eFolder BDR for Replibit

Addendum to Replibit Administration Guide

for Replibit

Addendum to Replibit Administration Guide
Version 1.0

eFolder Addendum

This document is an **eFolder-specific Addendum** to the, *"Replibit Administration Guide."*
It should be used in conjunction with this guide which can be accessed from the following link:
https://backup.securewebportal.net/efolder/files/Replibit/Replibit_Administrators_Guide.pdf

This Addendum contains the following five sections specific to eFolder's backup process:

eFolder Customer Support

At eFolder, we want to help you quickly resolve your technical issues and value your input to build products that incorporate your suggestions.

To contact eFolder Technical Support, call 1-800-352-0248 and select Option 2, then Option 1 or submit questions to ReplibitSupport@eFolder.net.

For known problem resolutions, open a browser and navigate to:

Knowledgebase:

https://secure.efoldering.com/support/index.php?/efolder/Knowledgebase/List/Index/69/bdr-for-replibit

1. eFolder BDR for Replibit - Notes

Installing the Replibit OS

- With some hardware, Replibit will automatically start the install **without any prompts**. This will delete all data on the drive that you are using to install Replibit. Therefore, do *not* boot a machine with the Replibit install that has data on it if you want to keep the data.

- Before you can deploy the Replibit appliance on-site for a customer, you MUST register your customers and locations in the **Replibit Licensing Portal**. If this registration process is *not* completed in the Licensing Portal, you will not see, or be able to set up, customers or locations when you sign into Replibit; (Replibit needs to communicate to the Licensing Portal to pull in your customer data); therefore, registering your customers and locations in the Licensing Portal is *not* an optional step. Please see the, "Using the Licensing Portal," section in the, ***"Replibit Administration Guide,"*** for specific steps on Performing the registration process in the Replibit Licensing Portal.

- When installing Replibit, the typical download is approximately 1.5 GB so please wait up to five (5) minutes for the download to complete. You can check the, "View Downloads" internet explorer pop-up window for a status.

2. eFolder BDR for Replibit - Seeding Process

Why use a preload (seed) drive?

- If you have a large amount of data to initially backup for an account, you may want to streamline this process by requesting a preload (seed) drive from us.

- To help determine if this procedure may be necessary for you, please see the Knowledgebase articles below to estimate how long the initial backup job will take when sending data over the Internet.

- We recommend using a preload (seed) drive any time you are backing up more than 100GB of data on a standard Internet connection.

- eFolder offers a round-trip preloading (seeding) service, which includes everything required to properly preload (seed) your account. Depending on the shipping option you choose, it could take a few days to receive your drive, so we recommend starting the process as soon as possible.

- Please review How to Request a Preload Drive to get started.

- If you decide to request your preload drive, please click Request a Preload (Seed) Drive.

- Note: Instructions for EU/Canadian partners can be found: How_to_preload_to_an_eFolder_data_center_in_EMEA_or_Canada.pdf

How to preload (seed) Replibit data to a hard drive

1. Log in to your local Replibit Appliance.

2. On the **Management** menu, click the **Protected Systems** tab.

3. On the **Protected Systems** page, locate the agent you are seeding in the **Systems Name** column and click the **Seed** icon in the **Actions** column on the right.

4. A new window appears asking for the location of your seed drive. Make sure your seed drive is connected and select the root directory as the storage location; then, click **OK**.

5. Repeat steps 3 and 4 for each agent you are seeding to your Replibit Cloud Vault.

6. To monitor the seed creation job, select the **Jobs** tab on the **Vaults Management** menu and highlight the agent to display a percent status indicator. A green check mark appears when processing is completed.

7. When all the protected systems have been seeded to the USB drive, disconnect and ship it back using the provided shipping label.

   Note: Please be sure to create a *readme.txt file* on the USB seed drive that includes the following information:

   - The name of the Replibit Cloud node you are seeding, such as *rb-mynode1*, and
   - Your full contact information.

   Without this information, you could experience a delay in processing your seed data.

8. You will receive an email from our Data Center first telling you that they have received the drive and then a second email with the URL link(s) that you will need to import the seed into your Vault.

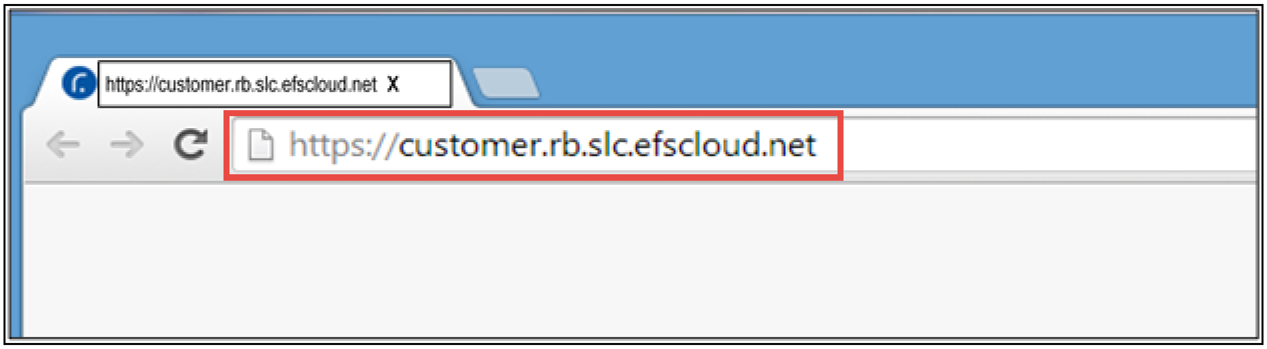
9. After you receive the URL link(s), log on to your Vault and click on the seed icon next to the protected system and then enter the URL link. Only import one seed at a time. Monitor the import in the Jobs section.

3. eFolder BDR for Replibit - Vault Set up Process

After you order an eFolder BDR for Replibit, eFolder will provision a core and email you the information for accessing your eFolder Vault. If you have *not* received this information, please check with the contact person within your organization before proceeding with these steps.

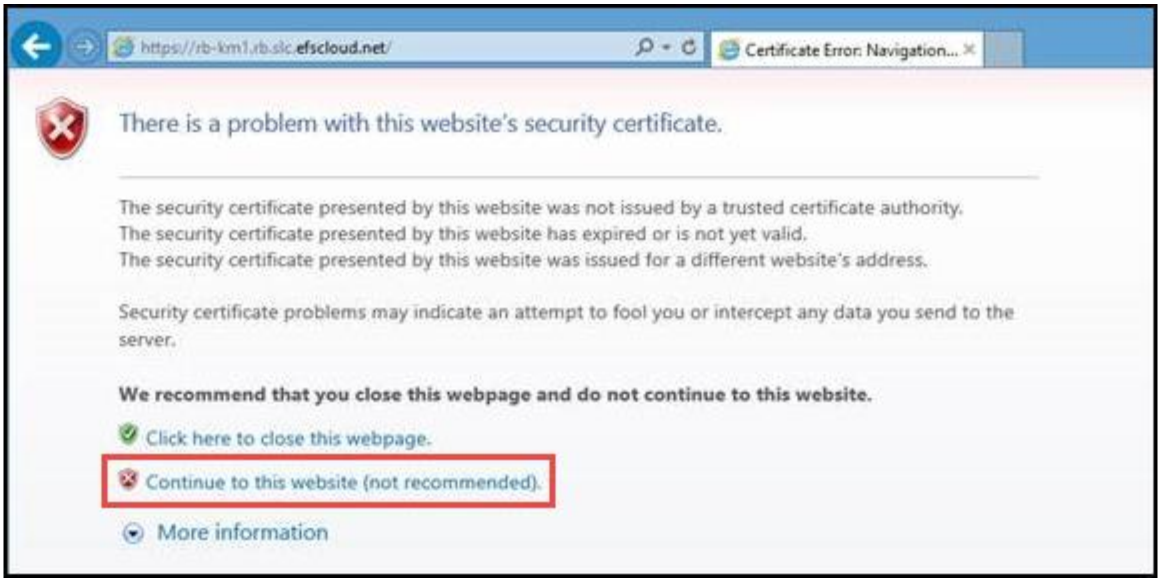
1. Enter the web URL from eFolder in a browser window. This is your eFolder Vault. When you enter the link, it will open a browser.

Note: The following URL is provided only as an example.



https://customer.rb.slc.efscloud.net X
https://customer.rb.slc.efscloud.net

When accessing the URL, you may see a message from you browser that a self-signed certificate does *not* match the full hostname–this is normal and should be ignored. If you see a message indicating the connection is not safe, ignore it and click,"**Continue to this website**."



https://rb-km1.rb.slc.efscloud.net/
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

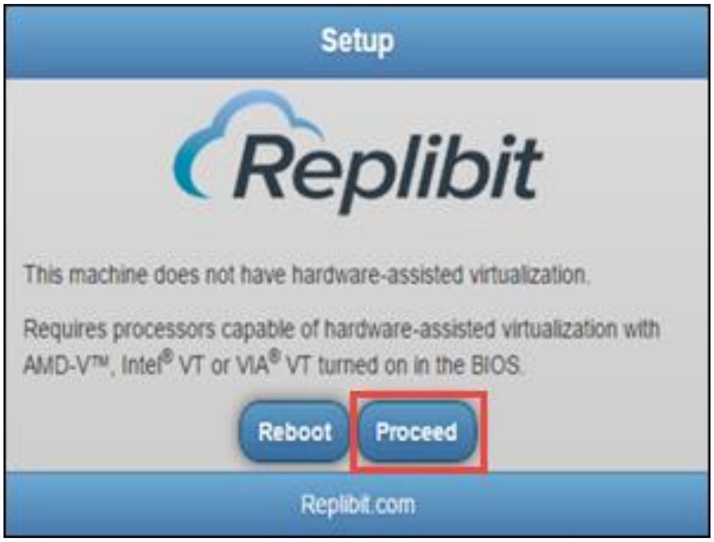
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

2. This is the normal window that will display. Click **Proceed** to continue.

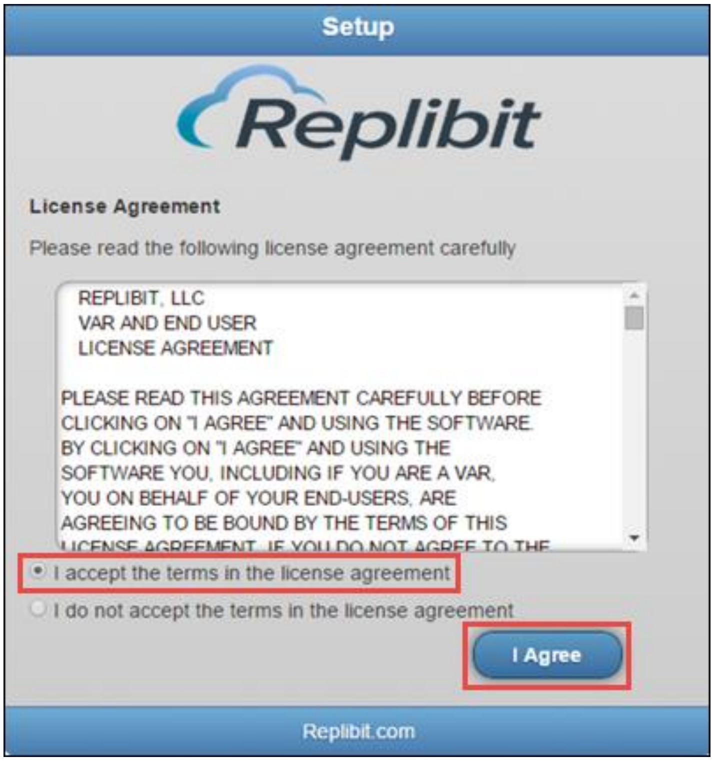


Setup

This machine does not have hardware-assisted virtualization.

