Disaster Recovery (Direct Customers) User Guide

Arcserve UDP Cloud Direct

v6.2.2

arcserve

Legal Notice

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

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

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

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

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

The manufacturer of this Documentation is Arcserve.

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

Contact Arcserve Support

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

Contact Support

With Arcserve Support:

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

Contents

Chapter 1: Understanding UDP Cloud Data Protection

This section contains the following topics:

Introduction

The Arcserve UDP Cloud Direct Disaster Recovery solution enables customers to protect and recovery on-premises servers in the Arcserve Cloud to guard against potential disruptions to their business operations. The solution provides protection for physical and virtual (VMware and Hyper-V) servers running Windows or Linux operating systems. With UDP Cloud Direct, customers are able to achieve business continuity by restoring data from the Arcserve Cloud.

The Arcserve UDP Cloud Direct Disaster Recovery solution has three primary components:

- **UDP Cloud Direct Agent** – lightweight software application that easily installs on a server, and enables the creation of a backup image of the server. The agent transfers the backup image and subsequent restore points to the Arcserve Cloud for off-site protection.
- **UDP Cloud Direct Portal** – web-based interface that enables administration of server backups and server recovery in the Arcserve Cloud.
- **Arcserve Cloud** – cloud infrastructure managed by Arcserve that protects customer environments, and serves as a recovery site in the event of a disaster or disruption to a customer’s primary site. With the UDP Cloud Direct Disaster Recovery solution, customers are provisioned resources such as a private virtual data center, random access memory (RAM), and external IP addresses.

How to Set up a UDP Cloud Direct Partner Account

In order to use UDP Cloud Direct, you need to have a UDP Cloud Direct Partner account. If you do not have an existing UDP Cloud Direct Partner account, your Arcserve Sales Representative will be able to assist you with this process.

Once the process of creating a new UDP Cloud Direct Partner account is initiated, you should receive an email at the email address provided in order to complete account setup. Click on the link provided in the email and you will be directed to the UDP Cloud Direct Portal where can specify your new UDP Cloud Direct Partner account credentials. When completed, you can navigate to the URL and log onto the UDP Cloud Direct Portal using your new credentials.

How to Protect Systems

Protecting systems requires deploying the UDP Cloud Direct Agent.

This section contains the following topics:

- Deploying Arcserve UDP Cloud Direct Agent
- Downloading Arcserve UDP Cloud Direct Agent
- Installing Arcserve UDP Cloud Direct Agent
- Registering Arcserve UDP Cloud Direct Agent

Deploying UDP Cloud Direct Agent

A key component of UDP Cloud Direct is the UDP Cloud Direct Agent. This backup agent must be installed on each system which contains data that you want to protect in the Arcserve Cloud.

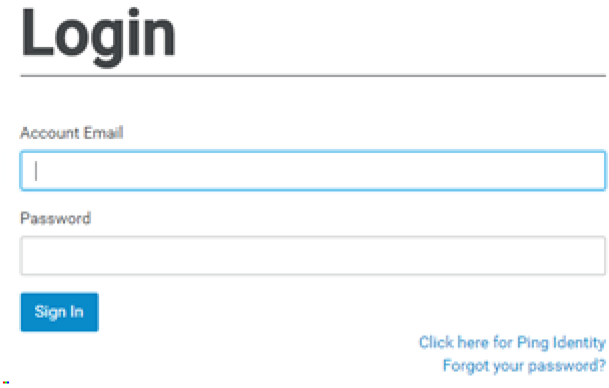
For VMware virtual environments, you can choose to deploy the UDP Cloud Direct Virtual Appliance. This virtual appliance enables agentless backup of VMware virtual machines. The UDP Cloud Direct Virtual Appliance eliminates the need to install the backup agent on each individual VMware virtual machine. Steps to deploy the UDP Cloud Direct Virtual Appliance for VMware are described here.

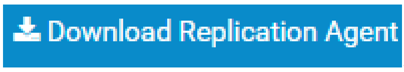
Downloading UDP Cloud Direct Agent

The UDP Cloud Direct backup agent is available from the UDP Cloud Direct Portal.

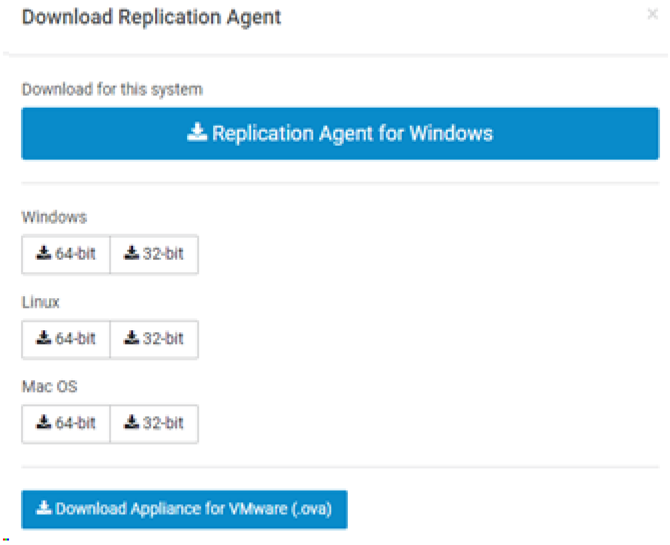
Follow these steps:

1. Log into the UDP Cloud Direct Portal using your account credentials.



2. On the *Systems* tab, click .

3. From the pop-up window, select download for the appropriate operating system.


Download Replication Agent
×
Download for this system
Replication Agent for Windows
Windows
64-bit
32-bit
Linux
64-bit
32-bit
Mac OS
64-bit
32-bit
Download Appliance for VMware (.ova)

4. Note the file name and location of the downloaded file.

You have downloaded the UDP Cloud Direct Agent successfully.

Installing UDP Cloud Direct Agent

For agent-based protection of system data, the UDP Cloud Direct Agent must be installed on each system that you want to protect.

Follow these steps:

1. Locate the downloaded file for the UDP Cloud Direct Agent. If necessary, copy the file to the system the you want to protect.
2. Launch the installer to begin installing the backup agent on the system to protect.

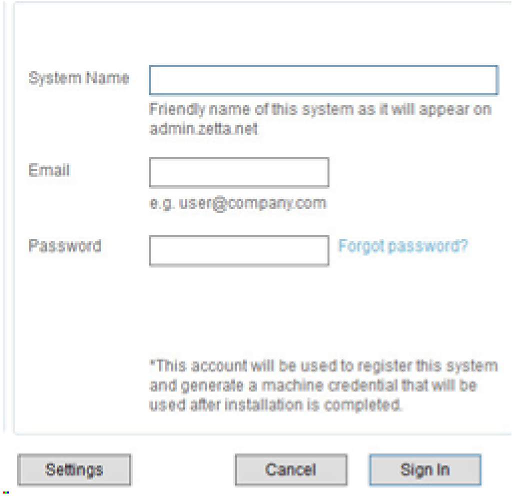
ArcserveUDPCloudDirectSetup_5.5.49873_x64 9/29/2016 5:15 PM Windows Installer Package

Registering UDP Cloud Direct Agent

After the backup agent is installed on the system, it must be registered with the Arcserve Cloud. Once the installation completes, you will be prompted to register the backup agent.

To register UDP Cloud Direct Agent, follow these steps:

1. Once the installation is complete, the registration window opens.



System Name

Friendly name of this system as it will appear on admin.zetta.net

Email

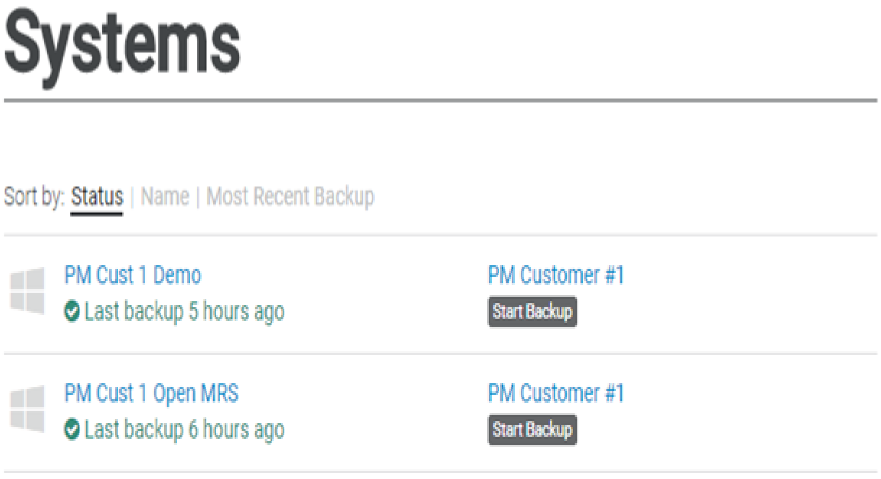
e.g. user@company.com

Password

*This account will be used to register this system and generate a machine credential that will be used after installation is completed.

2. At the prompt, enter a name for the system as you want it to appear in the UDP Cloud Direct Portal or keep the default name.
3. Enter the email address and password of your UDP Cloud Direct account credentials.
4. Click Sign In again to register the system.

   You will be presented with the UDP Cloud Direct Portal showing the system added to the Systems tab for the specified customer.



Systems

Sort by: Status | Name | Most Recent Backup

PM Cust 1 Demo ✓ Last backup 5 hours ago	PM Customer #1 Start Backup
PM Cust 1 Open MRS ✓ Last backup 6 hours ago	PM Customer #1 Start Backup

You have registered the UDP Cloud Direct Agent successfully.

How to Set up UDP Cloud Direct Virtual Appliance

For VMware virtual environments, the UDP Cloud Direct Virtual Appliance can be deployed to enable agentless protection of one or more VMware virtual machines. The virtual appliance eliminates the need to install the UDP Cloud Direct agent on each virtual machine.

