UDP on AWS Cloud: Deployment Guide

Note: For more information, refer to AWS User Guide.

Troubleshooting Reference for Arcserve UDP

Refer to Release Notes of each version for Limitations and Known Issues on individual feature.

Refer to Arcserve UDP Solutions Guide Troubleshooting chapter for overall Troubleshooting.

Arcserve UDP Log Collections

- Arcserve UDP Console Logs under <Install Path>/Management/logs
- Arcserve UDP RPS, Proxy and Windows Agent Logs under <Install Path>/Engine/logs and <Install Path>/Engine/Configuration
- Arcserve UDP Linux Agent Logs under /opt/Arcserve/d2dserver/logs
Arcserve UDP on AWS Cloud: Deployment Guide

Scenario 4- Instant VM of Linux in AWS EC2 (Backup to Amazon S3 directly and Start Instant VM from AWS S3 in AWS EC2)

Arcserve UDP Linux Backup Server supports backup from Linux source node to Amazon S3 storage directly and starts Instant VM of Linux from Amazon S3 in AWS EC2. This feature is available in Arcserve Unified Data Protection v6.5.

Architecture

The scenario is applicable to such customers who want to use the Amazon S3 as the data storage and back up the data to Amazon S3 directly.

The customer needs to deploy a Linux Backup Server On-Premise and in AWS EC2. The local Linux Backup server can be used to perform Backup jobs and store the data to Amazon S3 directly. To use Amazon S3 as backup storage, the customer needs first to create a bucket that will be dedicated for backup storage. Cloud Linux Backup Server only needs to be started when you need to run restore functions such as Linux instant VM in cloud.

If the production machine is down because of the hardware failure or other reasons, the customer can start the Cloud Linux Backup Server to perform a Linux Instant VM in AWS EC2 from Amazon S3 directly, and then the new EC2 Instance can be ready to use within minutes.

With traditional BMR, you need to restore all the data first, and then reboot the Instance for use. But, with Linux instant VM, you can launch an EC2 Linux Instance within minutes as the production machine instead of restoring all the data first. Linux Instant VM can help to reduce the downtime of production machines and improve the RTO to minutes.

When a Linux Instant VM job in EC2 is performed, it will create an EC2 instance, restore some data and files related to system boot first, and then reboot the EC2 Instance. The Instance can be ready to use when the system boot is finished. At the backend, it will still retrieve the data from the recovery point if the data has not been recovered. But, this process is not aware of upper level applications.

If Linux Instant VM in EC2 is for your permanent use, you can enable automatic data recovery when the EC2 Instance is ready to use. Also, reboot is not required when recovery is complete.
Arcserve UDP on AWS Cloud: Deployment Guide

Planning Deployment

Planning Deployment requires the following options:

- Considerations
- Arcserve UDP Components required
- Prerequisites
- Deployment Steps

Considerations

Below are considerations for planning deployment in AWS EC2 and On-Premise site for the scenario Instant VM of Linux in AWS EC2 (Backup from On-Premise to Amazon S3 directly, start Instant VM from Amazon S3 in AWS EC2).

Important! Before deployment, refer to Arcserve UDP Release Notes and Compatibility Matrix to understand system requirements and supported Operating Systems for each component.

- Refer to Arcserve UDP v6.5 release notes for System Information on each component, and navigate to Product Update to view the latest v6.5 level system information.
- Refer to Arcserve UDP v6.5 Compatibility Matrix for supported Operating Systems.
- Refer to Arcserve UDP v6.5 release notes for Supported Languages.
- Refer to Arcserve Product Download page for detailed download link. We recommend the latest version.
Arcserve UDP Components required

Arcserve UDP Components Download

Important! This scenario is supported from Arcserve UDP version 6.5. We recommend deploying the latest Update. The installed component version on AWS or On-Premise must match.

- Unified Installer

  For new environment that does not have UDP installed before, we recommend utilizing unified installer to download and install the latest released update with v6.5 together.

    - Unified installer download link for v6.5 is ASDownloader.exe that always publishes the latest released Arcserve Products. This link includes not only Arcserve UDP, but also Arcserve Backup and Arcserve HA.
    - For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

    Note:

    - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
    - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration, or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- Product individual release download

  Arcserve Product Download page: You can get all Arcserve UDP version download link for individual package, we recommend installing the latest version.

  Arcserve UDP Agent (Linux) Download Links: You can get all Arcserve UDP Linux version download link. Select matched Arcserve UDP Linux version with Arcserve UDP Console.

    Note:

    - For new customer, we recommend downloading the remaster build and install to get the major release with the latest Update together.
    - For existing customer, we recommend downloading the individual Update package that has smaller size or select Check for Updates from Arcserve UDP Console.
    - Refer to individual Update Release Notes Installation Chapter for detailed steps or download link.
    - For more detailed steps, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.
Auto Update

Existing v6.5 UDP customer can automatically upgrade to the latest update by Check for Updates from Arcserve UDP Console Help menu or wait for scheduled time to automatically download the latest Update that is configured at Update Configuration (Default time: Sunday 3:00 AM).

Note: Arcserve UDP Linux Backup Server does not support Auto Update.

Arcserve UDP Components System Requirements for AWS EC2

- Arcserve Unified Data Protection Agent (Linux) Backup Server
  - RHEL 7.x, CentOS 7.x, SuSE SLES 12.x, Ubuntu 14.04, or above recommended
  - 4 GB RAM or above
  - 4 GB disk space for /tmp folder, 6 GB disk space for /opt folder as minimum disk space (Ext 2,3,4 & Reiser FS v3 file systems)

  Note: Refer to Arcserve UDP v6.5 Compatibility Matrix for supported Operating Systems

Arcserve UDP Components System Requirements for On-Premise

- Arcserve Unified Data Protection Console
  - Window 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

- Arcserve Unified Data Protection Agent (Linux) Backup Server
  - RHEL 7.x, CentOS 7.x, SuSE SLES 12.x, Ubuntu 14.04, or above recommended
  - 4 GB RAM or above
  - 4 GB disk space for /tmp folder, 6 GB disk space for /opt folder as minimum disk space (Ext 2,3,4 & Reiser FS v3 file systems)

- (Optional) Arcserve Unified Data Protection Host-Based Agentless Backup Proxy (to protect Linux VM in Hypervisor)
  - Window 2003 R2 Server or above
  - 1 x CPU with 4 core (2.7 GHz) or above
  - 10 GB or more
  - 8 GB RAM or above
Prerequisites

Prerequisites and General Configuration of AWS EC2:

- You must have Virtual Private Cloud (VPC) and Subnet created to run Linux Backup Server in AWS EC2.
  - You can find VPC settings at EC2 Management Console -> Services -> Networking & Content Delivery -> VPC.
    