Requires processors capable of hardware-assisted virtualization with AMD-V™, Intel® VT or VIA® VT turned on in the BIOS.

3. After reading the agreement, select, *"I accept the terms in the license agreement"* if you are in agreement; then, click **I Agree**.



Setup

License Agreement

Please read the following license agreement carefully

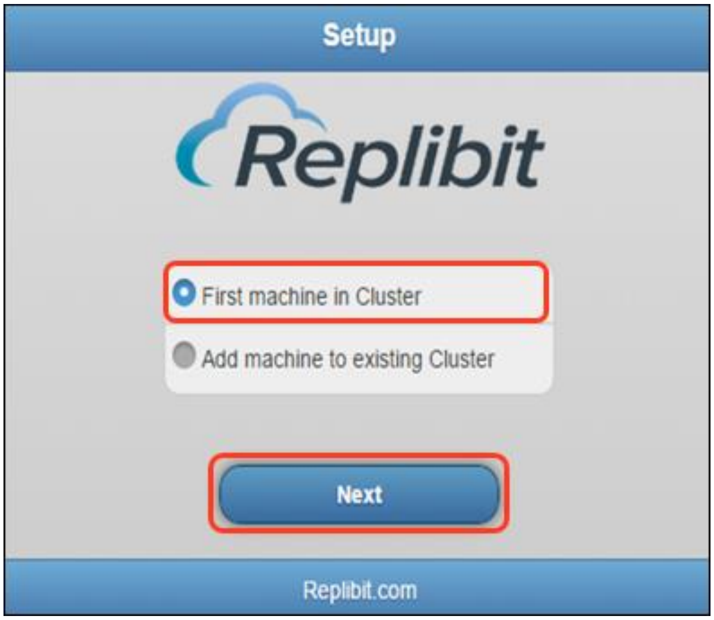
REPLIBIT, LLC
VAR AND END USER
LICENSE AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE CLICKING ON "I AGREE" AND USING THE SOFTWARE. BY CLICKING ON "I AGREE" AND USING THE SOFTWARE YOU, INCLUDING IF YOU ARE A VAR, YOU ON BEHALF OF YOUR END-USERS, ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE

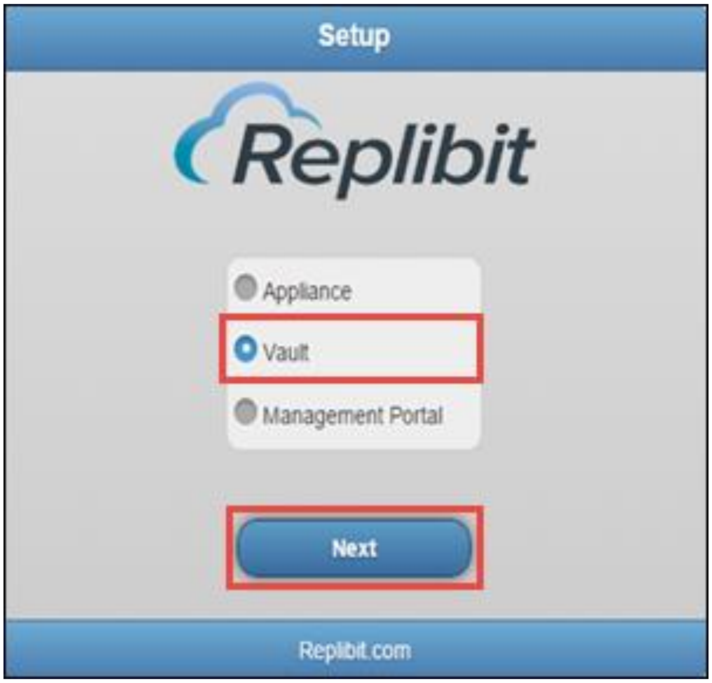
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

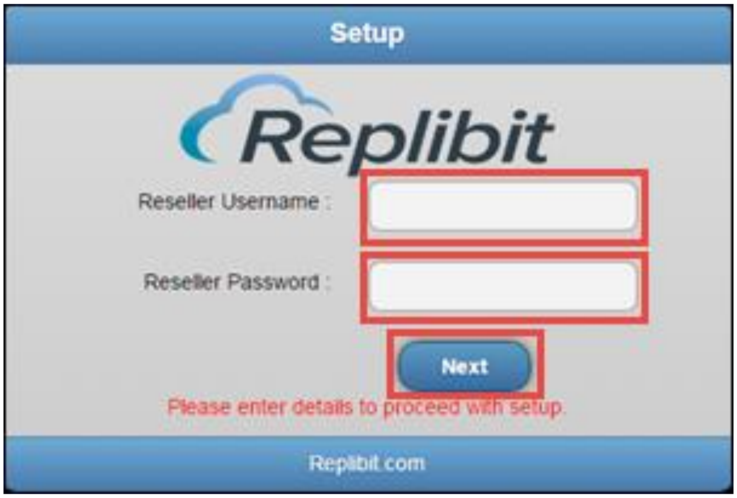
4. Select **First machine in Cluster**; then, click **Next**.



5. Select **Vault**; then click **Next**.

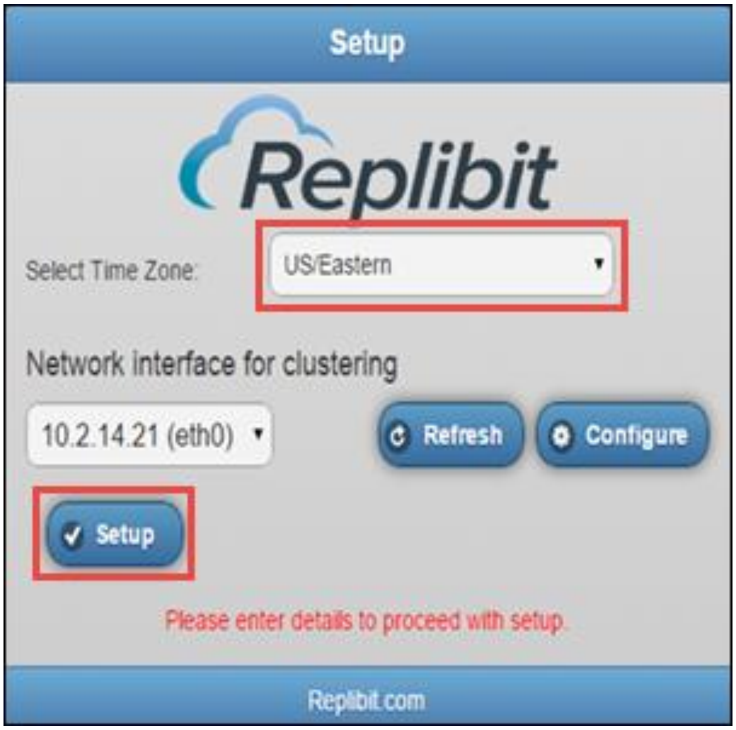


6. Type the *Reseller Username* and *Reseller Password* in their respective fields. Note: these are the Replibit License Portal credentials you received from eFolder. Click **Next**.



Please enter details to proceed with setup.

7. Select your **Time Zone** from the drop-down menu; then, click **Setup**.



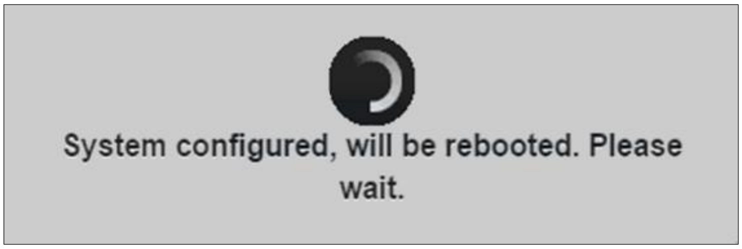
Select Time Zone: US/Eastern

Network interface for clustering

10.2.14.21 (eth0)

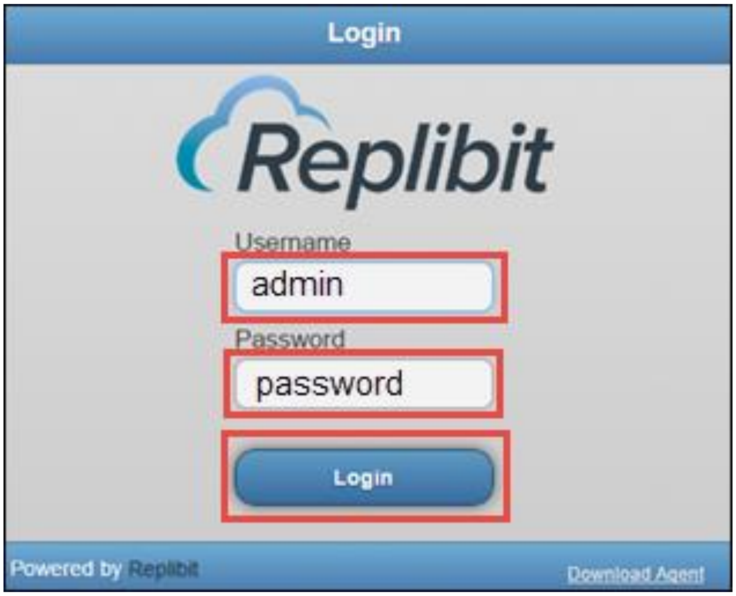
Please enter details to proceed with setup.

8. The system will then reboot. To complete the setup configuration, please allow ample time (up to three minutes) and wait until this process completes.



System configured, will be rebooted. Please wait.