This section contains the following topics:

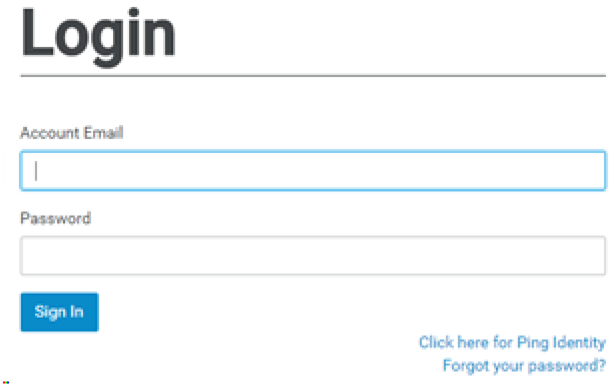
- Downloading UDP Cloud Direct Virtual Appliance
- Deploying UDP Cloud Direct Virtual Appliance
- Registering UDP Cloud Direct Virtual Appliance

Downloading UDP Cloud Direct Virtual Appliance

The UDP Cloud Direct Virtual Appliance is available as a *.ova* file from the UDP Cloud Direct Portal.

To download UDP Cloud Direct Virtual Appliance, follow these steps:

1. Log into the UDP Cloud Direct Portal using your account credentials.



2. On the *Systems* tab, click Download Replication Agent.
3. From the pop-up window, click Download Appliance for VMware (.ova).
4. Make a note of the file name and directory where you saved the download.

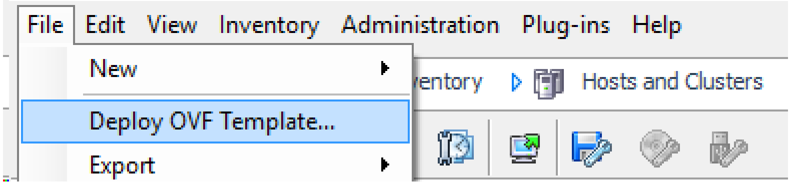
You have downloaded the UDP Cloud Direct Virtual Appliance successfully.

Deploying UDP Cloud Direct Virtual Appliance

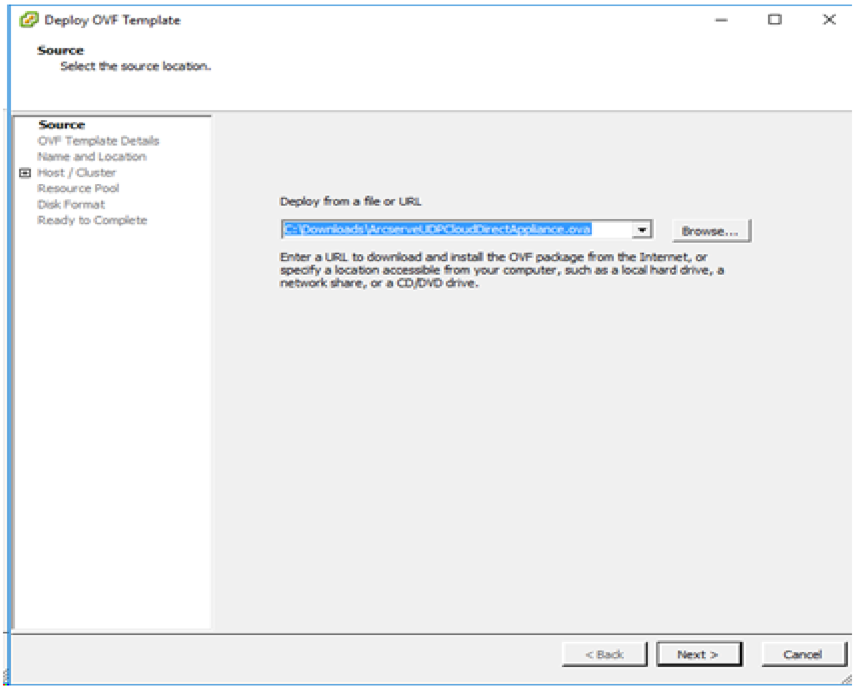
Use the VMware vSphere Web Client to deploy the UDP Cloud Direct Virtual Appliance into your VMware vSphere environment.

Follow these steps:

1. Launch the VMware vSphere Web Client and log in.
2. In the vSphere Web Client, click on File, and then select Deploy OVF Template.



3. Click *Browse* and navigate to the location where you downloaded the *.ova* file.



Deploy OVF Template

Source

Select the source location.

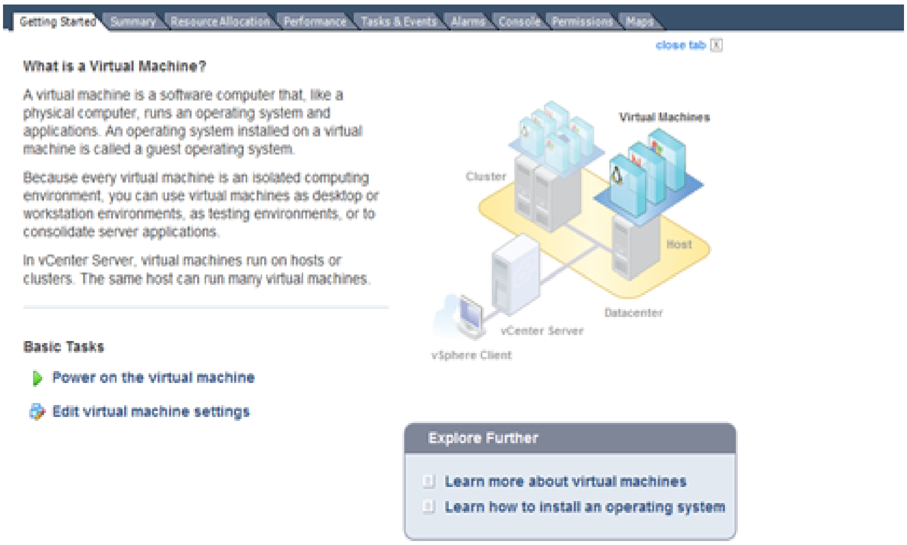
Deploy from a file or URL

C:\Downloads\ArcserveUDPCloudDirectAppliance.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

4. Select the file and click **Next**.
5. Proceed through the rest of the setup process until you get to *Ready to Complete*, and then click **Finish**. The UDP Cloud Direct Virtual Appliance is deployed. Once completed, click **Close**.

6. Navigate to *Getting Started* and select the UDP Cloud Direct Virtual Appliance, and then click *Power on the virtual machine*.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.

Basic Tasks

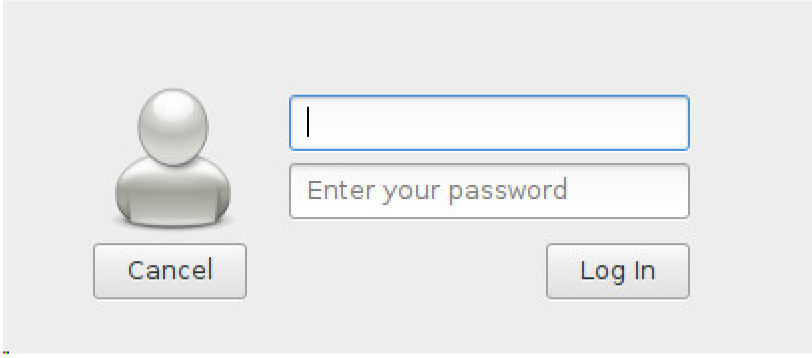
You have deployed the UDP Cloud Direct Virtual Appliance successfully.

Registering UDP Cloud Direct Virtual Appliance

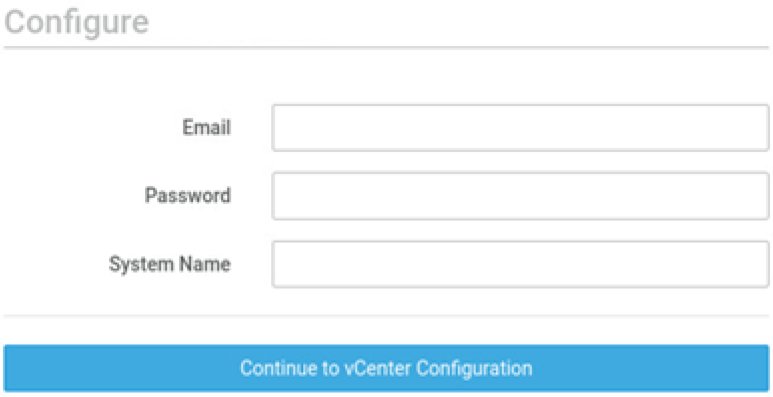
Once the Virtual Appliance is installed and powered on, you need to register the UDP Cloud Direct Virtual Appliance with the Arcserve Cloud.

Follow these steps:

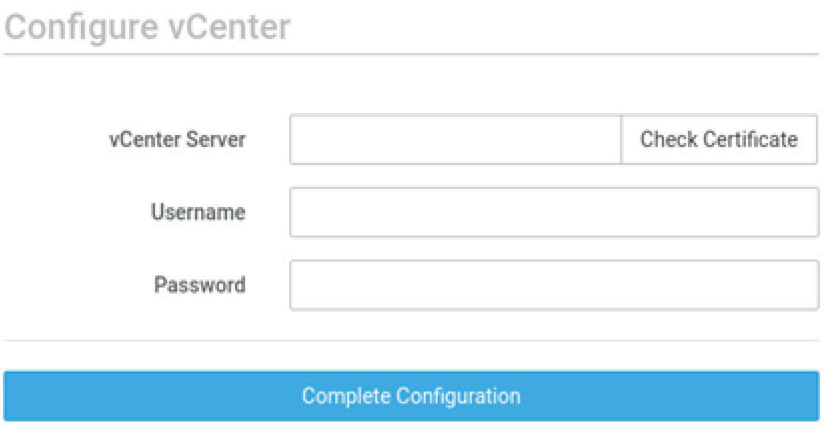
1. In the VMware vSphere Web Client, navigate to *Console* tab for the virtual appliance.



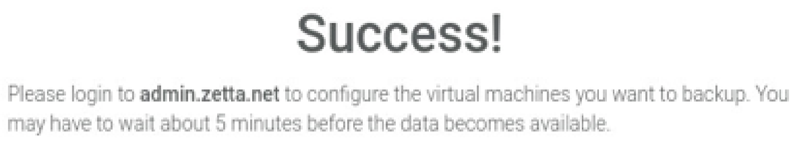
2. Enter the default user name *zetta*, the default password *zettazetta*, and click *Log In*.
3. Enter the user account credentials (email/password) of a user that was created under your account that leverages the virtual appliance, and then click *Continue to vCenter Configuration*.