    Access AWS EC2 Management Console.

  - You can find subnet settings at EC2 Management Console -> Services -> Networking & Content Delivery -> VPC -> Subnets.

- You must have a Public IP for Linux Backup Server in AWS that is used for Instant VM Proxy. Following are two ways to get public IP in AWS EC2:
  - Allocate Elastic IP and assign it to EC2 instance (Recommended)
  - Automatically assign when launching EC2 instance
You must have **AWS Access** and **Secret Keys** for a user with permission to manage AWS EC2.

- You can find Access key at **IAM -> Users -> Security Credentials**

You must have below **Ports** enabled in **Security Group Setting** on AWS.

- UDP Linux Backup Server:
  - Internet and Intranet Inbound 8014
  - Intranet Inbound 8016, 8017

**On-Premise Side Prerequisites and General Configuration:**

Prepare servers in advance to be deployed as Arcserve UDP Console, Recovery Point Server, Linux Backup Server, and those servers must meet system requirements for each component.

Servers in Arcserve UDP Console or Recovery Point Server role must be able to connect with the target instance in EC2.

**Deployment Steps**

Follow below steps to prepare Amazon S3 bucket and AWS EC2 instance first and then install required Arcserve UDP components and configure Instant VM of Linux in AWS EC2.

**Step1. Create an Amazon S3 bucket as Storage**

To use Amazon S3 as backup storage, you need to first create a bucket that will be dedicated for backup storage. Then, you can use this bucket as backup destination if it is a CIFS share when you configure Arcserve.
UDP plan with the backup task. The storage URL looks like “s3://bucket_name” (or “s3://China/bucket_name” for Amazon China). Fill key ID as username and fill key as password.

Note: This step can be skipped if you already have the Amazon S3 bucket created.

To Create an S3 bucket, follow these steps:

1. Sign into the AWS Management Console and open the Amazon S3 console using https://console.aws.amazon.com/s3/.
2. Click Create bucket.
3. In the Bucket name field, type a unique DNS-compliant name for your new bucket.
4. For Region, select desired region for the bucket to reside.
5. Click Create.

A bucket is created in Amazon S3. For more information, refer to Amazon S3 Getting Started Guide.

Step 2. Deploy Arcserve UDP Linux Backup Server (as Instant VM Proxy) on AWS EC2

Log into AWS EC2 Management Console using your AWS account

You can launch an Arcserve UDP Agent (Linux) instance directly using Amazon Machine Image (AMI) in AWS Cloud. After launching the Arcserve UDP Agent (Linux) instance, you can open the user interface from any computer using a web browser and the server is referred as the Backup Server.
For more details, refer to Install Arcserve UDP Agent (Linux) In AWS Cloud in Arcserve UDP Agent for Linux User Guide.

Launch AWS Instance at EC2 dashboard -> Instances -> Launch Instances

1. Search “Arcserve_Unified_Data_Protection_Agent_Linux” in Community AMIs, and select one AMI that matches your UDP Console version. For example, if your UDP Console version is v6.5 Update2 build number 4175.667, then you need to select AMI Arcserve_Unified_Data_Protection_Agent_Linux_6.5.4175.667.

2. Select an Instance Type.
   - Instance type t2.xlarge (Variable ECUs, 4 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 16 GiB memory, EBS only) is recommended.
   - Instance type t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only) is the minimal requirement.
   
   Note: Refer to the System Information for Linux Backup Server for detailed information. Other instance type with higher performance is recommended.
3. **Configure Instance Details.**

   **Step 2: Choose an Instance Type.**

   **Step 3: Configure Instance Details.**

   **Notes:**
   - Make sure the RPS and Linux backup server can connect to each other.
   - Enable *Auto-assign Public IP* if you do not want to use Elastic IP as auto-assign public IP cannot be changed after instance is launched.
   - Enable *CloudWatch* if you want to monitor detailed information.
   - Use dedicated instance if you want high performance.

4. **Add Storage for Instance**
Storage depends on your business requirement.
Minimum Storage: 40 GB
Recommended Storage: 80 GB

5. **Add Tag** for Instance.
   You can add tag for your instance to make it easy to find.

6. **Configure Security Group**.
   UDP Linux Backup Server require below Ports opened.
   - Internet and Intranet Inbound 8014
   - Intranet Inbound 8016, 8017

7. Review the instance configurations and launch it.
   After the AWS EC2 Instance is launched, Arcserve UDP Linux Backup Server will be running in this Instance. Browse [https://hostname:8014](https://hostname:8014) to verify if Linux Backup Agent Console is running properly (default user is udpuser).
Step 3. Arcserve UDP Console Installation for On-Premise

3.4 Download and Install UDP console

- Installation by Unified Installer
  - Unified installer download link for v6.5 is ASDownloader.exe.
  - For more information, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  Notes:
  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration, or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- Installation by Setup Wizard
  - Access Arcserve Product Download page to get all UDP version download link for individual package. We recommend installing the latest version.
  - For more information, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

3.5 Launch Arcserve UDP Console from Start Menu after installation is complete

Arcserve UDP Console will be launched in browser like https://console_hostname:8015/ (for example, protocol and port need to match your setup configuration). Log into Console using correct Account and Password.
Step 4. On-Premise Arcserve UDP Linux Backup Server Installation and Configuration

- Download Arcserve UDP Agent (Linux) build
  
  Open All Arcserve UDP Linux Download Links and select one Arcserve UDP Linux build that matches the Arcserve UDP console version.