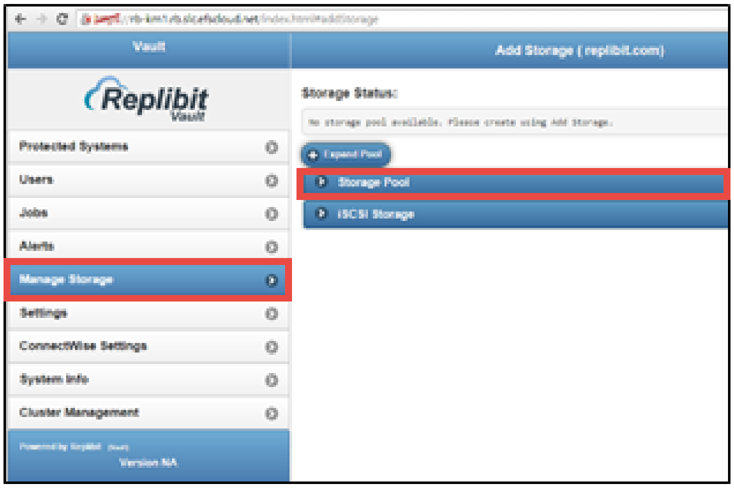
9. Type the *Username* and *Password* in their respective fields. Note: The default is *admin* and *password* with all characters in lower case; then click **Login**



Username: admin

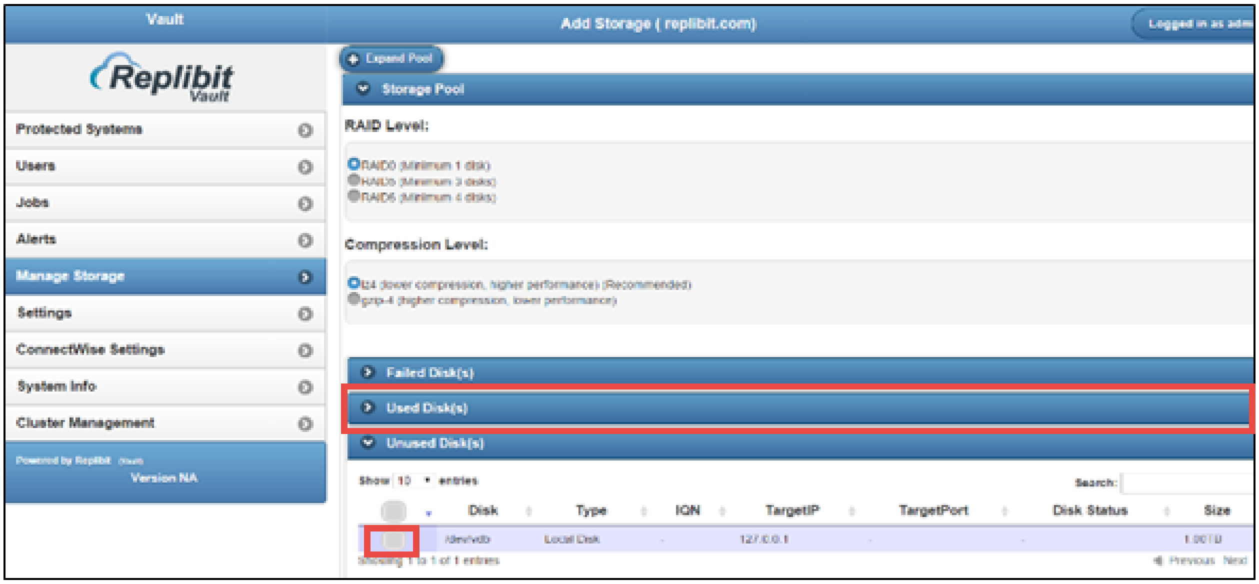
Password: password

10. After login, the Vault Management screen is displayed. Click **Manage Storage** on the left; then, click **Storage Pool** on the right.



No storage pool available. Please create using Add Storage.

11. Select the **Unused Disks** tab; then click on the gray button to add a disk.



RAID Level:

● RAID0 (Minimum 1 disk)
○ RAID5 (Minimum 3 disks)
○ RAID6 (Minimum 4 disks)

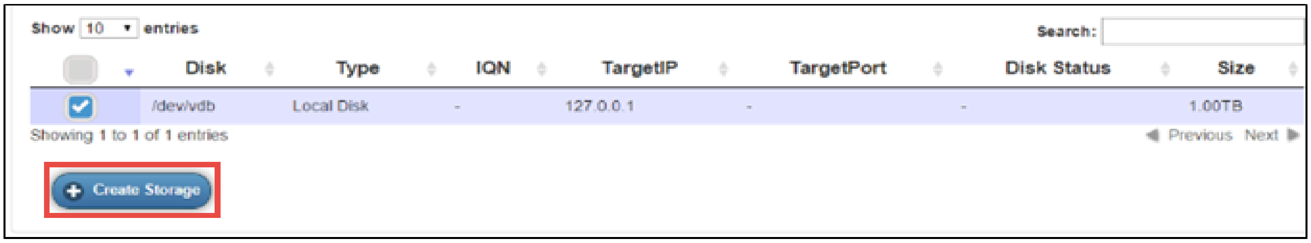
Compression Level:

● lz4 (lower compression, higher performance) (Recommended)
○ gzip-4 (higher compression, lower performance)

□	Disk	Type	IQN	TargetIP	TargetPort	Disk Status	Size
□	/dev/vdb	Local Disk	-	127.0.0.1	-	-	1.00TB

Showing 1 to 1 of 1 entries

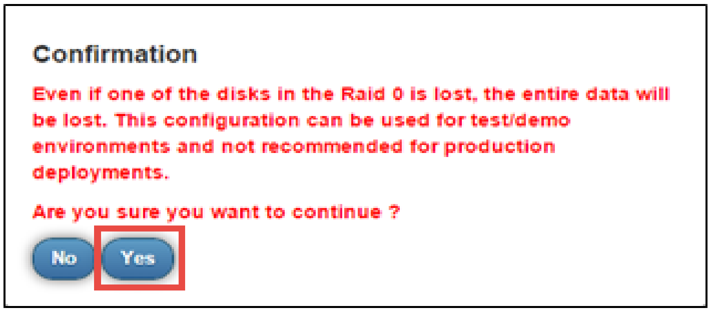
12. Click **Create Storage**.



□	Disk	Type	IQN	TargetIP	TargetPort	Disk Status	Size
☑	/dev/vdb	Local Disk	-	127.0.0.1	-	-	1.00TB

Showing 1 to 1 of 1 entries

13. When the "Confirmation" message appears, click **Yes** to continue.



Confirmation

Even if one of the disks in the Raid 0 is lost, the entire data will be lost. This configuration can be used for test/demo environments and not recommended for production deployments.

Are you sure you want to continue ?

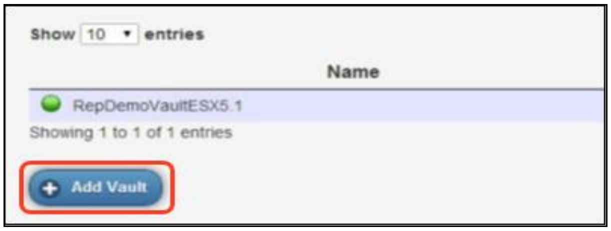
Assign Replication

NOTE: The following instructions apply to the Appliance Web Portal. Switch to the Appliance Web Portal to complete these steps.

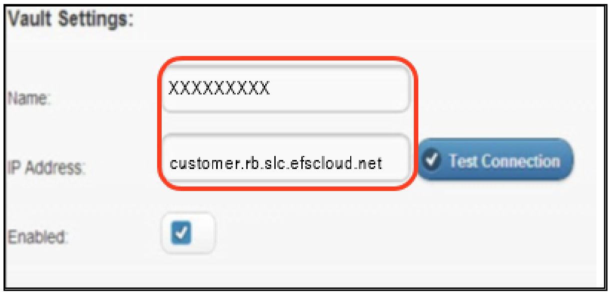
The *Vault Settings Page* in the Replibit Appliance Software is divided into three columns:

Name, IP, and Action.

1. Below the *Name* column, click Add Vault.



2. Enter any name you prefer in the *Name* field.
3. Enter your eFolder server name in the *IP Address* field. Do *NOT* include https://
4. Click Test Connection to verify the connection to the eFolder Vault.
5. After verifying the connection, check the Enabled checkbox.


Vault Settings:

Name: XXXXXXXXX

IP Address: customer.rb.slc.efscloud.net

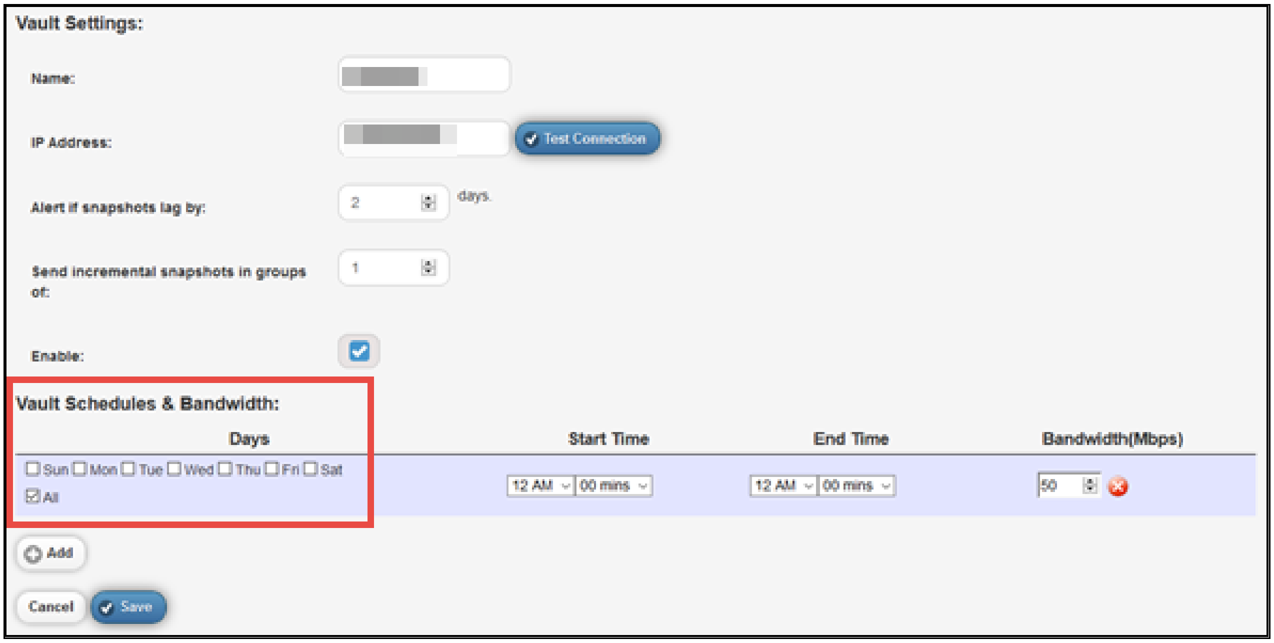
Enabled: ☑

Enter Vault Schedules and Bandwidth

An unlimited number of schedules can be entered for replication that have different bandwidths for each day and hour. However, if you skip certain hours in the schedule or do *not* enter a schedule, no offsite replication will occur during that time period. This may cause serious issues in the future. Schedule changes take effect immediately.