4. Enter your vCenter Server address, vCenter Username, and vCenter Password, and then click *Complete Configuration*.



You should get confirmation that the registration was successfully completed. It could take up to 5 minutes for data to become available in the UDP Cloud Direct Portal.


Success!

Please login to **admin.zetta.net** to configure the virtual machines you want to backup. You may have to wait about 5 minutes before the data becomes available.

5. **Optional step:** You can click *Change Appliance Password* to change the password for your UDP Cloud Direct Virtual Appliance using your current default password.

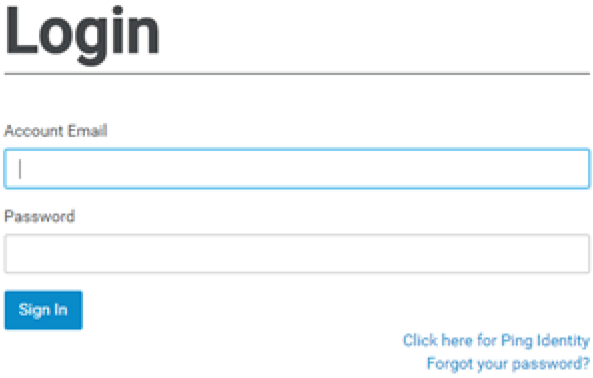
You have registered the UDP Cloud Direct Virtual Appliance successfully.

How to Configure the Backup Task

Protecting system data involves creating one or more backup tasks. You need to configure the backup tasks configured for systems where the UDP Cloud Direct Agent is installed. When using the Arcserve Cloud Virtual Appliance, a single backup tasks is used to backup up one or more virtual machines.

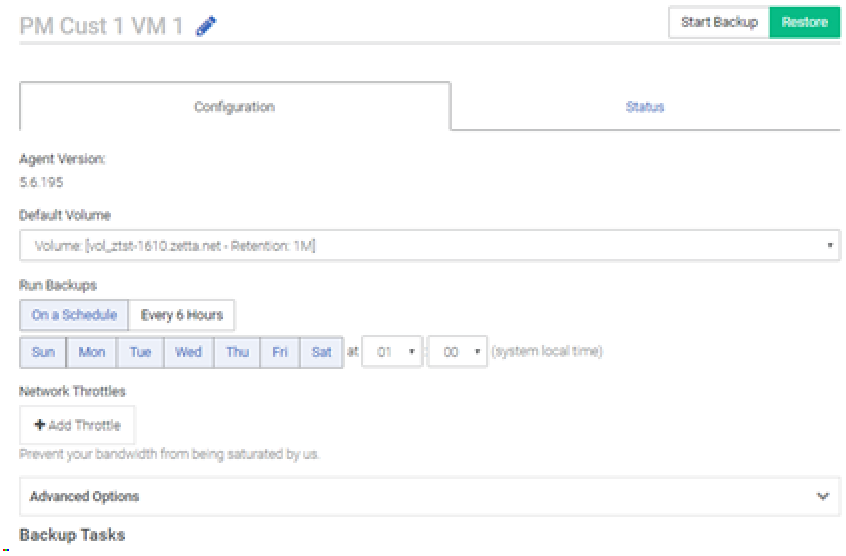
To create the backup task for a system, follow these steps:

1. Log into the UDP Cloud Direct Portal using your account credentials.



2. You are presented with the *System* tab. You should see the list of the registered systems. Click on the *Configuration* link to view the backup settings for the system.

Backup settings window opens.



Agent Version:
5.6.195

Default Volume
Volume: [vol_ztst-1610.zetta.net - Retention: 1M]

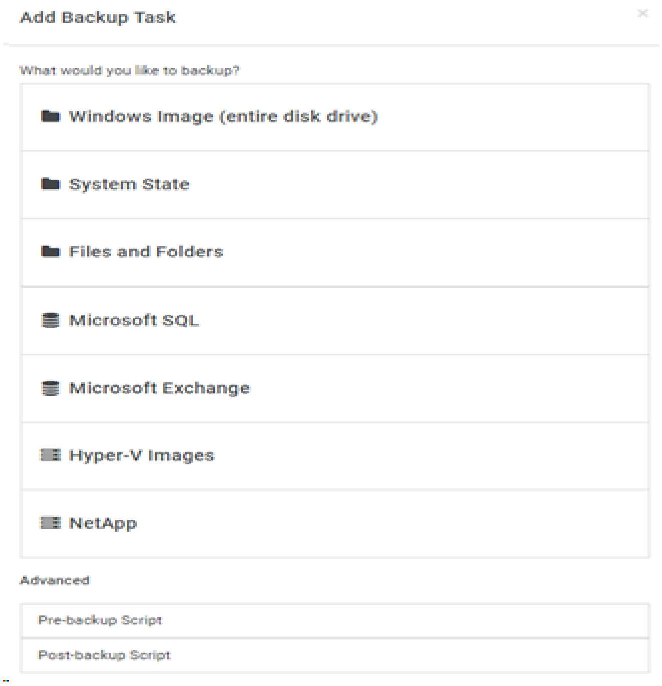
Run Backups
On a Schedule | Every 6 Hours
Sun | Mon | Tue | Wed | Thu | Fri | Sat at 01 : 00 (system local time)

Network Throttles
+ Add Throttle
Prevent your bandwidth from being saturated by us.

Advanced Options

Backup Tasks

3. Click ✚ Add Backup Task under the *Backup Tasks* section to create a new task. In order to leverage UDP Cloud Direct, you must create a *Windows Image Backup* backup task.



Add Backup Task ×

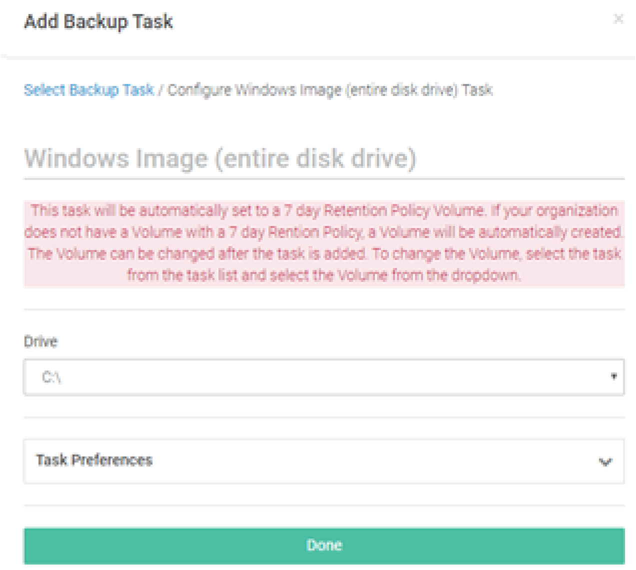
What would you like to backup?

- Windows Image (entire disk drive)
- System State
- Files and Folders
- Microsoft SQL
- Microsoft Exchange
- Hyper-V Images
- NetApp

Advanced

- Pre-backup Script
- Post-backup Script

4. From the pop-up window, click PM Customer #1 Start Backup Enable Disaster Recovery to create the backup task.



Add Backup Task

Select Backup Task / Configure Windows Image (entire disk drive) Task

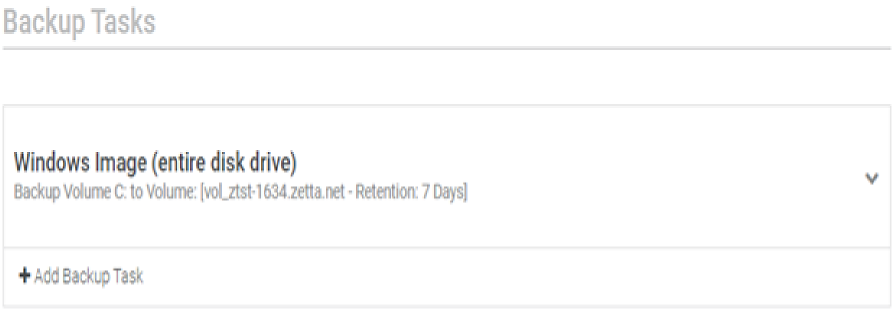
Windows Image (entire disk drive)

This task will be automatically set to a 7 day Retention Policy Volume. If your organization does not have a Volume with a 7 day Rention Policy, a Volume will be automatically created. The Volume can be changed after the task is added. To change the Volume, select the task from the task list and select the Volume from the dropdown.

Drive: C:\

5. Select the disk letter from the drop-down list.
6. Click Done on the task pop-up screen.

   The newly added task appears under the Backup Tasks section.



Backup Tasks

Windows Image (entire disk drive)
Backup Volume C: to Volume: [vol_ztst-1634.zetta.net - Retention: 7 Days]

Note: It is possible to create multiple tasks for each system. It is important to note that a single schedule applies to all of the tasks created for the system.

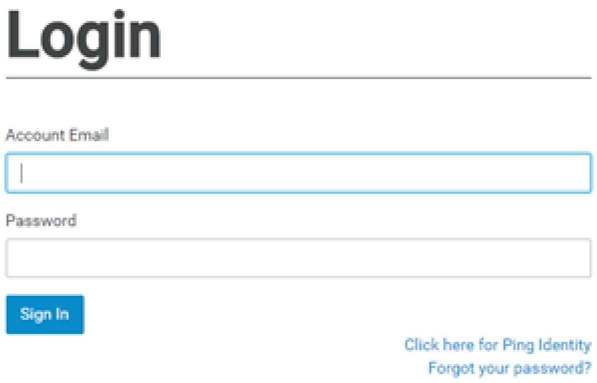
You have created and configured the backup task successfully.