- Install the Arcserve UDP Agent (Linux) Backup Server on the target server by following the steps in guide Install Arcserve UDP Agent (Linux)

Step 5. On-Premise Arcserve UDP Console Node Management

5.1 Create an Amazon S3 bucket on Arcserve UDP Console Cloud Accounts

You can create a bucket on AWS management console as mentioned in Step1 or create bucket directly in Arcserve UDP Console.

You can add a cloud account under UDP Console -> resources -> Destination -> Cloud Accounts -> Add a Cloud Account.

The bucket you created can be used in Backup plan configuration in the next step. For Linux backup to S3, you will need to manually add it as CIFS share there.

Note: For more information, refer to Add a Cloud Account in Arcserve UDP Solutions Guide.
5.2 Add On-Premise Linux Backup Server installed in Step4 on UDP Console->resources->All Nodes->Add Nodes->Add Linux Backup Server Node.

Refer to screenshot below or Arcserve UDP Solutions Guide Add Nodes topic.

Refer to the Compatibility Matrix to view supported Operating Systems for Linux Backup Server.

5.3 Add On-Premise Linux Node as target protected node on UDP Console->resources->All Nodes->Add Nodes->Add Linux Node.

Refer to screenshot below or Arcserve UDP Solutions Guide Add Nodes topic.

All target protected Linux nodes need to be added one by one so that could be add into Plan to protect in next step.

Refer to the Compatibility Matrix to view supported Operating Systems for Linux Node.
Step 6. On-Premise Arcserve UDP Console Configure Plan with Backup Task

To enable Linux IVM to AWS EC2 for this scenario, configure a plan with backup and replication task and complete that job in advance.

6.1 Add a Plan on UDP Console -> resource -> All Plans -> Add a Plan

Create a plan and name it, as in below screenshot.

6.2 Add a Linux Backup Task

Follow these steps to add a Linux Backup task as the first task on this new plan:

Note: For more information, refer to How to Create a Linux Backup Plan in Arcserve UDP Solutions Guide.

1. From Task Type, select Backup: Agent-Based Linux.
2. From Source, select Linux Backup Server (Select the On-Premise Linux Backup Server added in Step 5.2).
3. From Source, select Node by clicking Add (Select the On-Premise Linux node added in Step 5.3).
4. From Destination, configurations
   a) Select Local disk or shared folder as Destination Type.
   b) Select CIFS share, and manually type the Amazon S3 storage in the following format:

   s3://<Region ID>/<Bucket Name>
   - Shortcut for Amazon S3 Global: s3://<Bucket Name>
   - Shortcut for Amazon S3 China: s3://China/<Bucket Name>

   c) Click arrow and provide Amazon S3 access information.

5. From Schedule, configure backup schedule.
6. From Advanced, configure any Pre/Post Script or Email alert.
7. Save the plan.
Step 7. Create and Manage Instant Virtual Machine on AWS EC2

Prerequisites:

- **Create Access Key ID and Secret Access Key on AWS Management Console**

  Launch Instant VM needs to use the access key for API calls, **Access Key ID** and **Secret Access Key** to prepare in advance under AWS Management Console for your AWS account.

  You can create, rotate, disable, or delete access keys (access key IDs and secret access keys) for your AWS account root user. Anyone who has an access key for your AWS account has unrestricted access to all the resources in your account, including the billing information.

  When you create an access key, AWS gives you an opportunity to view and download the secret access key only once. If you do not download it or if you lose it, you can delete the access key and then create a new one.

  **Note:** For more information, refer to Managing Access Keys for Your AWS Account in AWS Documentation.

- **Add a Cloud Account for AWS EC2 in UDP Console**

  Navigate to UDP Console->resources->Destinations->Cloud Account->Add a Cloud Account

  **Note:** For more information, refer to Add a Cloud Account in Arcserve UDP Solutions Guide.

  Select Storage Service as **Amazon EC2** in the Add a Cloud Account dialog.

  - **Access Key ID**
    
    Identifies the user who is requesting access to this location.

  - **Secret Access Key**
    
    Refers to a password that is used to verify the authenticity of the request to access this location because your Access Key is not encrypted.

    **Important!** This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials at a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

  - **Proxy Settings (only when UDP Console must use Proxy to connect to AWS)**
    
    Specifies the proxy server settings. Select the check box of **Connect using a proxy server** if you want to enable this option. If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for
internet connections. You can also select this option if your proxy server requires authentication. Then, you must provide the corresponding authentication information (Domain Name|Username and Password) that is required to use the proxy server.

- **Add the Linux Backup Server in AWS EC2 to UDP Console as Linux IVM proxy**
  
  Navigate to UDP Console -> resources -> All Nodes -> Add Nodes -> Add Linux Backup Server Node to add this Linux Backup server, similar as in Step 5.2.
  
  **Note:** The default user is udpuser for the Linux Backup Server in AWS.

- **Need Backup task completed successfully**
  
  **Create an Instant VM on Node Management View or Destination Management view.**
  
  Creating an Instant VM involves the following five major steps:
  
  **Note:** For more information, refer to How to Create and Manage an Instant Virtual Machine on Amazon EC2 in Arcserve UDP Solutions Guide.

1. Open the Instant VM Wizard from UDP Console.
   
   Instant VM Wizard can be launched for specified Linux node from Node Management View or Destination Management View by selecting Create an Instant VM after right click on the Linux Node.
   
   **Note:** For more information, refer to Open the Instant VM wizard in Arcserve UDP Solutions Guide.

2. Select a Recovery Point that stored in Amazon S3 storage.
   
   **Note:** For more information, refer to Select the recovery point in Arcserve UDP Solutions Guide.
Select VM Location to launch Instant VM.