To enter a schedule:

1. At the bottom of the *Vault Settings Page*, select the **Days** you would like to run your replication.



Vault Settings:

Name: [redacted]

IP Address: [redacted]

Alert if snapshots lag by: 2 days.

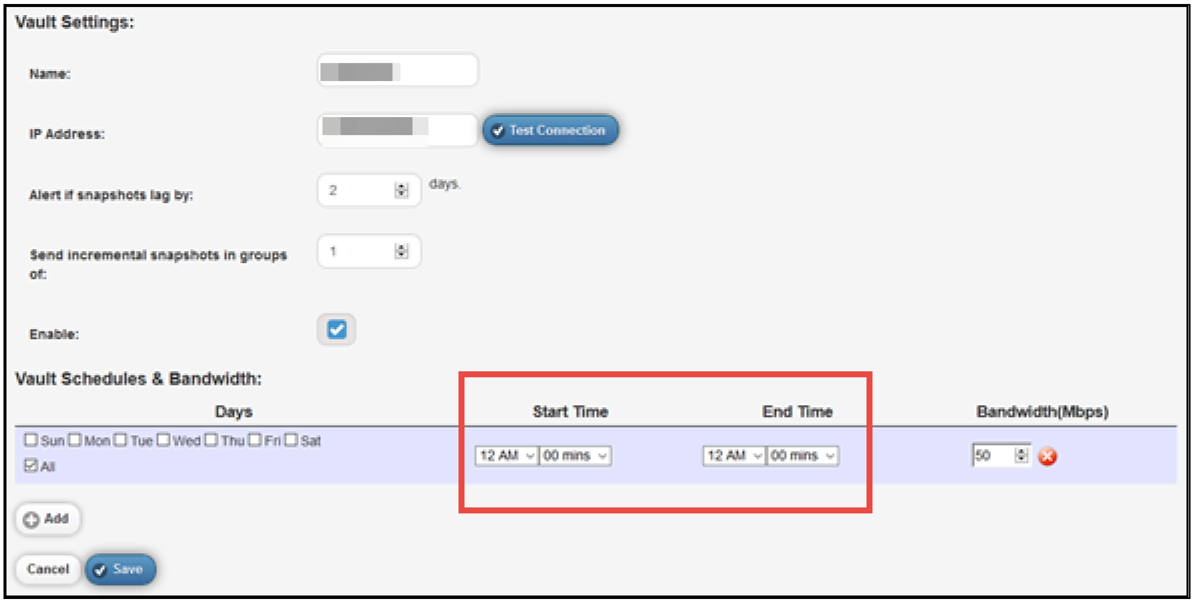
Send incremental snapshots in groups of: 1

Enable: ☑

Vault Schedules & Bandwidth:

Days	Start Time	End Time	Bandwidth(Mbps)
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ All	12 AM 00 mins	12 AM 00 mins	50

2. Then set the **Start Time** and **End Time** from each of the drop-down menus.



Vault Settings:

Name: [redacted]

IP Address: [redacted]

Alert if snapshots lag by: 2 days.

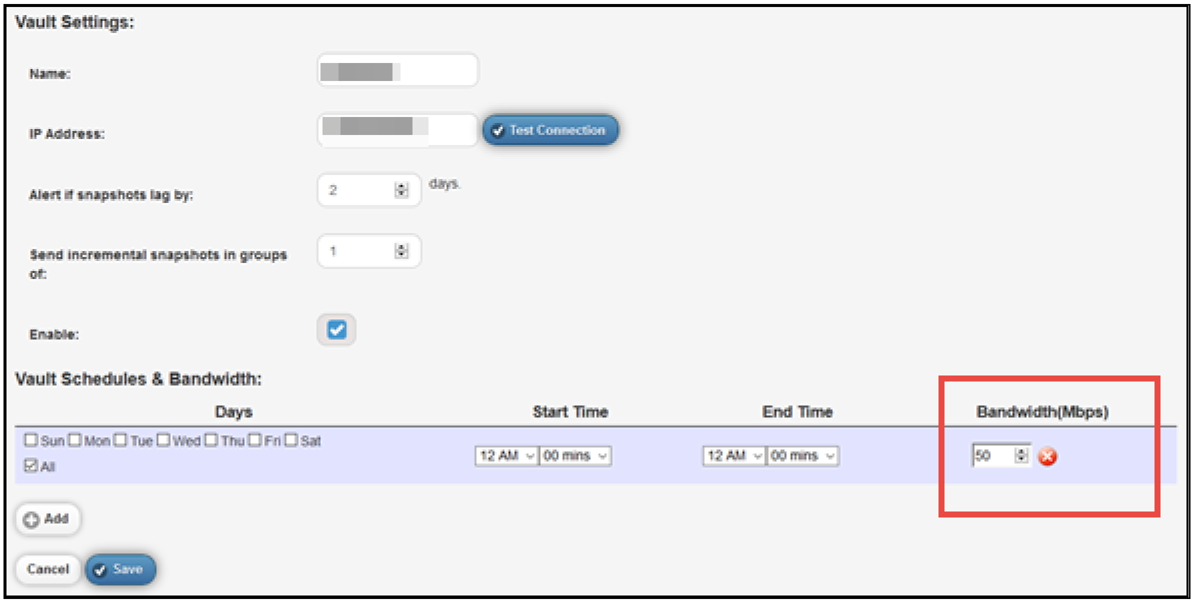
Send incremental snapshots in groups of: 1

Enable: ☑

Vault Schedules & Bandwidth:

Days	Start Time	End Time	Bandwidth(Mbps)
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ All	12 AM 00 mins	12 AM 00 mins	50

3. Click the down arrow and select the **Bandwidth** throttling.



Vault Settings:

Name: [redacted]

IP Address: [redacted]

Alert if snapshots lag by: 2 days.

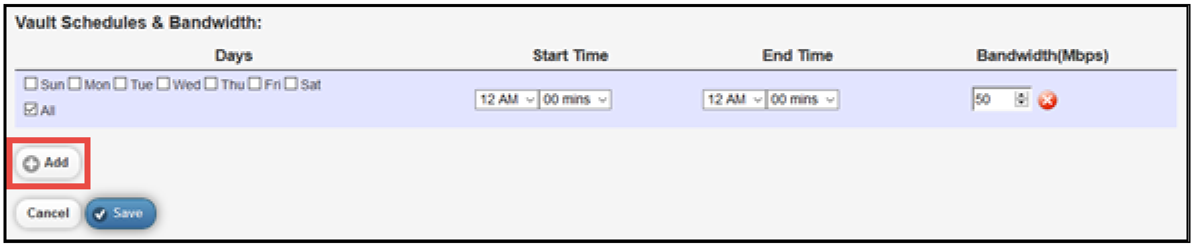
Send incremental snapshots in groups of: 1

Enable: ☑

Vault Schedules & Bandwidth:

Days	Start Time	End Time	Bandwidth(Mbps)
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ All	12 AM 00 mins	12 AM 00 mins	50

4. Click **Add** to create a schedule.

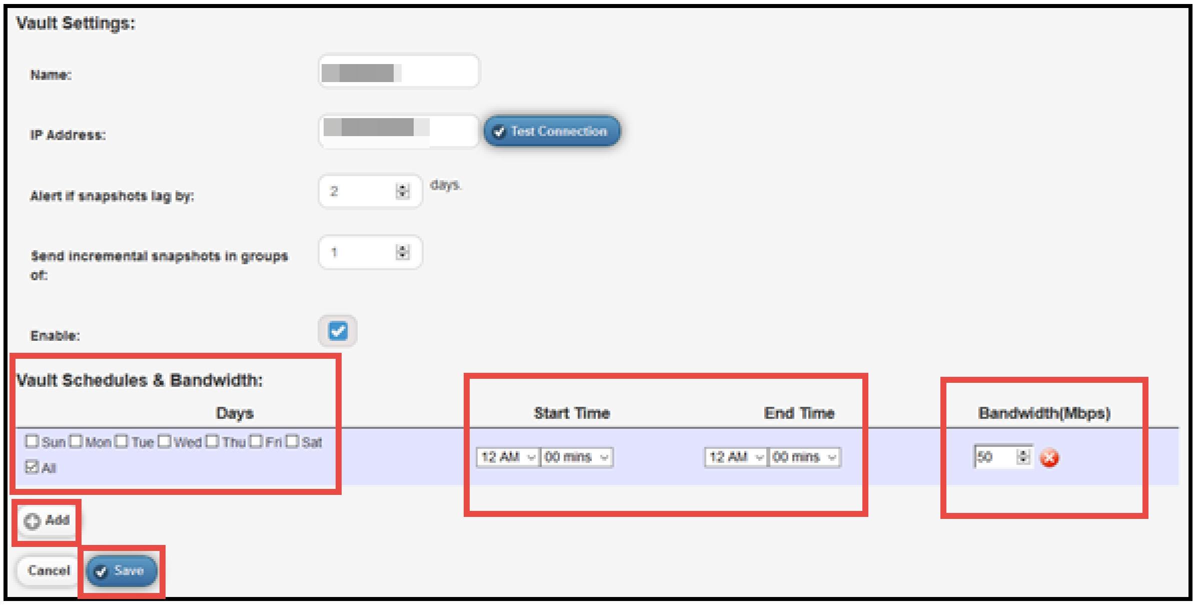


Vault Schedules & Bandwidth:

Days	Start Time	End Time	Bandwidth(Mbps)
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ All	12 AM 00 mins	12 AM 00 mins	50

5. Repeat Steps 1 through 4 to enter additional schedules.

6. Click **Save** when you are complete.



Vault Settings:

Name: [redacted]

IP Address: [redacted]

Alert if snapshots lag by: 2 days.

Send incremental snapshots in groups of: 1

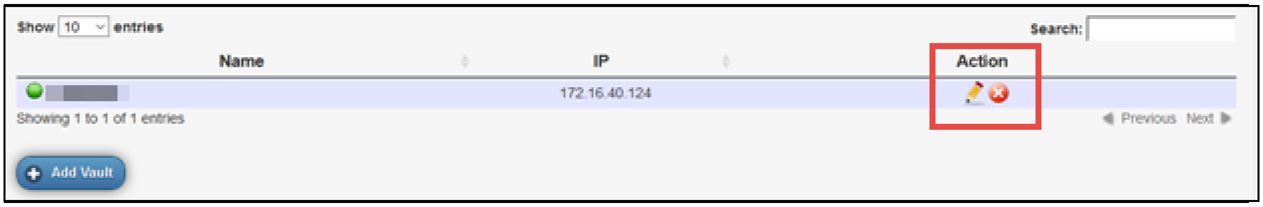
Enable: ☑

Vault Schedules & Bandwidth:

Days	Start Time	End Time	Bandwidth(Mbps)
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat ☑ All	12 AM 00 mins	12 AM 00 mins	50 ✖

To edit or delete a schedule:

1. Click an icon below the Action column on the Vault Settings Page to edit (✎) or delete (✖) a schedule.

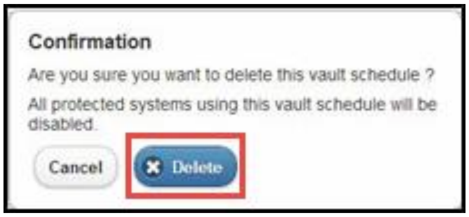


Show 10 entries Search:

Name	IP	Action
● [redacted]	172.16.40.124	✎ ✖

Showing 1 to 1 of 1 entries

2. Deleting a schedule displays the following "Confirmation" message. Please click **Delete** to permanently remove a schedule for replication.