How to Configure the Backup Using UDP Cloud Direct Virtual Appliance

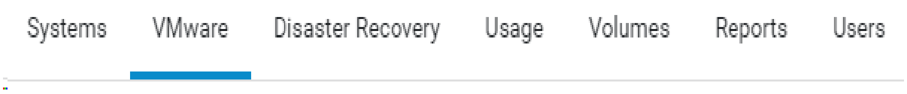
The UDP Cloud Direct Virtual Appliance allows for the protection of VMware virtual machines. Once deployed, the virtual appliance will discover all the virtual machines associated with the specified VMware vCenter server. The deployed virtual appliances and the discovered virtual machines will be listed on the *VMware* tab.

To configure the UDP Cloud Direct Virtual Appliance to backup VMware virtual machines, follow these steps:

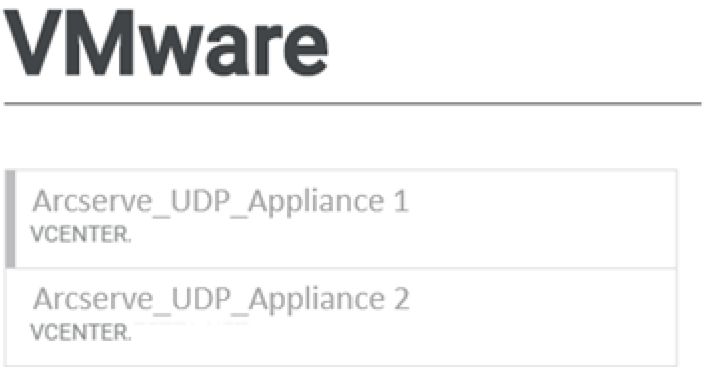
1. Log into the UDP Cloud Direct Portal using your account credentials.



2. Click the *VMware* link.



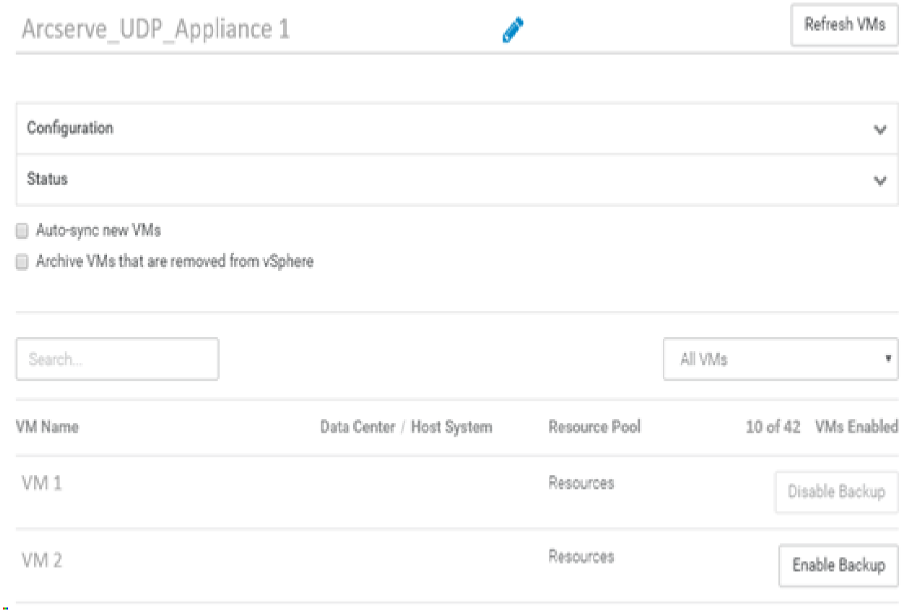
On the *VMware* tab, you will see a list of the registered UDP Cloud Direct Virtual Appliances.



Arcserve_UDP_Appliance 1
VCENTER

Arcserve_UDP_Appliance 2
VCENTER

3. Click the desired UDP Cloud Direct Virtual Appliance from the list. The virtual machines visible to the Virtual Appliance is listed.



- □ Auto-sync new VMs
- □ Archive VMs that are removed from vSphere

VM Name	Data Center / Host System	Resource Pool	10 of 42 VMs Enabled
VM 1		Resources	Disable Backup
VM 2		Resources	Enable Backup

4. Click Enable Backup for each virtual machine that you want the UDP Cloud Direct Virtual Appliance to backup. Once enabled for backups, the virtual machine will appear listed on the *Systems* tab.

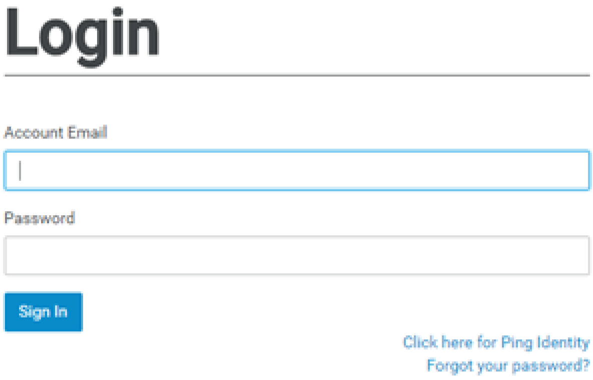
You have configured the backup using UDP Cloud Direct Virtual Appliance successfully.

How to Enable Disaster Recovery

Once the *Windows Image Backup* task is properly configured, then you can enable UDP Cloud Direct Disaster Recovery for the system. This will protect the system so that a virtual instance can be powered on in the Arcserve Cloud.

To enable disaster recovery, follow these steps:

1. Log into the UDP Cloud Direct Portal using your account credentials.

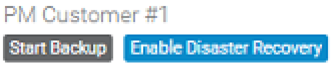


Login

Account Email

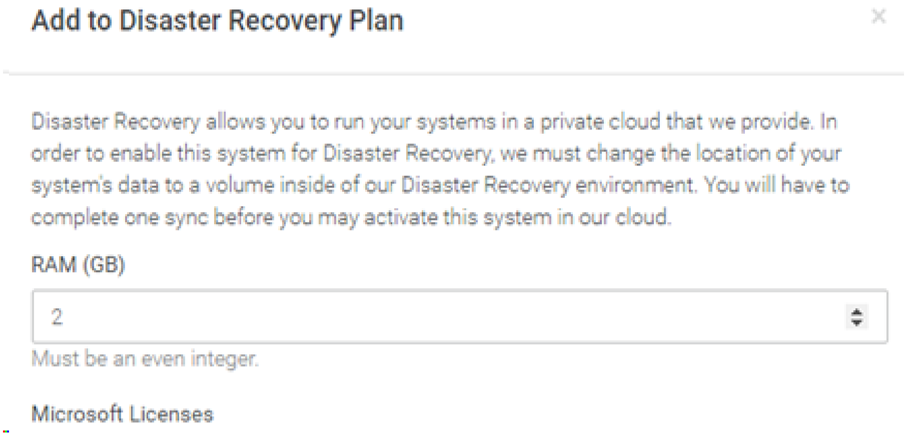
Password

On the *Systems* tab, you should see a list of the registered systems.



PM Customer #1

2. Click Enable Disaster Recovery for the desired system.
3. Specify the amount of Random Access Memory (RAM) that you would like the virtual instance of the system to have when it is run in the Arcserve Cloud.
4. Specify the appropriate Microsoft licenses if known.



Add to Disaster Recovery Plan

Disaster Recovery allows you to run your systems in a private cloud that we provide. In order to enable this system for Disaster Recovery, we must change the location of your system's data to a volume inside of our Disaster Recovery environment. You will have to complete one sync before you may activate this system in our cloud.

RAM (GB)

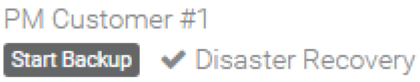
2

Must be an even integer.

Microsoft Licenses

5. Click Save.
6. Click Close on the acknowledgment pop-up screen.

Note: After disaster recovery is enabled for the system, you should notice that the indicator showing that Disaster Recovery is enabled for the system.



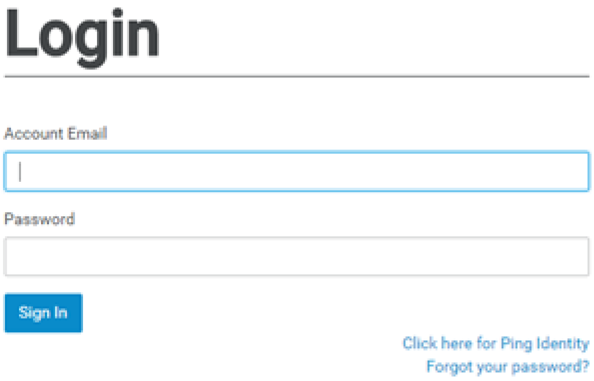
You have enabled the Disaster Recovery successfully.

How to Enable Disaster Recovery for Virtual Machine

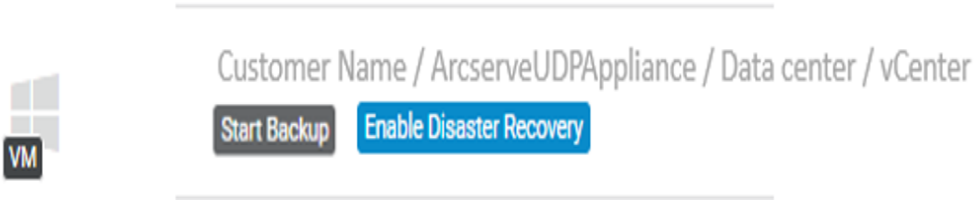
The UDP Cloud Direct Virtual Appliance enables agentless protection for VMware virtual machines. Once deployed, the virtual appliance will discover all the virtual machines associated wth a specified VMware vCenter server. In Virtual machines that have backups enabled, you can enable the disaster recovery protection.

To enable disaster recovery for protected VMware virtual machines, follow these steps:

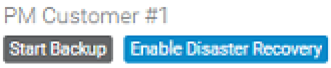
1. Log into the UDP Cloud Direct Portal using your account credentials.



On the *Systems* tab, you should see a list of the registered systems and protected virtual machines.


VM
Customer Name / ArcserveUDPAppliance / Data center / vCenter
Start Backup
Enable Disaster Recovery

2. Click Enable Disaster Recovery for the desired virtual machine.
3. Specify the amount of Random Access Memory (RAM) that you would like the virtual instance of the system to have when it is run in the Arcserve Cloud.
4. Specify the appropriate Microsoft licenses if known.