Specify **Cloud Type** as Amazon EC2 and the **Account Name** that you prepared in advance to create the Instant VM.

**Note:** For more information, refer to Select the VM location in Arcserve UDP Solutions Guide.

3. Select a Recovery Server to run Instant VM.

Specify the Linux Backup Server in AWS EC2 as proxy to run Instant VM.

**Note:** For more information, refer to Select the recovery server in Arcserve UDP Solutions Guide.
4. Specify the following Instant VM machine details for AWS EC2 Cloud Instance:

**VM Name**
Specifies the name of the Instant VM. The name of the source node prefixed with “UDPIVM_” becomes the default name of the Instant VM. You can modify the name. Some special characters, such as `@`, \ and so on, are not allowed in the name.

**Description**
(Optional) Specifies the description for the Instant VM.

**Region**
Specifies the region of your Amazon EC2 account.

**Instance Type**
Specifies the supported instance type.

**Volume Type**
Specifies the type of volume.

**Network**
Specifies the network existing on the Amazon EC2 account.

**Subnet**
Specifies the subnet existing on the Amazon EC2 account.

**Auto-assign Public IP**
Specifies the public IP assigned to the VM.
Primary IP
Specifies the primary IP of VM. Specifies automatically if you do not specify.

Select a Security Group
Specifies the security group. You can select multiple groups. If you do not select, automatically creates a new security group.

Advance: Change Host Name
Specifies the host name of new VM.

Advance: Recover data automatically after Instant VM is started
Specifies if data recovery takes place automatically, after creating the Instant VM.

Note: For more information, refer to Specify the Instant VM details in Arcserve UDP Solutions Guide.

5. Submit the Instant VM job

After Virtual Machine Settings configuration, click Finish.

When Boot VM dialog open, select Boot Now, Boot Later option

Boot Now: Automatically starts the VM after creating the VM.

Boot Later: You can start the VM manually after the Instant VM job is complete.

The Instant VM job is successfully created.

After the job is complete, you can view the Instant VM at resources, Infrastructure, Instant Virtual Machine.
Note: For more information, refer to Submit the Instant VM job in Arcserve UDP Solutions Guide.

Manage an Instant Virtual Machine

You can manage the Instant VM from Console. You can power-on or power-off an Instant VM from the UDP Console. Also, you can delete any Instant VM.

Note: The UDP Console displays only those Instant VM that are created from the recovery points managed from the selected Site.

For more details, refer to the following topics in Arcserve UDP Solutions Guide:

- Start or Stop an Instant Virtual Machine
- Restart an Instant Virtual Machine
- Delete an Instant Virtual Machine
- Convert the Linux Instant Virtual Machine to an Independent Virtual Machine
- Migrate the Linux Instant Virtual Machine from Amazon EC2 to a Physical Machine
Troubleshooting

**AWS EC2 Instances Monitor**

Monitor Console/RPS/Proxy using functions provided by Amazon EC2

- **Use Status Checks** feature to verify whether Amazon EC2 has detected any problems that might prevent your instances from running applications. 
  
  **Note:** For more details, refer to [How to configure Status Checks](#) in AWS User Guide.

- **Use CloudWatch** to view metrics for CPU utilization, data transfer, and disk usage activity from Amazon EC2 instances for no additional cost. For an additional cost, CloudWatch provides detailed monitoring for EC2 instances with higher resolution and metric aggregation.
  
  **Note:** For more details, refer to [How to use CloudWatch](#) AWS User Guide.

Log into Console/RPS/Proxy to monitor the CPU/Memory/Disk usage.

When the performance is low, you can resize the instance or attach a new volume

- Resize the instance to improve the performance.
  
  For more details, refer to [How to resize instance](#) in AWS User Guide.

- Attach new volume
  
  For more details, refer to [How to Attach new volume to instance](#) in AWS User Guide.

**Arcserve UDP Function Troubleshooting**

Troubleshooting on AWS EC2 when Linux Instant VM is not started or unreachable

EC2 instances do not have a physical monitor through which you can view their console output. If you perform an Instant VM job to an AWS EC2 Instance, sometimes the Instance may:

- fail to start VM after the Instant VM job
- become unreachable after the Instant VM job

Then, you can get the [Console Output of the Instance](#) or [Capture a Screenshot of the Instance](#) for more useful information for troubleshooting.

Open the [AWS EC2 Management Console](#).

To get Console Output of the AWS EC2 Instance

Console output is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started.

- In the left navigation pane, select Instances, and select the instance.
- Select Actions, Instance Settings, Get System Log.
To Capture a Screenshot of the AWS EC2 Instance

If you are unable to reach your instance through SSH or RDP, you can capture a screenshot of your instance and view it as an image. This provides visibility to the status of the instance and allows for quicker troubleshooting. There is no data transfer cost for this screenshot. The image is generated in JPG format, no larger than 100 KB.
In the left navigation pane, select Instances.
Select the instance to capture.
Select Actions, Instance Settings, Get Instance Screenshot.
Right-click on the image to download and save it.
Note: For more information, refer to AWS User Guide.

Troubleshooting Reference for Arcserve UDP

Refer to Release Notes of each version for Limitations and Known Issues on individual feature.

Refer to Arcserve UDP Solutions Guide Troubleshooting chapter for overall Troubleshooting.

Arcserve UDP Log Collections

- Arcserve UDP Console Logs under <Install Path>/Management/logs
- Arcserve UDP RPS, Proxy and Windows Agent Logs under <Install Path>/Engine/logs and <Install Path>/Engine/Configuration
- Arcserve UDP Linux Agent Logs under /opt/Arcserve/d2dserver/logs
Scenario 5– File Copy/File Archive to AWS S3 (Protect data files from On-Premise to AWS S3)

File Copy/File Archive to AWS S3 feature supports protecting on-premise files in AWS S3 Cloud. First, backup will run on on-premise servers then the files are copied to AWS S3 buckets using File Copy/File Archive task. This feature is available from Arcserve Unified Data Protection V5.0 Update 4 (we recommend using it from the latest UDP 6.5 version).