Confirmation

Are you sure you want to delete this vault schedule ?

All protected systems using this vault schedule will be disabled.

After deleting a schedule, any protected system using this schedule will no longer replicate offsite. Deleting the Vault schedule does *NOT* delete the Vault nor does it delete any data at the offsite location. However, all new incrementals sent to the Replibit Appliance are placed in a queue. If too many dates are queued and the client's bandwidth is low, the Vault may need reseeding.

Note:

- eFolder Hosted Vaults
  The Replibit vaults that are hosted at eFolder do *not* allow virtualization directly on the Vault and the *Nightly Boot VM Check* option should *not* be used. In a real world disaster which requires the protected systems to be virtualized in the cloud, you must first contact eFolder Tech Support and request a CCNode. We will configure your Vault to export to a CCNode and then send you the instructions needed on how to recover the protected systems.

4. eFolder BDR for Replibit - Troubleshooting Common Installation Issues

Because the "troubleshooting" section is updated on a frequent basis, please download a current copy prior to each use from the following link:

eFolder BDR for Replibit - Troubleshooting Guide

To quickly troubleshoot frequent Replibit tasks, please access detailed instructions from the following links:

A. How to download your initial Replibit ISO software

B. How to troubleshoot failed backup jobs using the Replibit Backup Analysis Tool

C. How to troubleshoot Replibit VSS issues

D. How to troubleshoot your CPU usage

E. How to troubleshoot the Appliance not communicating with the Replibit Licensing Portal

F. How to perform the Appliance migration process

G. How to replace a failed disk in the backup storage pool

A. How to download your initial Replibit ISO software

To install Replibit, you will need to download the Replibit ISO file and burn the ISO to a bootable flash drive.

1. Before you begin your Replibit Software download, note that Replibit *may* automatically start the installation without any prompts when using certain hardware; therefore, please use a machine that you do *not* need to preserve any data on, as Replibit may delete your computer's contents during the install process.

2. Download the latest version of the Replibit Software using the link below; (select your download link under, *"Downloads"* from the Replibit page, agree to the *"License Agreement"* Terms and Conditions, and click ***Open/Save***):

   Replibit .iso download

   Note: This downloading process may take up to five minutes (the typical download is approximately 1.5 GB), so please check your *"View Downloads"*—Internet Explorer pop-up window for a status if needed.

For comprehensive step-by-step instructions on the complete installation process, please refer to the, "***Replibit Administration Guide,"*** using the following link: https://backup.securewebportal.net/efolder/files/Replibit/Replibit_Administrators_Guide.pdf

B. How to troubleshoot failed backup jobs using the Replibit Backup Analysis Tool

1. Once you have installed Replibit, it is *highly recommended* to check your backups. Test your backups by:
   - mounting,
   - booting as a VM,
   - exporting as a virtual disk, and
   - exporting as a Bare Metal Restore.

2. If you experience *any* failed backup jobs, please troubleshoot them using the following procedure:
   - Download the latest copy of the Replibit Backup Analysis Tool from the KB article:

   Backup Analysis Tool or

   http://ftp.replibit.net/isodownload/RepAnalysisTool.exe

   The Replibit Backup Analysis Tool will analyze the health of a Protected System, capture logs, and creates a text file with a synopsis of any issues it finds.

Note:

- You will need Administrator Privileges to run the Replibit Backup Analysis Tool.
- You will need to run the tool on the Protected System from an elevated command prompt after stopping the Replibit service.
- The tool will create a .zip file in the **C:\ReplibitAnalysisTool\Replibit** folder along with all other files.
- Please send eFolder *only* the .zip file when directed.
- When you run the tool, please click the **Enter** button when prompted to keep the data local.

After the tool is finished, you can open up the text file it created (problems.txt) and start troubleshooting the items it detected.

Some of the Replibit Backup Analysis Tool integrity tests include:

- Ensuring that Replibit can traverse the directory structure,
- Numerating out the directories,
- Reading-down the Master File Table and looking for orphan objects,
- Checking for a bad pointer within the Master File Table,
- Checking for high fragmentation levels (which affects virtualization from Windows),
- Checking for any DLL mismatches,
- Running a real-time tracking mechanism that creates a hash file,
- Running a full differential in the last backup day (automatically) to compare every block in the backup set to that of the production set,
- Real-time resilvering of data,
- Tracking Window Boot DLL files' expectation of virtualization (proper modifications to Boot DLL files greatly impacts stability and performance on Virtualization).

If any piece of the data set exceeds the tolerances, Replibit will proactively fail the backup and send you a notification so you can troubleshoot.

C. How to troubleshoot Replibit VSS issues

Replibit and VSS Troubleshooting

When a Replibit backup fails, the problem is almost always caused by the failure of the Microsoft VSS provider, or one of the application-specific VSS writers. This section and the, *"Replibit and VSS Troubleshooting"* link above will help you to diagnose these failures.

The top 10 reasons for backup failures associated with VSS include:

1. Snapshot creation failed due to Windows VSS failure.
2. There is not enough Shadow Copy storage space to create a backup.
3. A VSS writer is in a failed state.
4. A volume does not pass a CheckDisk (chkdsk).
5. The Master File Table is highly fragmented.
6. A volume is extremely fragmented.
7. Another application interrupted the snapshot creation.
8. An uninstalled backup application left behind its VSS provider.
9. The OS does not pass a System File Checker (SFC) scan.
10. A Windows Server Backup disk is online.

If you require additional troubleshooting on VSS issues, please access your related error(s) from the articles in the VSS Search Results:

- VSSADMIN List Writers and their Services - VSS
- Backup failure, VSS WMI Writer unregistered
- Windows Event Log: VSS Event ID 12292
- Error: "snapshot creation for the volume has failed" in aristos.log.
- Remove Unwanted VSS Provider
- Re-registering VSSAdmin - Writers not stable
- Old Installation of Acronis Prevents Replibit Backups
- Selected writer 'SqlServerWriter' is in failed state Status: 8
- Event ID 12297 — VSS Shadow Copy Creation and Storage Space Availability

D. How to troubleshoot your CPU usage

If you are experiencing performance issues, please follow these steps:

1. Look at the system resources.
   a) CPU and RAM usage are easy to monitor by opening Task Manager.
   b) Additionally, the disk sub-system can greatly affect VSS performance.

2. Monitor the CPU before and after the backup to set a baseline and to observe the change.
   a) If the system is running an old or low-end CPU, you may already have a high CPU usage baseline, and running another service will exceed your CPU's capacity.
   b) If this is the case, please adjust the 'Worker Threads' or set the 'Affinity' to increase the backup duration using the Knowledgebase articles shown below; the Replibit agent defaults to backup all volumes and uses four worker threads per processor core. The KB articles below demonstrate how to specify which volumes are backups and how many worker threads are utilized.

   Modifying the Replibit Agent - Set Volumes and Worker Threads - aristos.cfg

   https://replibit.kayako.com/Knowledgebase/Article/View/16/0/modifying-the-replibit-agent---set-volumes-and-worker-threads---aristoscfg

   Note: Lowering the amount of worker threads will reduce the speed of the backup. If the backups start overlapping, you may need to increase the time between snapshots.

3. As with the CPU, monitor the RAM and pagefile usage prior to, and during, a backup.
   a) If the Protected System is already using all of the available RAM, the VSS service will end up using the slower pagefile.
   b) Adding more RAM is the best option but you can also look at reducing the amount of RAM other services are using.
   c) By default, exchange and SQL will use all available RAM.
   d) A quick web search will guide you on setting the maximum RAM that different services can use.
   e) Run **chkdsk** and then defrag all the partitions being backed up.
   f) Remember that VSS needs free disk space to create the ShadowCopies.

How to troubleshoot your CPU usage (continued)

g) If changing worker threads to as low as one still does not work, you can try changing the affinity on aristosagent to lower CPU usage while a backup is running by executing these two commands from a raised CMD or .BAT file:

```
wmic process where name="AristosAgent.exe" CALL setpriority "below normal" PowerShell
"$Process = Get-Process AristosAgent; $Process.ProcessorAffinity=1"
```

Note: As guidance, you can create a .BAT file with the two commands, then create a recurring scheduled task to run the .BAT file during or after a scheduled backup kicks off. Then you will know that *AristosAgent.exe* will be running.

E. How to troubleshoot the Appliance not communicating with the Replibit Licensing Portal

1. When you set up your Replibit Appliance for the first time, you will need to logon with a Replibit Reseller Account so you can choose the Customer and Location.
2. If you are having trouble connecting to: *licesing.replibit.com*, please follow the troubleshooting steps below:
    a. Change the DNS setting to 8.8.8.8; then try to log on again.
    b. Verify that outbound traffic is *not* being blocked.

F. How to perform the Appliance migration process

Note: Please perform each of the following migration steps below *one at a time on each protected system.* DO *NOT* ATTEMPT TO DO THIS ON ALL SYSTEMS AT THE SAME TIME.

1. Stop and disable the Replibit service on the Protected System.
2. Disable replication of the Protected System on the original appliance.
3. Add 20 days to the Retention Policy on both the appliance and the vault so data will *not* be deleted during this process.
4. Migrate the Protected System via USB or Network in the **Details** page of that Protected System on the appliance.
5. After the migration is complete, verify on the new Appliance that the data is there and is recoverable. Additionally, boot in **Test** mode.
6. Change the IP address of the appliance in *aristos.cfg* located in **c:\program files (x86)\replibit** to the new appliance's IP.
7. Enable the Replibit service on the Protected System.
8. After several backups have run, repeat the verification process by ensuring that the data is present and is recoverable.
9. Enable Replication on the new Appliance to the Vault.
10. After the replication is back in sync, remove the 20 days on the retention policy.