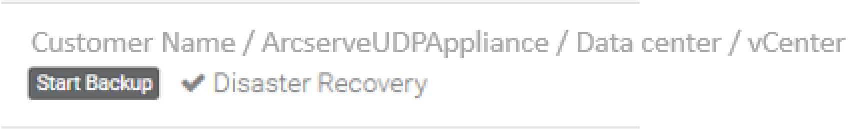


PM Customer #1

5. Click Save.

6. Click Close on the acknowledgment pop-up screen.

   Note: After disaster recovery is enabled for the virtual machine, you should notice that the indicator showing that Disaster Recovery is enabled for the virtual machine.



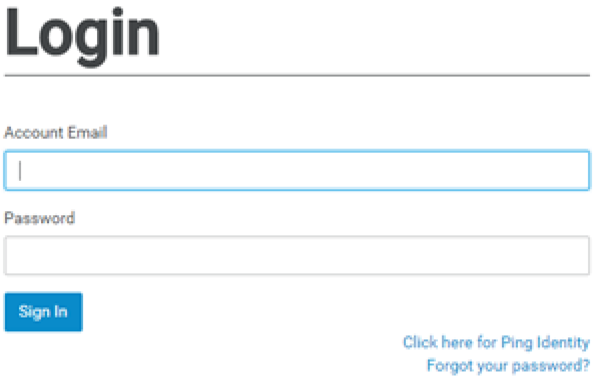
Customer Name / ArcserveUDPAppliance / Data center / vCenter

How to Run the Backup Task

The data of a system is not protected until the backup tasks have run at least once. The backup tasks configured for a system will run according to the configured schedule. It is also possible to initiate the backup tasks to run manually.

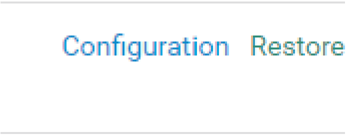
To manually initiate the backup tasks of a system to run, follow these steps:

1. Log into the UDP Cloud Direct Portal using your account credentials.

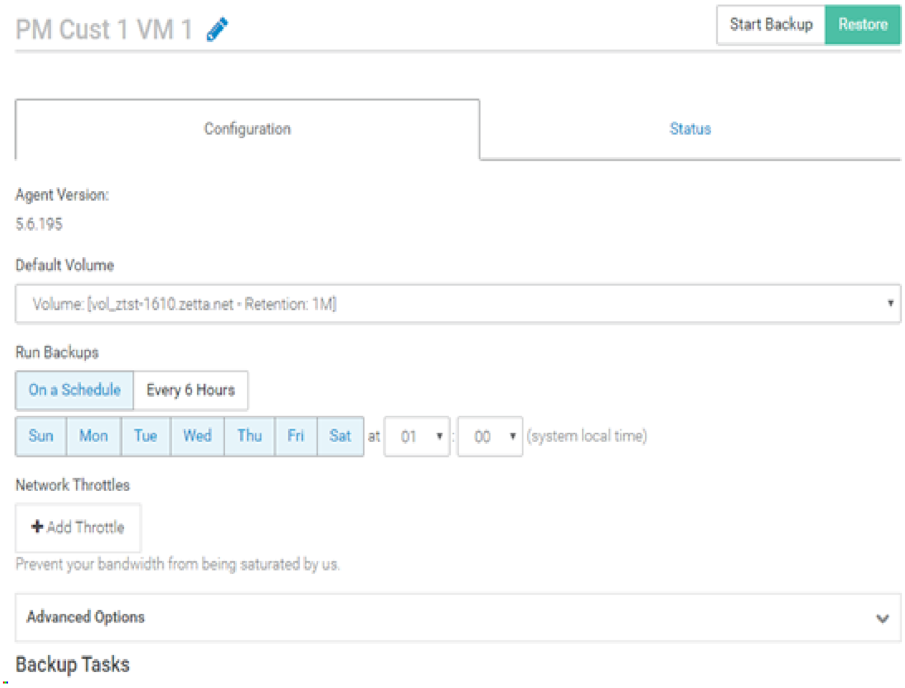


On the *Systems* tab, you will see a list of the registered systems.

2. Click on the *Configuration* link to view the backup settings for the system.



Backup Settings window opens.



PM Cust 1 VM 1

Agent Version:
5.6.195

Default Volume
Volume: [vol_ztst-1610.zetta.net - Retention: 1M]

Run Backups
On a Schedule | Every 6 Hours
Sun Mon Tue Wed Thu Fri Sat at 01 : 00 (system local time)

Network Throttles
Prevent your bandwidth from being saturated by us.

Backup Tasks

3. Click Start Backup to manually start the all of the backup tasks configured for the system. The tasks will also run according to the configured schedule. The configured schedule applies to all tasks configured for the system.

   Note: To manually start a backup, you can click Start Backup for the system on the *Systems* tab.

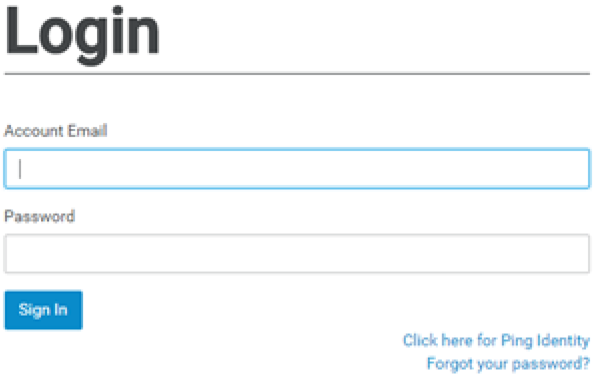
You have started the backup task successfully.

How to Run the Backup Using UDP Cloud Direct Virtual Appliance

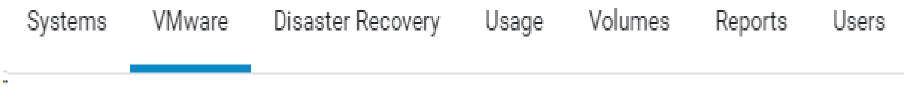
The UDP Cloud Direct Virtual Appliance will perform a backup of all its associated virtual machines where backup has been enabled. The virtual appliance will perform that backups according to the configured scheduled or backups can be manually initiated.

To initiate the virtual appliance to backup all enabled virtual machines manually, follow these steps:

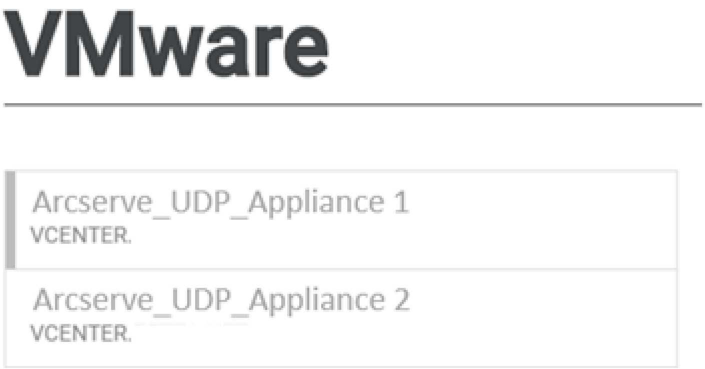
1. Log into the UDP Cloud Direct Portal using your account credentials.



2. Click the *VMware* tab.

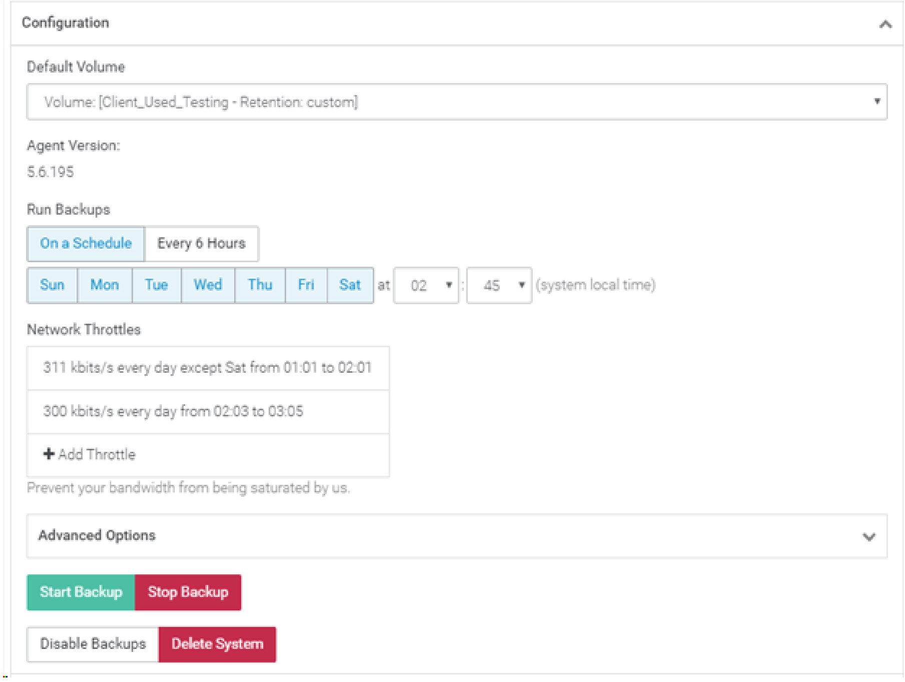


On the *VMware* tab, you will see a list of the registered UDP Cloud Direct Virtual Appliances.



3. Click the desired UDP Cloud Direct Virtual Appliance from the list. The virtual machines visible to the Virtual Appliance is listed.

4. Expand the *Configuration* section for the selected Virtual Appliance.



Configuration

Default Volume

Volume: [Client_Used_Testing - Retention: custom]

Agent Version:
5.6.195

Run Backups

On a Schedule | Every 6 Hours

Sun | Mon | Tue | Wed | Thu | Fri | Sat at 02 : 45 (system local time)

Network Throttles

311 kbits/s every day except Sat from 01:01 to 02:01

300 kbits/s every day from 02:03 to 03:05

+ Add Throttle

Prevent your bandwidth from being saturated by us.