Architecture

File Copy

The scenario is for the customers who have already deployed the data protection solution on-premise and want to protect the data files in AWS Cloud as one more copy.

File Archive

The scenario is applicable to such customers who have already deployed the data protection solution on-premise and want to protect the data files in AWS Cloud as one more copy and delete the source data files from on-premise servers.

The on-premise solution comprises of UDP console, RPS server and UDP Agents. The customers can back up their nodes to Local Machine, Remote Share or RPS. After successful backup, File Copy/File Archive Task reads the backed-up data and copies the data files configured in the plan to AWS S3 cloud. During this process, it accesses the AWS S3 Cloud and creates the S3 bucket with the given access details in Console.

You can restore the data files from AWS S3 cloud using restore options.
Planning Deployment

Planning Deployment requires the following options:

- Considerations
- Arcserve UDP Components required
- Prerequisites
- Deployment Steps

Considerations

Below are considerations for planning to protect the data files in AWS S3 from On-Premise (Backup to Local Destination or Remote Shares or RPS and then File Copy/File Archive to AWS S3).

Important! Before deployment, refer to Arcserve UDP Release Notes and Compatibility Matrix to understand system requirements and supported Operating Systems for each component.

- Refer to Arcserve UDP v6.5 release notes for System Information on every component, and navigate to Product Update to view the latest v6.5 level system information.
- Refer to Arcserve UDP v6.5 Compatibility Matrix for supported Operating Systems.
- Refer to Arcserve UDP v6.5 release notes for Supported Languages.
- Refer to Arcserve Product Download page for detailed download link. We recommend the latest version.

Arcserve UDP Components required

Arcserve UDP Components Download

Important! This scenario is supported from Arcserve UDP Version 5.0. We recommend deploying the latest Version 6.5 with Update is recommended.

- Unified Installer

For new environment that does not have UDP installed before, we recommend utilizing unified installer to download and install latest released update with v6.5 together.

- Unified installer download link for v6.5 is ASDownloader.exe that always publishes the latest released Arcserve Products. This link includes not just Arcserve UDP, but also Arcserve Backup and Arcserve HA.
- For detailed steps, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

Note:

- When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
- When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration, or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.
Product Individual Release Download
Arcserve Product Download Page: You can get all Arcserve UDP version download link for individual package. We recommend installing the latest version.
Arcserve UDP Agent (Linux) Download Links: You can get all Arcserve UDP Linux version download link, and require select matched Arcserve UDP Linux version with Arcserve UDP Console.

Note:
- For new customer, we recommend downloading the remaster build to install the major release with the latest Update together.
- For existing customer, we recommend downloading the individual Update package that has smaller size, or click Check for Updates from Arcserve UDP Console.
- Refer to individual Update Release Notes Installation Chapter for detailed steps or download link.
- For more information, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

Auto Update
Existing v6.5 UDP customer can automatically upgrade to the latest update by using Check for Updates from Arcserve UDP Console Help menu or wait for scheduled time to automatically download the latest Update that is configured at Update Configuration (Default time: Sunday 3:00 AM).

Arcserve UDP Components System Requirements for On-Premise

Arcserve Unified Data Protection Console
- Windows 2008 R2 Server or above
- 1 x CPU with 4 Core (2.7 GHz) or above
- 40 GB (for OS installation)
- 8 GB RAM or above
- Backup Storage – depends on your source data size

Arcserve Unified Data Protection Recovery Point Server
- Windows 2008 R2 Server or above
- 1 x CPU with 4 Core (2.7 GHz) or above
- 40 GB (for OS installation)
- 8 GB RAM or above
- Backup Storage – depends on your source data size
Arcserve UDP on AWS Cloud: Deployment Guide

- **Arcserve Unified Data Protection Agent**
  - Windows 2003 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 4 GB RAM or above
  - Backup Storage – depends on your source data size

**Prerequisites**

*AWS S3 Prerequisites and General Configuration:*

- You must have **AWS Access** and **Secret Keys** for a user with permission to manage AWS S3.

  You can find Access key at **IAM -> Users -> Security Credentials**

- To see S3 Buckets created in UDP Console.
  - Log into **AWS Console -> Services -> S3**
    - Access **AWS S3 Management Console**.
On-Premise Prerequisites and General Configuration:

Prepare servers in advance to be deployed as Arcserve UDP Console, Recovery Point Server, Agent servers and those servers must meet system requirements for each component.

UDP Agent servers must be able to connect to target AWS S3.

Deployment Steps

Follow below Steps to install required Arcserve UDP components.

Step 1. On-Premise Arcserve UDP Console Installation

1. Download the latest Arcserve UDP v6.5 installation package to install Console

   - Installation by Unified Installer
     - Unified installer download link for v6.5 is ASDownloader.exe.
     - For more information, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

   - Installation by Setup Wizard
     - Arcserve Product Download page: You can get all UDP version download link for individual package. We recommend installing the latest version.
     - For more information, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

   Note:
   - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
   - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.
1.2 Download and Install UDP RPS and Agents

- **Installation by Unified Installer**
  - Unified installer download link for v6.5 is `ASDownloader.exe`.
  - For more information, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**
  - When the **Choose Components to Download** dialog opens, select **Arcserve UDP** that will only download the latest package of Arcserve UDP.
  - When the **Installation Method** dialog opens, select **Express Installation** mode to install RPS as default configuration or select **Advanced Installation** mode to install components separately and then you can customize the installation path and protocol.

- **Installation by Setup Wizard**
  - Arcserve Product Download page: You can get all UDP version download link for individual package. We recommend installing the latest version.
  - For more information, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

**Step 2. Launch Arcserve UDP Console after installation completed from Start Menu**

Arcserve UDP Console will be launched in browser like `https://console_hostname:8015/` (for example, protocol and port need to match your setup configuration).
Log into Console with correct Account and Password.
Step 3. On-Premise Arcserve UDP Recovery Point Server Installation and Configuration

Arcserve UDP Recovery Point Server can be deployed from Arcserve UDP Console, or add it to Console after RPS Server is installed on that server.