For comprehensive step-by-step instructions on the complete installation process, please reference the, ***"Replibit Administration Guide,"*** using the following link:

https://backup.securewebportal.net/efolder/files/Replibit/Replibit_Administrators_Guide.pdf

G. How to replace a failed disk in the backup storage pool

https://replibit.kayako.com/Knowledgebase/Article/View/113/0/replacing-a-failed-disk-in-the-backup-storage-pool

1. If your pool has lost a disk but the RAID is still intact (you have *not* lost two disks in a RAID5 or three disks in a RAID6), your pool will be in a degraded state.
2. Use the *Storage Pool* drop-down to find the **Failed Disk(s)** section. In this section you should be able to see your failed disk.
3. After physically replacing the failed disk:
    a. Recreate the disk as a RAID0 (if the RAID controller is *not* passing the disks as JBOD) with a disk of equal or greater size. In this scenario, you will need to reboot.
    b. After this is complete, use the *Storage Pool* drop-down to find the **Unused Disk(s)** section. In this section, you should find an unused disk.
4. Return to the **Failed Disk(s)** section, and click **Replace** next to the failed disk. Select the correct Unused Disk and click **Replace.**
5. A popup will display notifying you that the disk is being replaced.
6. While the disk is being replaced, you will see the resilvering status under *Storage Status*.
7. When the resilvering process is complete, the pool will return to an Online Status.

Key Replibit Knowledgebase Links & Guides:

All Replibit Knowledgebase articles

eFolder's Replibit FAQ

How To Create an eFolder BDR for Replibit Preload (Seed) Drive PDF

Replibit Backup Analysis Tool (no port or ticket needed)

Top 10 Reasons for Backup Failures

eFolder BDR for Replibit – Quick Start Guide

UEFI Based Systems

Hard Drive Configuration Requirements - Best Practice

eFolder BDR for Replibit Supported Environments Guide

eFolder BDR for Replibit Best Practices for Software Installation

Replibit Ports

Modifying the Replibit Agent - Set Volumes and Worker Threads

How to fix missing BCD files with EISA partitions - BootVM Fails

OpenDNS - Network Security Service

ConnectWise Integration Guide

Appliance Migration Process

Bare Metal Restore Guide

5. eFolder BDR for Replibit - Disaster Recovery Process

Solution Overview

Prepare for the worst-case scenario with the eFolder Continuity Cloud. Downtime of critical infrastructure can cost a business dearly. When disaster strikes, backups will not be enough to keep businesses operating smoothly. The eFolder Continuity Cloud allows bare-metal backup images stored in eFolder's storage cloud to be virtualized in the cloud in minutes or hours, not days or weeks. These virtual servers can then be connected to the Internet and existing LAN networks through a virtual firewall and router or VPN tunnels.

Note: To successfully deploy a Replibit Protected System on a CC Node, you will need a general knowledge of Replibit, Hyper-V, and Pfsense.

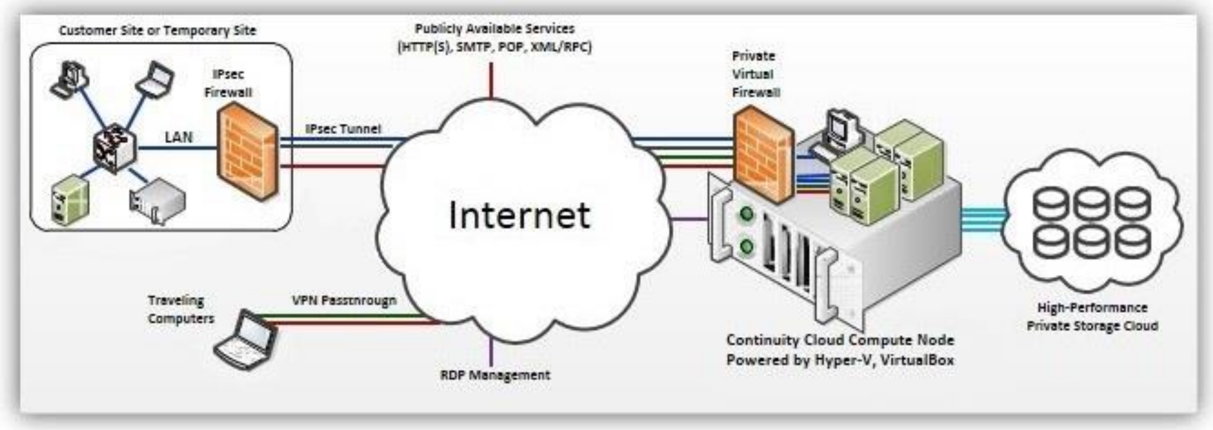
Technical Overview

The eFolder Continuity Cloud allows fast recovery from partial site or entire site failures. In the event of a server failure, (or the failure of an entire site), a local eFolder BDR Appliance can first be used to easily, quickly, and transparently virtualize the failed server(s) onsite. If the BDR has been destroyed or is otherwise unavailable, the continuity cloud can be activated to bring the failed infrastructure back up. Powerful virtual routing and firewalling features provide easy and, in certain configurations, fully transparent access to virtualized servers.

To begin using the eFolder Continuity Cloud:

- Submit a critical (highest priority) support ticket, including details of the resources needed (such as the number of servers, total RAM, disk space, and so forth) and the account(s) containing the data for the computers to be virtualized.
- eFolder will respond to these requests 24/7/365 and will provision one or more Continuity Cloud compute nodes for your dedicated use. Once provisioned, you will have full self-management capabilities of the resources on the compute node and will be self-sufficient.

Technical Overview (continued)


Customer Site or Temporary Site
IPsec Firewall
LAN
IPsec Tunnel
Publicly Available Services (HTTP(S), SMTP, POP, XML/RPC)
Private Virtual Firewall
Internet
Traveling Computers
VPN Passthrough
RDP Management
Continuity Cloud Compute Node Powered by Hyper-V, VirtualBox
High-Performance Private Storage Cloud

- Once you agree to the acceptable use terms, you are given RDP access to the compute node(s).

- After logging in to a compute node, you will have full access to self-configure the virtual router and virtual firewall, allowing the configuration of any needed VPNs and NAT/PAT policies.

- If you choose to virtualize a bare-metal backup image directly without any conversion process (only available for certain types of bare-metal backups, or where "hot standby" VMs have already been created automatically

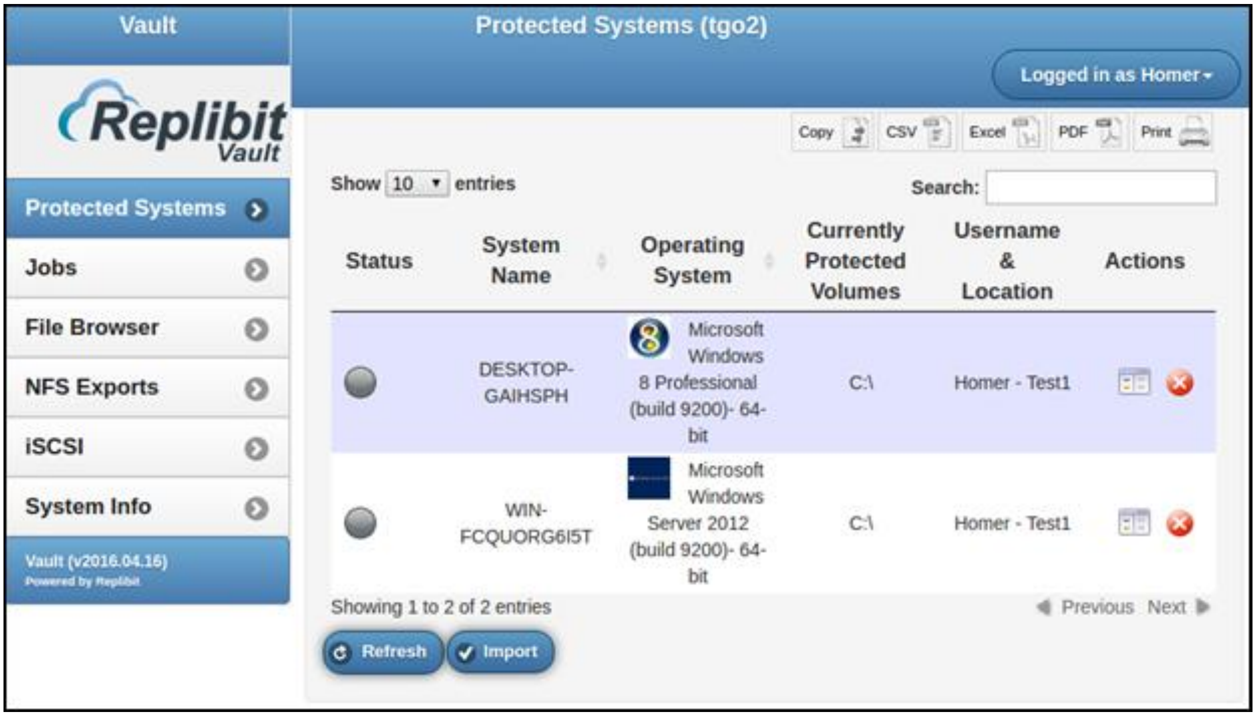
- The VMs can be brought up with a variety of networking configurations.
  - A test mode is available where the VMs are fully isolated on a virtual network.
  - More common is the mode where VMs are bridged to a VLAN that is dedicated to and connected to all of a partner's provisioned compute nodes.
  - The virtual router and firewall control the flow of traffic to and from this internal, private VLAN to a VLAN dedicated to the external connectivity of the virtual network.
  - All compute nodes are assigned several public IPv4 addresses (IPs are provisioned as requested, up to one public IP address per VM that needs to be virtualized).
  - All traffic to these public IPs are automatically routed to the external VLAN dedicated to the partner's compute node(s).

Technical Overview (continued)

- The virtual router/firewall has full control over the entire network—virtualized servers can be exposed in a DMZ, NAT/PAT can be used, IPsec VPN tunnels can be configured, and VPN connections can be passed through to virtualized servers.
- IPsec VPN tunnels are especially powerful for a partial-site failure situation where the customer site's firewall is still operational and can form a VPN tunnel to the virtual router/firewall running in the cloud. In this situation, the internal IP addresses of the virtualized servers in the cloud can be the same as they were before, and thus users can transparently use the virtualized servers running in the cloud without any configuration changes. Additionally, any public services such as POP3 and OWA can be exposed through NAT/PAT policy rules—Partners then update the DNS records of their servers to point to the new public IP addresses, and these public services then become available again, just as before.
- When the original servers are ready to be recovered, the virtualized servers can take incremental backups, which will update the backed up data with the normal process. You can then download and restore these bare metal images or request a copy of the data on a USB drive or NAS device.
- Finally, you should submit a ticket to de-provision the cloud compute nodes, and the cloud compute nodes are then automatically wiped clean back to their original state so that they are ready for use by the next Partner.