Advanced Options

Start Backup | Stop Backup

Disable Backups | Delete System

5. Ensure that the virtual appliance is backing up the virtual machines to the desired volume.

6. Click Start Backup to initiate the UDP Cloud Direct Virtual Appliance to backup all of its associated virtual machines for which backups have been enabled.

You have started the backup using UDP Cloud Direct Virtual Appliance successfully.

How to Use Cloud Recovery

A key benefit of UDP Cloud Direct Disaster Recovery is providing customers the ability to run virtual instances of protected systems in the cloud in the event that a disaster impacts their on-premises environment. The process of powering on virtual instances of servers in the cloud and leveraging the cloud as a recovery site is often referred to a Failover.

About Failover

The Failover process involves all steps necessary to ensure that a customer can leverage the cloud as they would their on-premises environment to continue running their critical business operations. Important aspects of the Failover process include powering on virtual instances of protected systems in the cloud and enabling secure connectivity to the recovered environment.

The UDP Cloud Direct Disaster Recovery solution enables the administration of the failover process through the *Disaster Recovery* tab of the UDP Cloud Direct Portal.

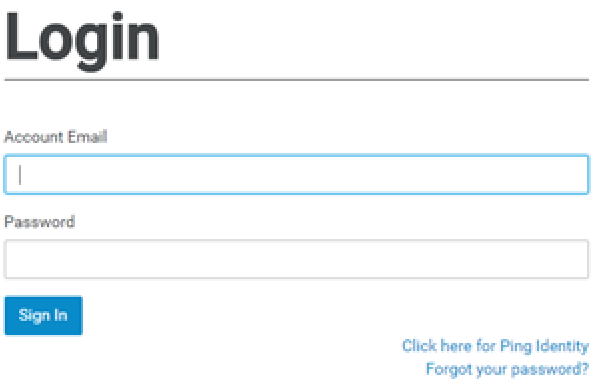
This section contains the following topics:

- Activating systems in the Cloud
- Connecting to the Cloud

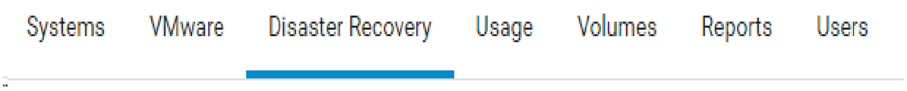
Activating Systems in the Cloud

To access the Disaster Recovery tab, follow these steps:

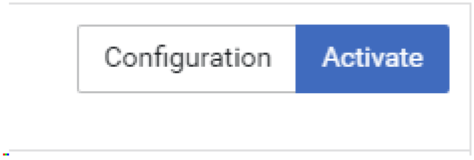
1. Log into the UDP Cloud Direct Portal using your account credentials.



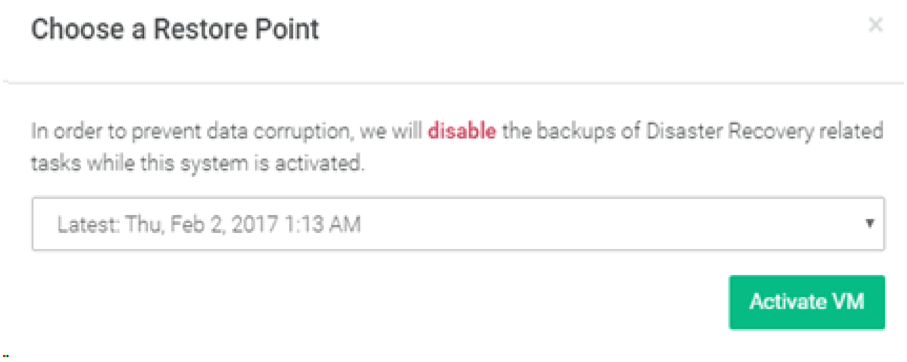
2. Click the *Disaster Recovery* link.



3. Under the *Idle VMs* section, click the *Activate* button to initiate the activation of a virtual instance of a protected system in the cloud.



4. Select the desired restore point from the drop-down list.

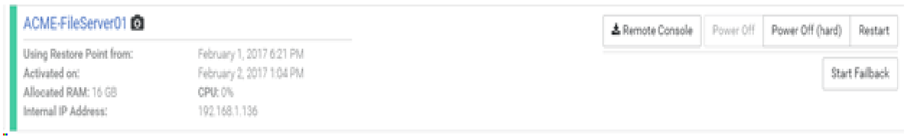


In order to prevent data corruption, we will **disable** the backups of Disaster Recovery related tasks while this system is activated.

Latest: Thu, Feb 2, 2017 1:13 AM ▾

5. Click Activate VM to power on the virtual instance in the cloud.

Note: Once activated, the virtual instance will appear in the listed *Active VMs* section, along with information about the virtual instance and administrative buttons.



ACME-FileServer01

Using Restore Point from:	February 1, 2017 6:21 PM
Activated on:	February 2, 2017 1:04 PM
Allocated RAM: 16 GB	CPU: 0%
Internal IP Address:	192.168.1.136

You have activated the system in Cloud successfully.

Connecting to the Cloud

There are multiple options for securely connecting to the Arcserve Cloud in order to leverage the virtual instances of recovered servers.

This section contains the following topics:

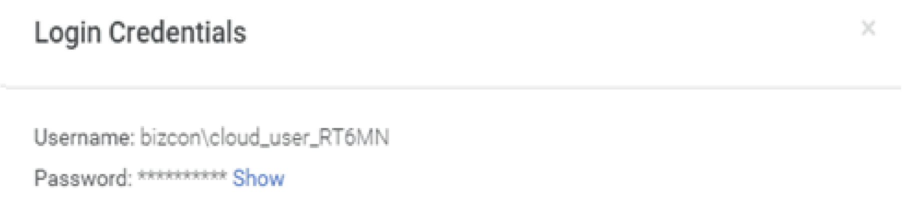
- How to Connect to Remote Console
- How to Connect to Point to Site VPN
- How to Connect to Site to Site VPN
- How to Failback an Activated Virtual License

How to Connect to Remote Console

A remote console can be established with a single virtual instance running in the Arcserve Cloud. A remote console connection enables a user to access a virtual instance running in the cloud using the remote desktop protocol.

To establish a remote console connection with an activated virtual instance from the *Disaster Recovery* tab, follow these steps:

1. Click Remote Console for the activated system to download the remote desktop protocol (.rdp) file.
2. From the Login Credentials pop-up window, click the *Show* link to reveal the password required for the connection.

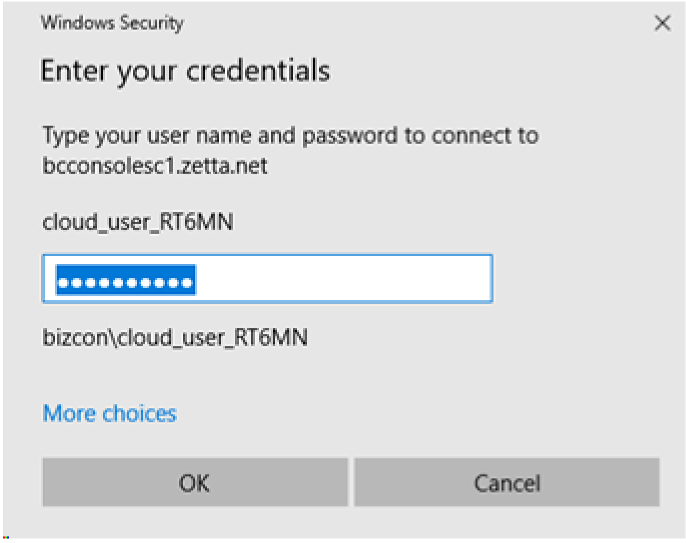


Login Credentials

Username: bizcon\cloud_user_RT6MN

Password: ********** Show

3. Launch the downloaded remote desktop protocol (.rdp) file.
4. Click *Connect* in the RemoteApp program dialog box.
5. Enter the password from the Login Credentials pop-up window into the Windows security dialog box.



Windows Security

Enter your credentials

Type your user name and password to connect to bcconsolesc1.zetta.net

cloud_user_RT6MN

•••••••••••

bizcon\cloud_user_RT6MN

6. Click *OK* to initiate the remote console connection. A web browser window should appear with the login screen of the virtual instance.

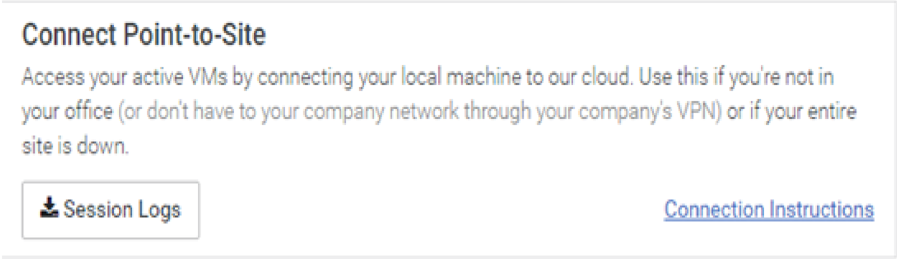
7. Click *Yes* when asked do you want to connect despite certificate errors.
8. Click Send Ctrl+Alt+Del at the top of the browser window.
9. Enter the Windows credentials for the virtual instance which are the same Windows credentials for the on-premises system at the time of the restore point.

You have connected to the remote Console successfully.

How to Connect to Point to Site VPN

A *Point to Site* connection enables a secure virtual private network (VPN) connection between a single client machine and the virtual private data center in the Arcserve Cloud. Such a connection would enable an end user at a coffee shop to establish a secure private connection to the recovered environment in the cloud. It is important to note that a separate connection would be needed if the end user also required access to systems that were still available in the on-premises environment. The on-premises systems would not be able to communicate with the recovered systems in the cloud via the “Point to Site” connection.

The instructions to establish a *Point to Site* connection is available on the *Disaster Recovery* tab in the *Connect Point-to-Site* dialog box.