Below are steps to add an RPS server on UDP Console and remotely deploy RPS to that server that does not have RPS server installed.

3.1 Launch Arcserve UDP Console

3.2 Add an RPS server On UDP Console-> resources-> Destination -> Add a Recovery Point Server and RPS server will be automatically deployed to the target server.

**Note:** For more information, refer to Add a Recovery Point Server in Arcserve UDP Solutions Guide.

RPS Server will be automatically deployed to that server according to the setting you configured. The default settings are displayed in the below screenshot.

3.3 Create a Data Store on UDP Console-> resources-> Destination -> Recovery Point Servers

Follow these steps to create a data store:

**Note:** For more information, refer to Add a Data Store in Arcserve UDP Solutions Guide.

1. Select the RPS server added in the last step.
2. Right click the server in the Centre Pane and select Add a Data Store from the drop-down menu.
3. Create a Data Store.
4. After the data store is created, verify the destination.

   After completing all the procedures involved in adding an RPS, verify if the RPS is added successfully.

   For more information, refer to Verify the Destination in Arcserve UDP Solutions Guide.

3.4 Add On-Premise Windows Node as target protected node on UDP Console->resources->All Nodes->Add Nodes->Add Windows Node

   Refer to screenshot below or Add Nodes in Arcserve UDP Solutions Guide;

   Refer to the Compatibility Matrix to view supported Operating Systems for Windows Node.
3.5 Add a Cloud Account for AWS S3 in UDP Console

Navigate to UDP Console > resources > Destinations > Cloud Account > Add a Cloud Account

*Note:* For more information, refer to [Add a Cloud Account](https://arcserve.com) in Arcserve UDP Solutions Guide.

- **Access Key ID**
  Identifies the user who is requesting access to this location.

- **Secret Access Key**
  Refers to a password that is used to verify the authenticity of the request to access this location because your Access Key is not encrypted.

  **Important:** This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials at a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

- **Proxy Settings (only when UDP Console must use Proxy to connect to AWS)**
  Specifies the proxy server settings. Select the check box of Connect using a proxy server if you want to enable this option. If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections. You can also select this option if your proxy server requires authentication. Then, you must provide the corresponding authentication information (Domain Name, Username, and Password) that is required to use the proxy server.
**Step 4. On-Premise Arcserve UDP Console Configure Plan with Backup and File Copy Task**

To enable File Copy to AWS S3 for this scenario, you need to configure a plan with backup and complete that job in advance.

4.1 **Add a Plan on UDP Console->resource->All Plans->Add a Plan**

Create a plan and name it, as in below screenshot.

4.2 **Add a Windows Backup Task**

Follow these steps to Add a Windows Backup task as the first task on this new plan.

   **Note**: For more information, refer to [How to Create a Windows Backup Plan](#) in Arcserve UDP Solutions Guide.

a. From Task Type, select **Backup: Agent-Based Windows**.

b. From Source, select Node by clicking **Add**.

c. From Destination, you can select Destination as Local Disk or Shared Folder or you can select **Arcserve UDP Recovery Point Server** as Destination Type (select the RPS added in Step 3.2 and Data Store created in Step 3.3).

d. From Schedule, configure backup schedule (To run CRP, only Daily, Weekly and Monthly Schedules are supported).

e. From Advanced, configure any Pre/Post Script or Email alert.

f. Save the plan (optional).

   **Note**: You can click Save the plan after all tasks are configured.

4.3 **Add a File Copy Task to the Plan**

After backup task configured, add a File Copy task that will copy your backup data from backup destination to target AWS S3 Bucket.

For more information, refer to [Add a File Copy Task to the Plan](#) in Arcserve UDP Solutions Guide.

In Task2: File Copy
1. In the Source tab, select the Type of recovery Point and click Add Source Path to configure the files to be copied to AWS S3 Cloud.

2. In the Source tab, select the Type of Recovery Point and click Add Source Path to configure the files to be copied to AWS S3 Cloud. You can also configure a filter.
3. Set Destination, select the Cloud Account created already in section 3.5.

4. Set Schedule.

4.4 Save the plan with Backup and File Copy task that will run as per schedule configured.

4.5 Add a File Archive Task to the Plan

**Note:** After successful copy of Source data files the File Archive task deletes the source data files from on-premise servers.

After backup task configured, add a File Archive task that will copy your backup data from the backup destination to target AWS S3 Bucket and delete the Source data files.

For more information, refer to **Add a File Archive Task to the Plan in Arcserve UDP Solutions Guide**.

In Task2: File Archive

1. In the Source tab, click Add Source Path and configure the files path to be copied to AWS S3 Cloud and delete after copy.
2. In the Add Source path, you can configure Filter as shown below.
3. Set Destination, select the Cloud Account created already in section 3.5.

**Note:** If File Copy and File Archive are configured in the same plan, then the same Cloud account cannot be configured for File Copy and File Archive.

4. Set Schedule.

4.4 Save the plan with Backup and File Archive task that will run as per schedule configured.
Step 5. Restore Files from AWS S3 Cloud

5.1 Select the node in Console-> Resources-> All nodes and right click on it as shown below and select Restore option.

5.2 Restore Window takes you to UDP Agent login as shown below. Provide the access details for UDP Agent login.
5.3 Select Restore Option and then select Browse Recovery Points
5.4 Select Cloud Account and select the files to restore as shown below

5.5 Select the destination to restore the files
**Troubleshooting**

**Arcserve UDP Function Troubleshooting**

*Troubleshooting Reference for Arcserve UDP*

1. Verify the internet connectivity on Agent
2. Verify if valid access key and secret key are used

Refer to Release Notes of each version for Limitations and Known Issues on individual feature.

Refer to Arcserve UDP Solutions Guide *Troubleshooting* chapter for overall Troubleshooting.