Exporting a Protected system

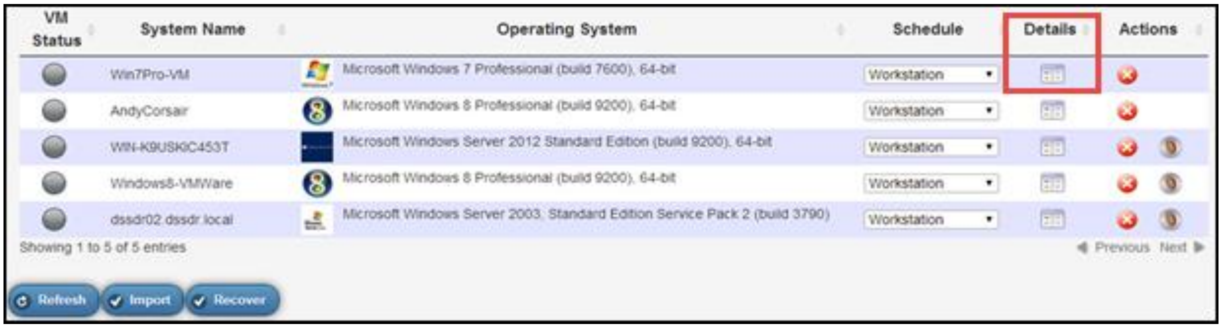
1. Log in to your Replibit Vault with the customer account and navigate to the **Protected Systems** menu.



Status	System Name	Operating System	Currently Protected Volumes	Username & Location	Actions
●	DESKTOP-GAIHSPH	Microsoft Windows 8 Professional (build 9200)- 64-bit	C:\	Homer - Test1	▦ ✖
●	WIN-FCQUORG6I5T	Microsoft Windows Server 2012 (build 9200)- 64-bit	C:\	Homer - Test1	▦ ✖

Showing 1 to 2 of 2 entries

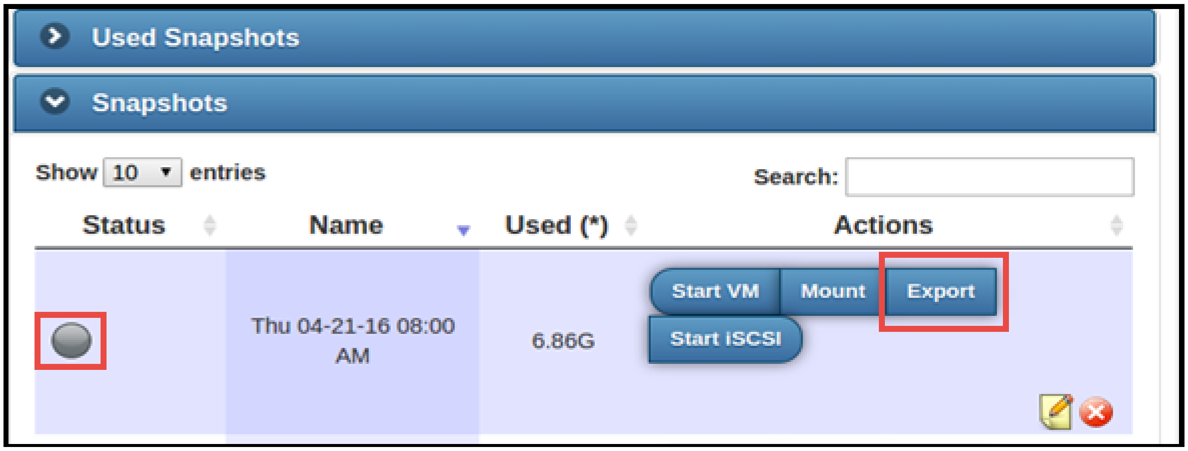
2. Find the Protected System that is needed to be recovered and click on **Details**.



VM Status	System Name	Operating System	Schedule	Details	Actions
●	Win7Pro-VM	Microsoft Windows 7 Professional (build 7600), 64-bit	Workstation	▦	✖
●	AndyCorsair	Microsoft Windows 8 Professional (build 9200), 64-bit	Workstation	▦	✖
●	WIN-K9USKIC453T	Microsoft Windows Server 2012 Standard Edition (build 9200), 64-bit	Workstation	▦	✖
●	Windows8-VMWare	Microsoft Windows 8 Professional (build 9200), 64-bit	Workstation	▦	✖
●	dssdr02.dssdr.local	Microsoft Windows Server 2003, Standard Edition Service Pack 2 (build 3790)	Workstation	▦	✖

Showing 1 to 5 of 5 entries

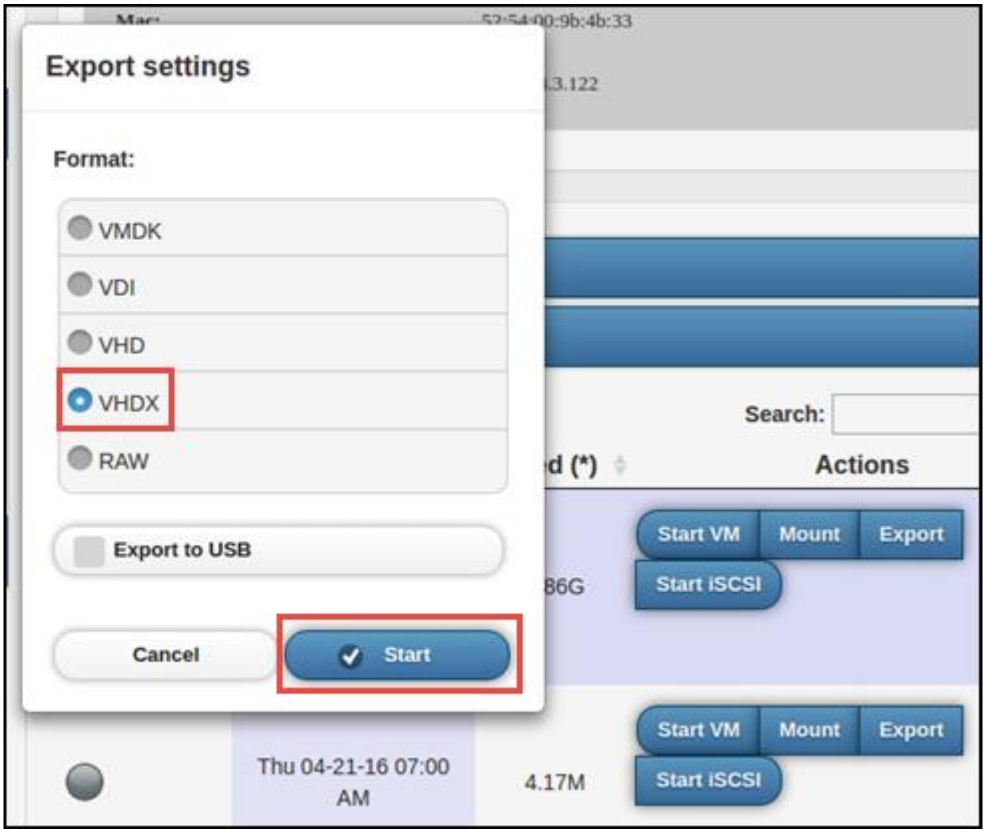
3. Locate the Shapshot that you need to recover and click on **Export**.



Show 10 entries

Status	Name	Used (*)	Actions
●	Thu 04-21-16 08:00 AM	6.86G	Start VM Mount Export Start iSCSI

4. Click on the VHDX option and then **Start.**



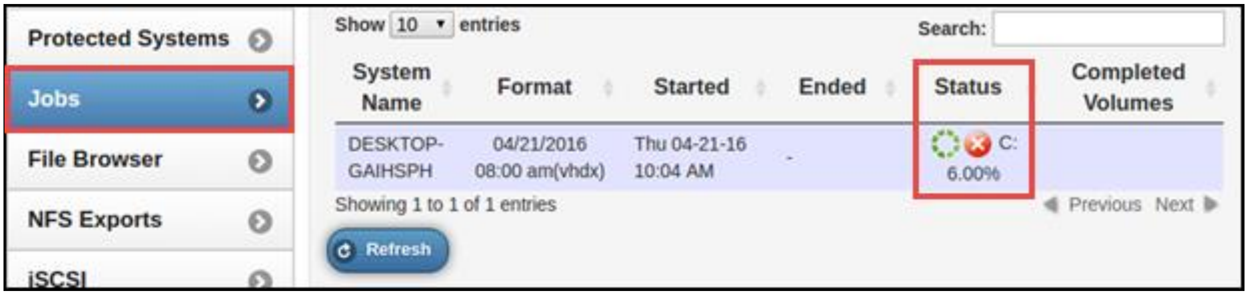
Export settings

Format:

○ VMDK
○ VDI
○ VHD
● VHDX
○ RAW

□ Export to USB

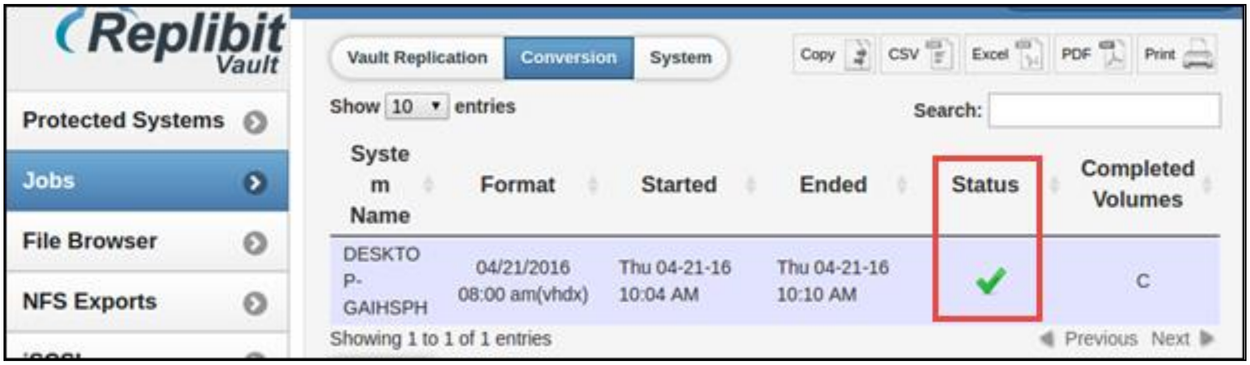
5. To monitor the Conversion process, select the ***Jobs menu*** under the **Conversion** tab.



System Name	Format	Started	Ended	Status	Completed Volumes
DESKTOP-GAIHSPH	04/21/2016 08:00 am(vhdx)	Thu 04-21-16 10:04 AM	-	C: 6.00%	

Showing 1 to 1 of 1 entries

When your conversion job is completed, the following window will display:



System Name	Format	Started	Ended	Status	Completed Volumes
DESKTOP-GAIHSPH	04/21/2016 08:00 am(vhdx)	Thu 04-21-16 10:04 AM	Thu 04-21-16 10:10 AM	✓	C

Showing 1 to 1 of 1 entries

While you are waiting on the Conversion job, connect to the CC Node using the credentials that were sent to you and start setting up the network and firewall.