Connect Point-to-Site

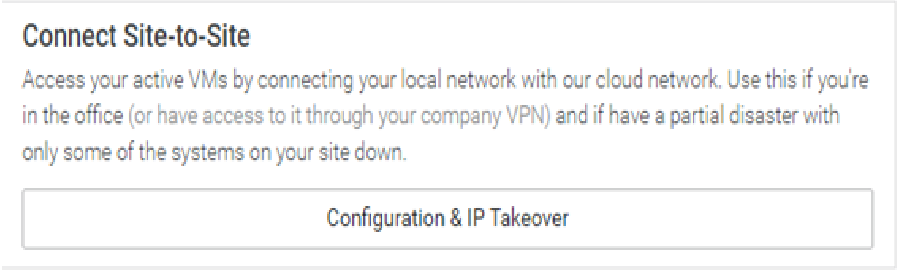
Access your active VMs by connecting your local machine to our cloud. Use this if you're not in your office (or don't have to your company network through your company's VPN) or if your entire site is down.

How to Connect to Site to Site VPN

A *Site to Site* connection enables a secure virtual private network (VPN) connection between an externally accessible IP address of an on-premises environment and the virtual data center in the Arcserve Cloud. This type of connection would eliminate the need for end user to each establish a *Point to Site* VPN connection. With a *Site to Site* connection, systems in the on-premises environment would be able to communicate with recovered systems in the cloud.

A *Site to Site* connection enables the ability to offer IP Takeover functionality. IP Takeover makes it possible for a virtual instance running in the cloud to assume the IP address of a failed on-premises system. When other on-premises systems or applications need to communicate with the failed on-premises system, the request will be forwarded to the virtual instance running in the cloud.

Arcserve offers the UDP Cloud Direct Virtual Network Appliance to assist with establishing a *Site to Site* connection. This virtual network appliance runs as a virtual machine in VMware vSphere, Microsoft Hyper-V, and Oracle VirtualBox environments. Once the virtual network appliance is deployed, the process of establishing a *Site to Site* connection can be completed on the *Disaster Recovery* tab of the UDP Cloud Direct Portal.



Connect Site-to-Site

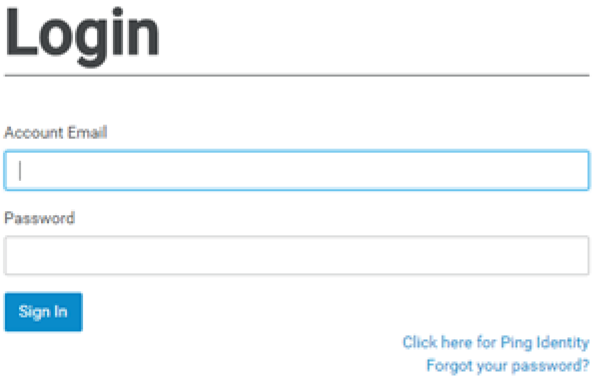
Access your active VMs by connecting your local network with our cloud network. Use this if you're in the office (or have access to it through your company VPN) and if have a partial disaster with only some of the systems on your site down.

How to Failback an Activated Virtual License

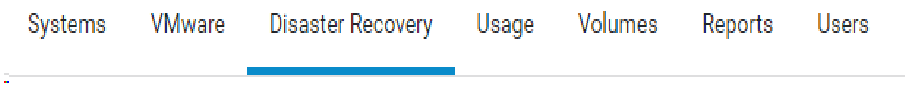
The Failback process involves all steps necessary to recover an on-premises environment following a disaster by leveraging virtual instances of systems running in the cloud. UDP Cloud Direct Disaster Recovery enables failback virtual instances from the Arcserve Cloud through the UDP Cloud Direct Portal. The failback process occurs over three iterations. First, a snapshot of the activated virtual instance taken and is then downloaded. Second, another snapshot of the activated virtual instance is taken, and only the differences between the two snapshots are downloaded. Finally, the activated virtual instance will be shut down so that a final snapshot can be taken and the remaining differences can be download. Once the download is complete, the resulting disk image can be used to create a virtual machine in the on-premises environment.

To failback an activated virtual instance, follow these steps:

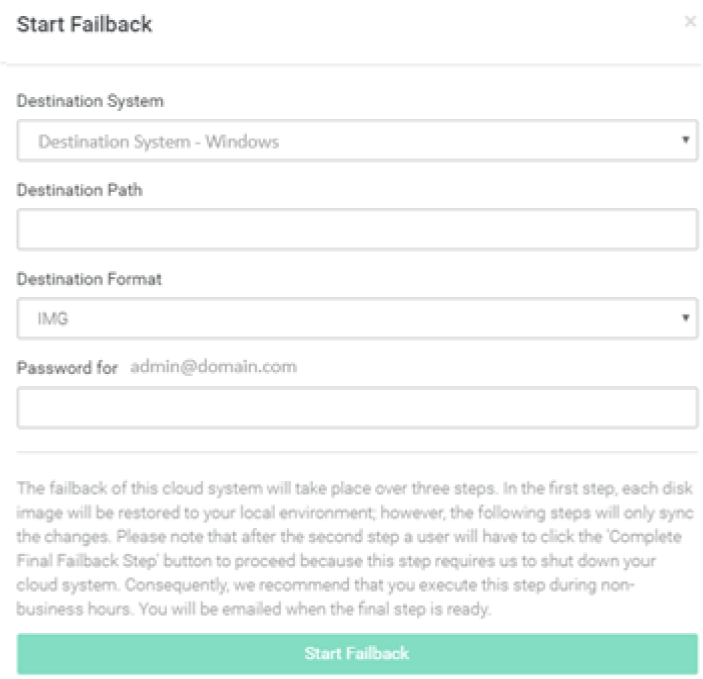
1. Log into the UDP Cloud Direct Portal using your account credentials.



2. Click the *Disastery Recovery* link.



3. Click Start Failback for an activated virtual instance.
4. Select a destination system from the drop-down list to which to download iterative snapshots of the disk image of the activated virtual instance.
5. Specify a path on the destination system.
6. Specify the desired format for the disk image file that will be downloaded.
7. Enter the password of your account credentials.



Start Failback ×

Destination System

Destination System - Windows ▾

Destination Path

Destination Format

IMG ▾

Password for admin@domain.com

The failback of this cloud system will take place over three steps. In the first step, each disk image will be restored to your local environment; however, the following steps will only sync the changes. Please note that after the second step a user will have to click the 'Complete Final Failback Step' button to proceed because this step requires us to shut down your cloud system. Consequently, we recommend that you execute this step during non-business hours. You will be emailed when the final step is ready.

Start Failback

8. Click Start Failback to begin the failback process. An email notification is sent when it is time for the final step of the process. The progress of the failback process will be displayed on the *Disaster Recovery* tab.
9. To initiate the final step of the download process, click Complete Final Failback Step › for the activated virtual instance.

   Note: Upon completion, a disk image file is available in the specified format, in the specified location, on the specified destination system. The disk image file is used to create a virtual machine in the On-premises environment as part of the process of recovering the on-premises environment.

Chapter 2: Exploring Tabs

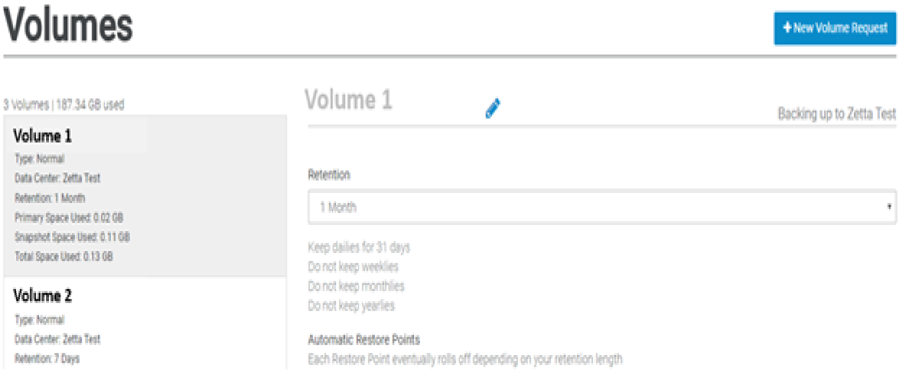
The UDP Cloud Direct solution protects the data of on-premises systems in the Arcserve Cloud. Within the Arcserve Cloud, the system data is stored in volumes. There are a few different types of volumes including Normal and ZeroCopy (for Disaster Recovery), and each volume is identified by its name, retention policy, and Arcserve data center location.

This section contains the following topics:

How to Use Volume Tab

The UDP Cloud Direct solution protects the data of on-premises systems in the Arcserve Cloud. Within the Arcserve Cloud, the system data is stored in volumes. There are a few different types of volumes including Normal and ZeroCopy (for Disaster Recovery), and each volume is identified by its name, retention policy, and Arcserve data center location.

The *Volumes* tab lists details of the volumes. On this tab, it is possible to rename the volume, as well as change its retention policy. It is also possible to request that a new volume be created.



Volumes

3 Volumes | 187.34 GB used

Volume 1
Type: Normal
Data Center: Zetta Test
Retention: 1 Month
Primary Space Used: 0.02 GB
Snapshot Space Used: 0.11 GB
Total Space Used: 0.13 GB

Volume 2
Type: Normal
Data Center: Zetta Test
Retention: 7 Days

Volume 1

Backing up to Zetta Test

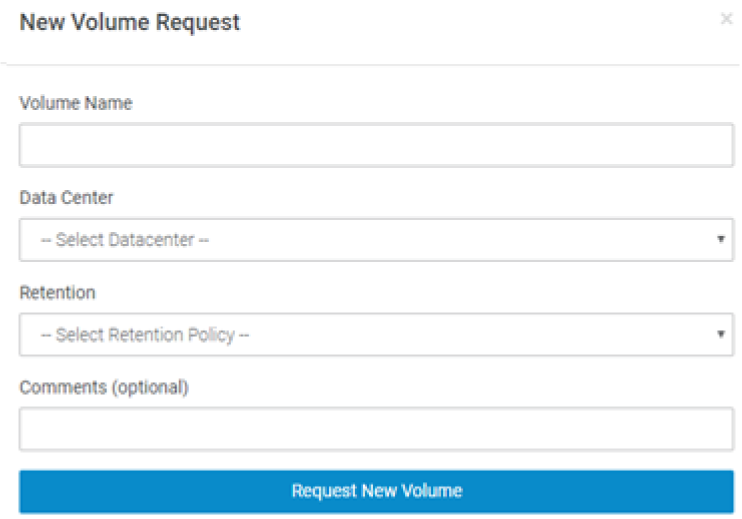
Retention: 1 Month

Keep dailies for 31 days
Do not keep weeklies
Do not keep monthlies
Do not keep yearlies

Automatic Restore Points
Each Restore Point eventually rolls off depending on your retention length

To create a new volume, follow these steps:

1. Click **+ New Volume Request**.
2. Specify a name for the new volume.
3. Specify a data center location.
4. Specify the retention policy for the volume.