*Note: For more information, refer to* [AWS S3 Guide](#)

**Arcserve UDP Log Collections**

- Arcserve UDP Console Logs under `<Install Path>\Management\logs`
- Arcserve UDP RPS and Windows Agent Logs under `<Install Path>\Engine\logs` and `<Install Path>\Engine\Configuration`
Scenario 6– Copy Recovery Points to AWS S3 (Protect data from On-Premise to AWS S3)

Copy Recovery Points to AWS S3 feature supports protecting on-premise data in AWS Cloud. First, backup will run on on-premise servers. Then, the data is copied to AWS S3 buckets using Copy Recovery Points task. This feature is available in Arcserve Unified Data Protection v6.5.

Architecture

The scenario is applicable to such customers who have already deployed the data protection solution at on-premise and want to protect the same data in AWS Cloud as one more copy.

The on-premise solution comprises of UDP console, RPS server, and UDP Agents. The customers can back up their nodes to Local Machine, Remote Share or RPS. After successful backup, then Copy Recovery Points Task reads the backed-up data and copies the same to AWS S3 cloud. During this process, it accesses the AWS S3 Cloud and creates the S3 bucket with the given access details in Console.

To recover the data or machine, you need to Download the Recovery Point from Cloud, mount and restore the data or perform a normal BMR.

Figure, Copy Recovery Point to AWS S3 (Backup to Local destination or Remote Share or RPS, Copy Recovery Point to RPS in AWS S3)
Planning Deployment

Planning Deployment requires the following options:

- Considerations
- Arcserve UDP Components required
- Prerequisites
- Deployment Steps

Considerations

Below are considerations for planning to protect the data in AWS S3 from On-Premise (Backup to Local Destination or Remote Shares or RPS, then Copy Recovery Point to AWS S3).

Important! Before deployment, refer to Arcserve UDP Release Notes and Compatibility Matrix to understand system requirements and supported Operating Systems for each component.

- Refer to Arcserve UDP v6.5 release notes for System Information on each component, and navigate to Product Update view the latest v6.5 level system information.
- Refer to Arcserve UDP v6.5 Compatibility Matrix for supported Operating Systems.
- Refer to Arcserve UDP v6.5 Release Notes for Supported Languages.
- Refer to Arcserve Product Download page for detailed download link. We recommend the latest version.

Arcserve UDP Components required

Arcserve UDP Components Download

Important! This scenario is supported from Arcserve UDP Version 6.5 and deploying the latest Update is recommended.

- Unified Installer

For new environment that does not have UDP installed before, we recommend utilizing unified installer to download and install latest released update with v6.5 together.

- Unified installer download link for v6.5 is ASDownloader.exe that always publishes the latest released Arcserve Products. This link includes not just Arcserve UDP, but also Arcserve Backup and Arcserve HA.
- For more information, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

Note:

- When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
- When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration, or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.
Arcserve UDP on AWS Cloud: Deployment Guide

- **Product individual release download**

  Arcserve [Product Download page](#): You can get all Arcserve UDP version download link for individual package, we recommend latest version to install.

  Arcserve [UDP Agent (Linux) Download Links](#): You can get all Arcserve UDP Linux version download link, and require select matched Arcserve UDP Linux version with Arcserve UDP Console.

  **Note:**
  - For new customer, we recommend downloading the remaster build to install that will install the major release with the latest Update together.
  - For existing customer, we recommend downloading the individual Update package that has smaller size, or select **Check for Updates** from Arcserve UDP Console.
  - Refer to individual Update Release Notes Installation Chapter for detailed steps or download link
  - Refer to Arcserve UDP Solutions Guide [Install Arcserve UDP Using the Setup Wizard](#) chapter for detailed steps.

- **Auto Update**

  Existing v6.5 UDP customer can automatically upgrade to latest update by **Check for Updates** from Arcserve UDP Console **Help** menu automatically or wait for scheduled time to automatically download latest Update that is configured at **Update Configuration** (Default time: Sunday 3:00 AM).

**Arcserve UDP Components System Requirements for On-Premise**

- **Arcserve Unified Data Protection Console**
  - Windows 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size

- **Arcserve Unified Data Protection Recovery Point Server**
  - Windows 2008 R2 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 8 GB RAM or above
  - Backup Storage – depends on your source data size
Arcserve on AWS Cloud: Deployment Guide

- **Arcserve Unified Data Protection Agent**
  - Windows 2003 Server or above
  - 1 x CPU with 4 Core (2.7 GHz) or above
  - 40 GB (for OS installation)
  - 4 GB RAM or above
  - Backup Storage – depends on your source data size

**Prerequisites**

**AWS S3 Side Prerequisites and General Configuration:**

- You must have **AWS Access** and **Secret Keys** for a user with permission to manage AWS S3.
  
  You can find Access key at **IAM -> Users -> Security Credentials**

  ![AWS IAM Security Credentials](image)

- To see S3 Buckets created in UDP Console
  - Log into **AWS Console -> Services -> S3**
  - Access **AWS S3 Management Console.**
On-Premise Side Prerequisites and General Configuration:

Prepare servers in advance to be deployed as Arcserve UDP Console, Recovery Point Server, Agent servers and those servers must meet system requirements for each component.

UDP Agent servers must be able to connect to target AWS S3.

Deployment Steps

Follow these steps to install required Arcserve UDP components:

Step 1. On-Premise Arcserve UDP Console Installation

1. Download the latest Arcserve UDP v6.5 installation package to install Console

   - Installation by Unified Installer
     - Unified installer download link for v6.5 is ASDownloader.exe.
     - For more information, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

   - Installation by Setup Wizard
     - Arcserve Product Download page: You can get all UDP version download link for individual package. We recommend installing the latest version.

   Note:
   - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
   - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.
1.2 Download and Install UDP RPS and Agents

- Installation by Unified Installer
  - Unified installer download link for v6.5 is ASDownloader.exe.
  - For more information, refer to Install Arcserve UDP Using the Unified Installer in Arcserve UDP Solutions Guide.

  **Note:**
  - When the Choose Components to Download dialog opens, select Arcserve UDP that will only download the latest package of Arcserve UDP.
  - When the Installation Method dialog opens, select Express Installation mode to install RPS as default configuration or select Advanced Installation mode to install components separately and then you can customize the installation path and protocol.

- Installation by Setup Wizard
  - Arcserve Product Download page: You can get all UDP version download link for individual package, we recommend latest version to install.
  - For more information, refer to Install Arcserve UDP Using the Setup Wizard in Arcserve UDP Solutions Guide.

**Step 2. Launch Arcserve UDP Console from Start Menu after completing installation**

Arcserve UDP Console will be launched in browser like https://console_hostname:8015/ (for example, protocol and port needs to match your setup configuration).

Log into Console with correct Account and Password.
Step 3. On-Premise Arcserve UDP Recovery Point Server Installation and Configuration

Arcserve UDP Recovery Point Server can be deployed from Arcserve UDP Console, or add it to Console after RPS Server is installed on that server.

Follow these steps to add an RPS server on UDP Console and remotely deploy RPS to the server that does not have RPS server installed.

3.1 Launch Arcserve UDP Console.
3.2 Add an RPS server On UDP Console -> resources -> Destination -> Add a Recovery Point Server and RPS server will be automatically deployed to the target server.

Note: For more information, refer to Add a Recovery Point Server in Arcserve UDP Solutions Guide.

RPS Server will be automatically deployed to that server according to the setting you configured. The default settings are displayed in the below screenshot.

3.3 Create a Data Store on UDP Console -> resources -> Destination -> Recovery Point Servers

Follow these steps to Create a Data Store:

Note: For more information, refer to Add a Data Store in Arcserve UDP Solutions Guide.

1. Select the RPS server added in the last step.
2. Right click the server in Centre Pane and select Add a Data Store from the drop-down menu.
3. Create a Data Store
4. After the data store is created, verify the destination.

After completing all the procedures involved in adding an RPS, verify if the RPS is added successfully.

Refer to Arcserve UDP Solutions Guide Verify the Destination topic for more details.

3.4 Add On-Premise Windows Node as target protected node on UDP

Console->resources->All Nodes->Add Nodes->Add Windows Node

Refer to screenshot below or Arcserve UDP Solutions Guide Add Nodes topic.

Refer to the Compatibility Matrix for supported Operating Systems for Windows Node.
3.5 Add a Cloud Account for AWS S3 in UDP Console

Navigate to UDP Console>resources>Destinations>Cloud Account>Add a Cloud Account

Note: For more information, refer to Add a Cloud Account in Arcserve UDP Solutions Guide.

- **Access Key ID**
  Identifies the user who is requesting access to this location.

- **Secret Access Key**
  Refers to a password that is used to verify the authenticity of the request to access this location because your Access Key is not encrypted.
  
  **Important!** This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials at a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

- **Proxy Settings (only when UDP Console must use Proxy to connect to AWS)**
  Specifies the proxy server settings. Select the check box of Connect using a proxy server if you want to enable this option. If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections. You can also select this option if your proxy server requires authentication. Then, you must provide the corresponding authentication information (Domain Name\Username and Password) that is required to use the proxy server.
Step 4. On-Premise Arcserve UDP Console Configure Plan with Backup and Copy Recovery Point Task

To enable Copy Recovery Point to AWS S3 for this scenario, need to configure a plan with backup and complete that job in advance.

4.1 Add a Plan on UDP Console->resource->All Plans->Add a Plan

Create a plan and name it, as displayed in below screenshot.

4.2 Add a Windows Backup Task

Follow these steps to Add a Windows Backup task as the first task on this new plan.

Note: For more information, refer to How to Create a Windows Backup Plan in Arcserve UDP Solutions Guide.

1. From Task Type, select Backup: Agent-Based Windows.
2. From Source, select Node by clicking Add.
3. From Destination, select Destination as Local Disk or Shared Folder or you can select Arcserve UDP Recovery Point Server as Destination Type (select the RPS added in Step 3.2 and Data Store created in Step 3.3).
4. From Schedule, configure backup schedule (To run CRP, Only Daily, Weekly and Monthly Schedules supported).
5. From Advanced, configure any Pre/Post Script or Email alert.
6. Save the plan (optional).
7. Note: You can click Save the plan after all tasks are configured.

4.3 Add a Copy Recovery Points Task

After backup task configured, add a Copy Recovery Points task that will copy your backup data from backup destination to target AWS S3 Bucket.

For more information, refer to Add a Copy Recovery Points Task to the Plan in Arcserve UDP Solutions Guide.

In Task2: Copy Recovery Points
1. Select the Source. You can select all or multiples or any one.

2. Set Copy Settings, select the Cloud Account created already in section 3.4.

3. Set Schedule for Copy.

4.4 Save the plan with Backup and Copy Recovery Points task that will run as per schedule configured.
Step 5. **Download Recovery Point from Cloud**

5.1 Select the node in Console-> Resources->All nodes and right click on it as shown below.

5.2 Select the Session as shown below.

5.3 Provide the destination, Compression and Encryption details and click Finish as shown below.

5.4 You can view the Recovery Point in Destination mentioned in section 6.3 once it is completed.
Troubleshooting

Arcserve UDP Function Troubleshooting

Troubleshooting Reference for Arcserve UDP

a. Verify the internet connectivity on Agent.
b. Verify if valid access key and secret key are used.

Refer to Release Notes of each version for Limitations and Known Issues on individual feature.

For more information, refer to Troubleshooting chapter for overall Troubleshooting.

Note: For more information, refer to AWS S3 Guide.

Arcserve UDP Log Collections

- Arcserve UDP Console Logs under <Install Path>/Management/logs
- Arcserve UDP RPS and Windows Agent Logs under <Install Path>/Engine/logs and <Install Path>/Engine/Configuration