New Volume Request

Volume Name:

Data Center: -- Select Datacenter --

Retention: -- Select Retention Policy --

Comments (optional):

5. Click Request New Volume.

   Note: The new volume request is received and processed by the Arcserve Team. After the request is successfully processed, the new volume will appear among the list on the *Volumes* tab. The new volume is available as a destination for configured backup tasks.

You have created the new volume successfully.

How to Use the Users Tab

The *Users* tab allows you manage the users who can access the UDP Cloud Direct Portal.

User Role Types

A user may be added to the account and given a particular role. Each role provides different access rights and administrative capabilities. The user role types are as follows:

- **Admin** – users have all privileges including system, volume, user, and support ticket management. They may also access and recover the data stored by every system in their organization
- **Billing** – users may view invoices and manage an organization’s payment information. They may also create and edit support tickets and view an organization’s retention information (For example, usage, volume retention).
- **Storage** – users are allowed to manage storage details (For example, volume retention, manual restore points) and create and edit support tickets.
- **Restore** – users may access and recover the data stored by systems that they have been granted access and the ability to manage support tickets.

Topic:

Adding a User from the Users Tab

How to Use the Reports Tab

The Reports tab lists the available types of reports and alerts. Each report type can be configured for scheduled delivery, or can be generated On Demand. Each alert type will send an email notification when the specified event occurs. Multiple instances of each report and alert can be created. The number of each report and alert type that is configured is displayed.

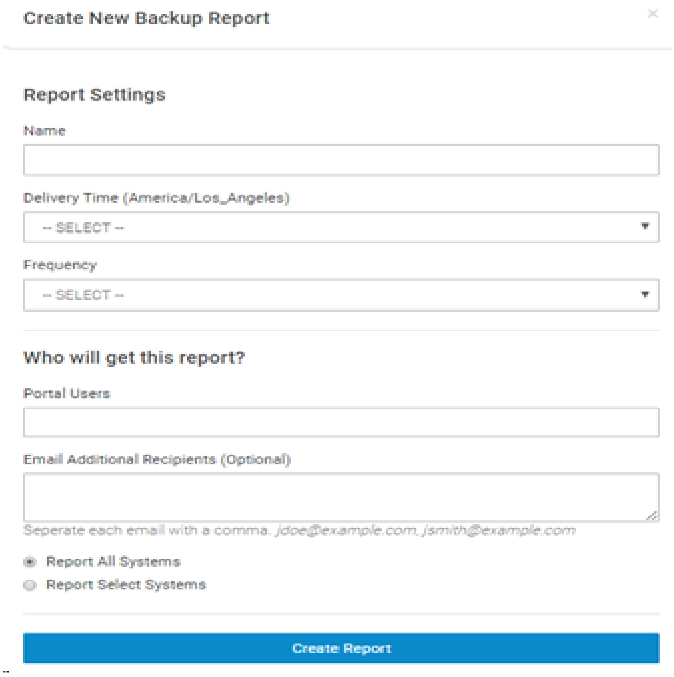
All reports are delivered through email, and all except the Daily Digest report are delivered with a Comma Separated Value (CSV) file attached that contains job details.

Reports and alerts can be generated to include all systems, or only selected systems.

To create a report, follow these steps:

1. Click on the desired report type.
2. Click on **+ Add Report** to create a new instance of the report.

   Note: Clicking ⭳ On Demand generates a report that is delivered as soon as possible to the email address of the current user.
3. Configure the report by providing a report name, the delivery time, the delivery frequency, report recipients, and the protected systems to include in the report.



Create New Backup Report

Report Settings

Name

Delivery Time (America/Los_Angeles)

-- SELECT --

Frequency

-- SELECT --

Who will get this report?

Portal Users

Email Additional Recipients (Optional)

Seperate each email with a comma. *jdoe@example.com, jsmith@example.com*

● Report All Systems

○ Report Select Systems

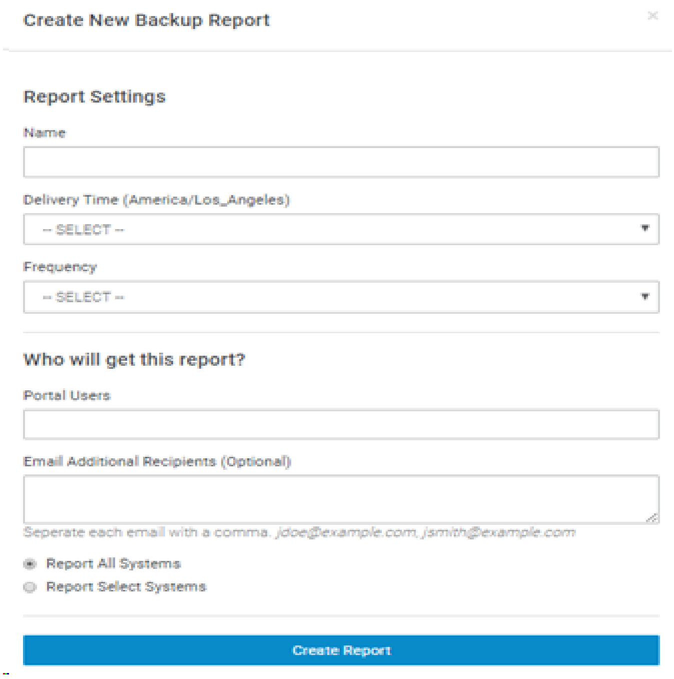
4. Click **Create Report** to create an instance of the report.

You have created the report successfully

How to Use the Alerts Tab

To create an alert, follow these steps:

1. Click on the desired alert type.
2. Click + Add Alert to create a new instance of the alert.
3. Configure the alert by providing a name, specifying the criteria, specifying the recipients, and specifying the protected systems for which to generate the alert.



Create New Backup Report ×

Report Settings

Name

Delivery Time (America/Los_Angeles)

-- SELECT --

Frequency

-- SELECT --

Who will get this report?

Portal Users

Email Additional Recipients (Optional)

Seperate each email with a comma. *jdoe@example.com, jsmith@example.com*

● Report All Systems

○ Report Select Systems

Create Report

4. Click Create Alert to create an instance of the alert.

You have created the alert successfully.

How to Use the Users Tab

The *Users* tab allows you manage the users who can access the UDP Cloud Direct Portal.

User Role Types

A user may be added to the account and given a particular role. Each role provides different access rights and administrative capabilities. The user role types are as follows:

- **Admin** – users have all privileges including system, volume, user, and support ticket management. They may also access and recover the data stored by every system in their organization
- **Billing** – users may view invoices and manage an organization’s payment information. They may also create and edit support tickets and view an organization’s retention information (For example, usage, volume retention).
- **Storage** – users are allowed to manage storage details (For example, volume retention, manual restore points) and create and edit support tickets.
- **Restore** – users may access and recover the data stored by systems that they have been granted access and the ability to manage support tickets.

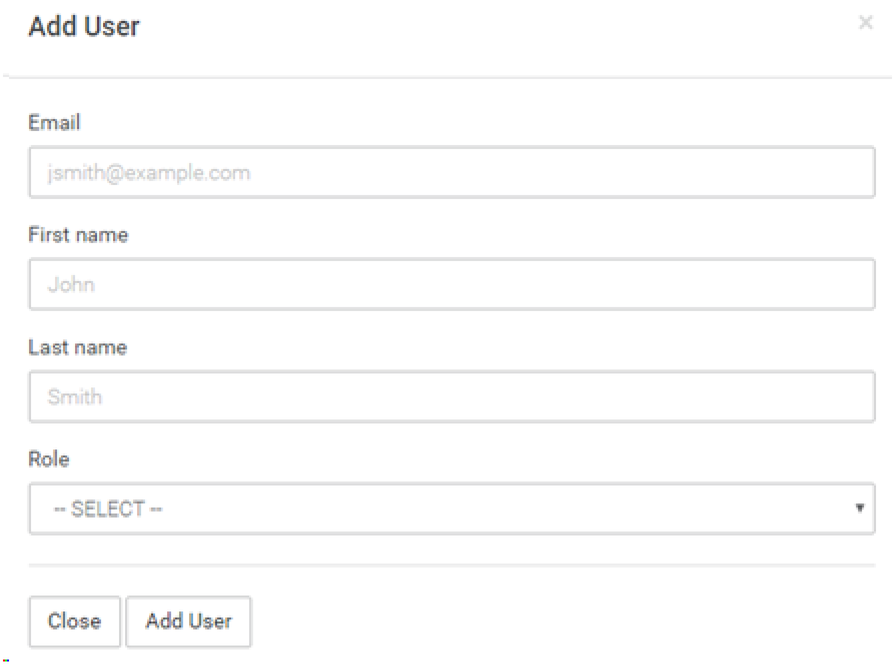
Topic:

Adding a User from the Users Tab

Adding a User from the Users Tab

To add a user from the Users tab, follow these steps:

1. Click + Add User.



2. Enter email address for the new user.
3. Enter user's First name.
4. Enter user's Last name.
5. Select the desired role for the user.
6. Click Add User to save the new user.

Note: An email is sent to the new user to verify the email address and complete the process. Upon receiving the email, the user will create their account credentials.

You have added the user from the *Users* tab successfully.

Chapter 3: Using Arcserve Knowledge Base

Arcserve Knowledge Base provides a repository of product documentation and helpful articles. You can search on key terms, and will be presented with related information to provide help and guidance.

Chapter 4: Accessing Release Notes

The release notes provide information on new features and functionality added to the product. The release notes may be found by clicking on the icon.