Virtual Firewall and Router Configuration

While the restore is running, configure the firewall on the Continuity Cloud node.

For help with this, please refer to the document "*Continuity Cloud Virtual Firewall.pdf*" using the link below. After the firewall policies are configured, you can resume with the next step.

https://secure.efoldering.com/efolder/files/ContinuityCloud/eFolder_Continuity_Cloud_Virtual_Firewall_Guide.pdf

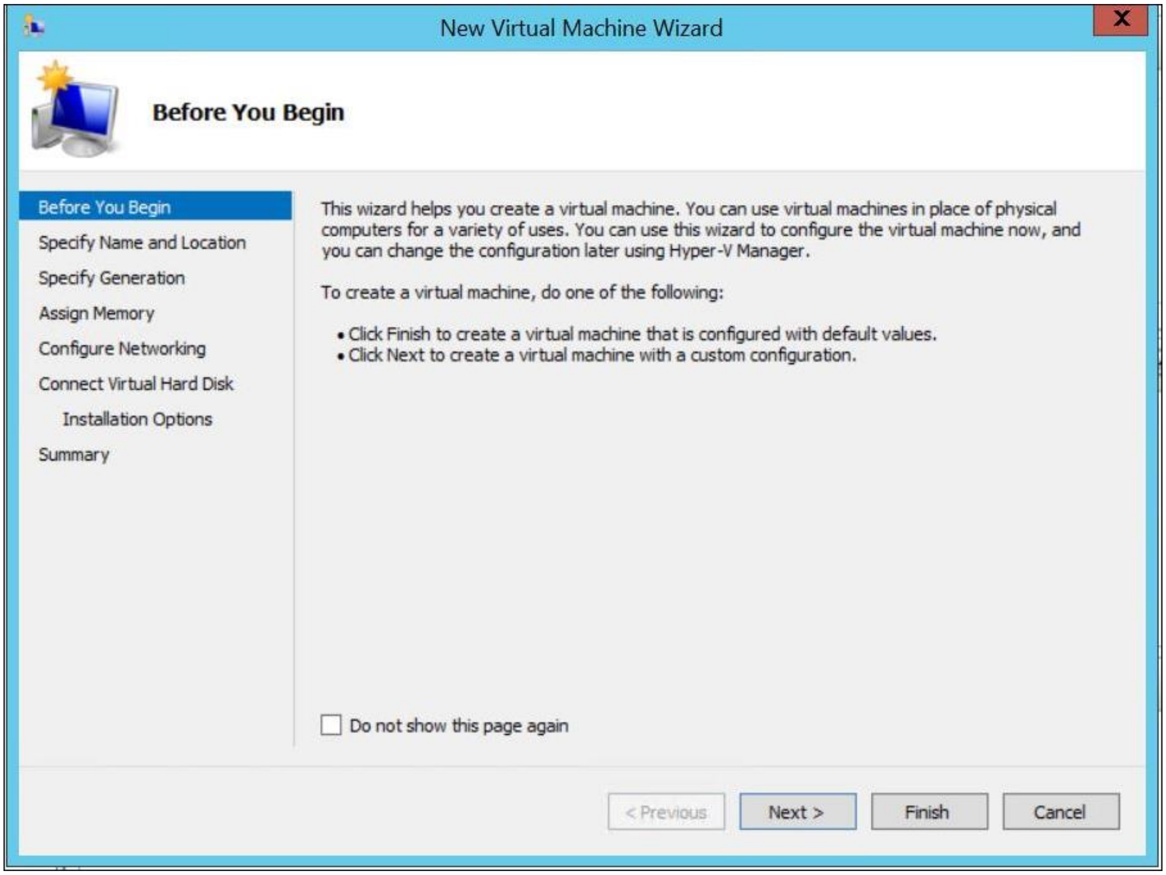
Manage and Start VMs

Now that your virtual router and firewall policies and configured, you are ready to start your VMs.

Use the Hyper-V console to connect to the VMs and log in and reconfigure the network to use the proper LAN IP address.

Important Note: If you are virtualizing an SBS server or domain controller, the first time the server boots, when the Windows boot menu appears, you should immediately press F8 and choose **Active Directory Restore Mode** or **Directory Services Restore Mode**. After the server comes up, log in as the local Administrator (.\Administrator) using the *Directory Services Restore Mode* password; then, edit the settings for the network adapter to reset the static IP and the DNS server address. For SBS servers, the DNS server address will be the same as the static IP (or 127.0.0.1).

1. Open the **Hyper-V Management** console.



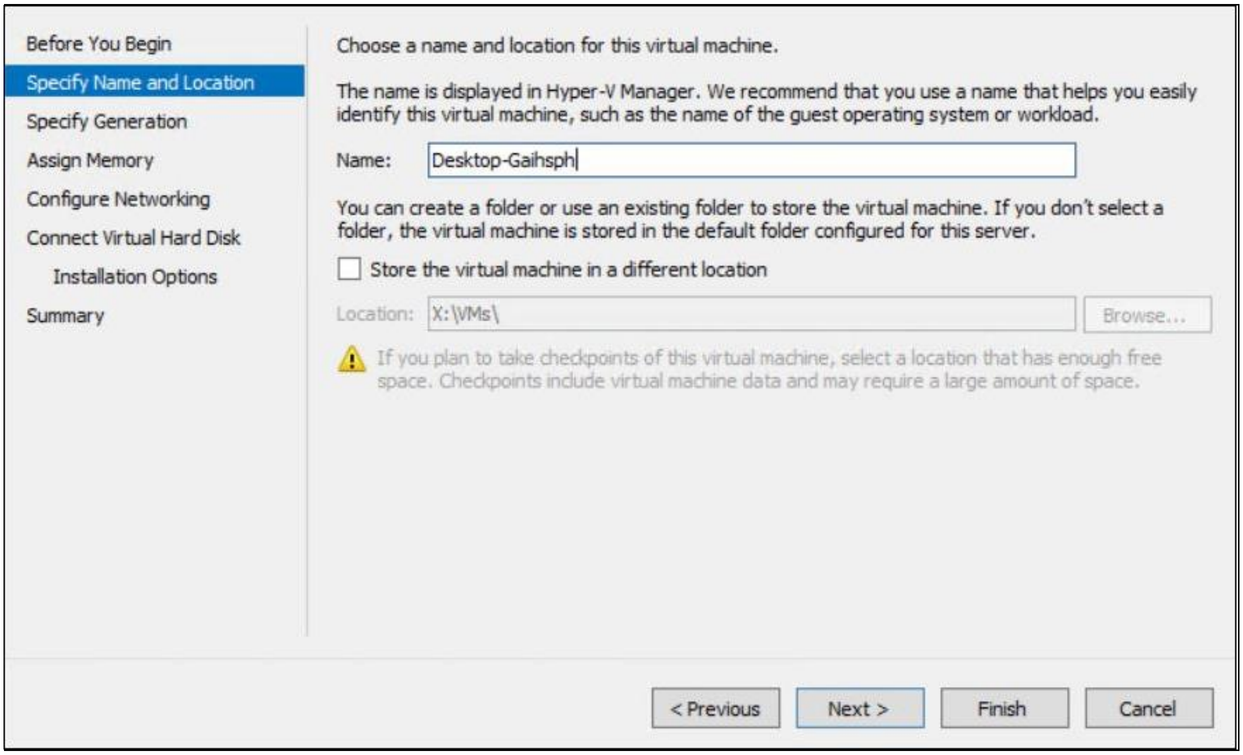
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

□ Do not show this page again

2. Create a new VM.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Desktop-Gaihsph

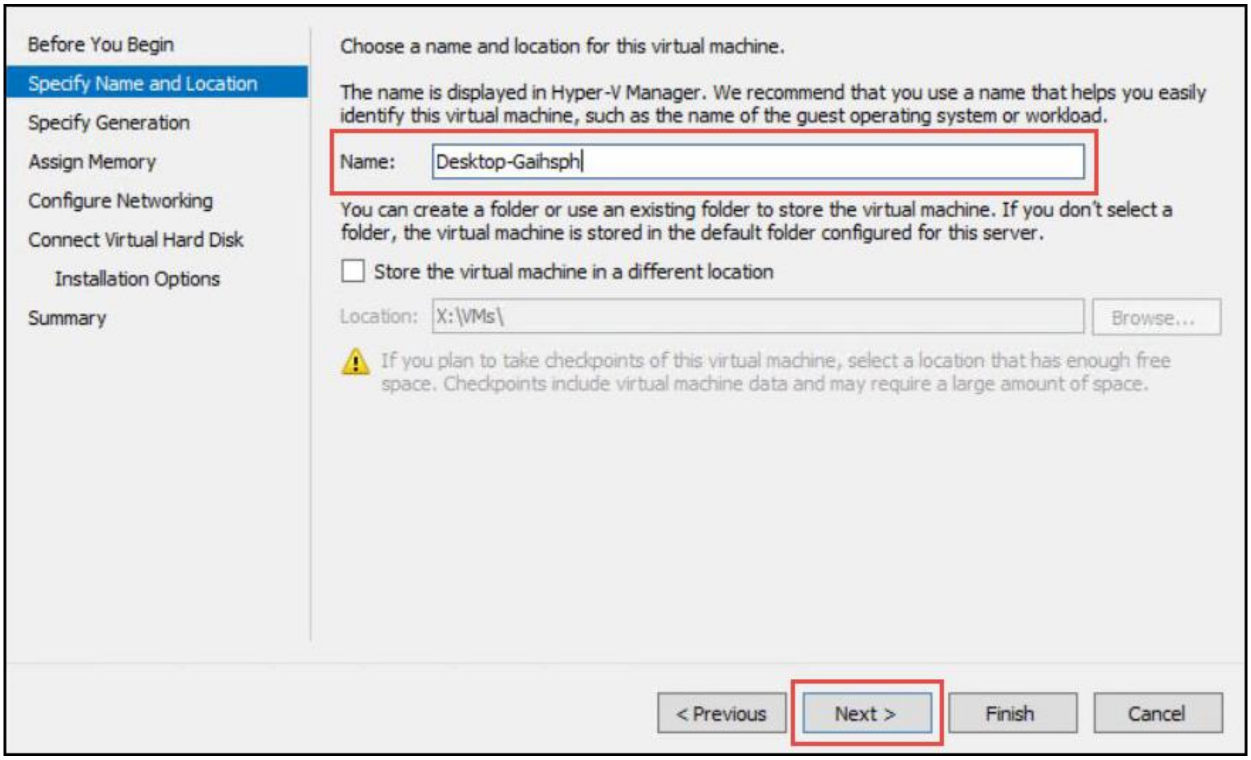
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

Location: X:\VMs\ Browse...

⚠ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

3. Enter name of system and click **Next.**



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Desktop-Gaihsph

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

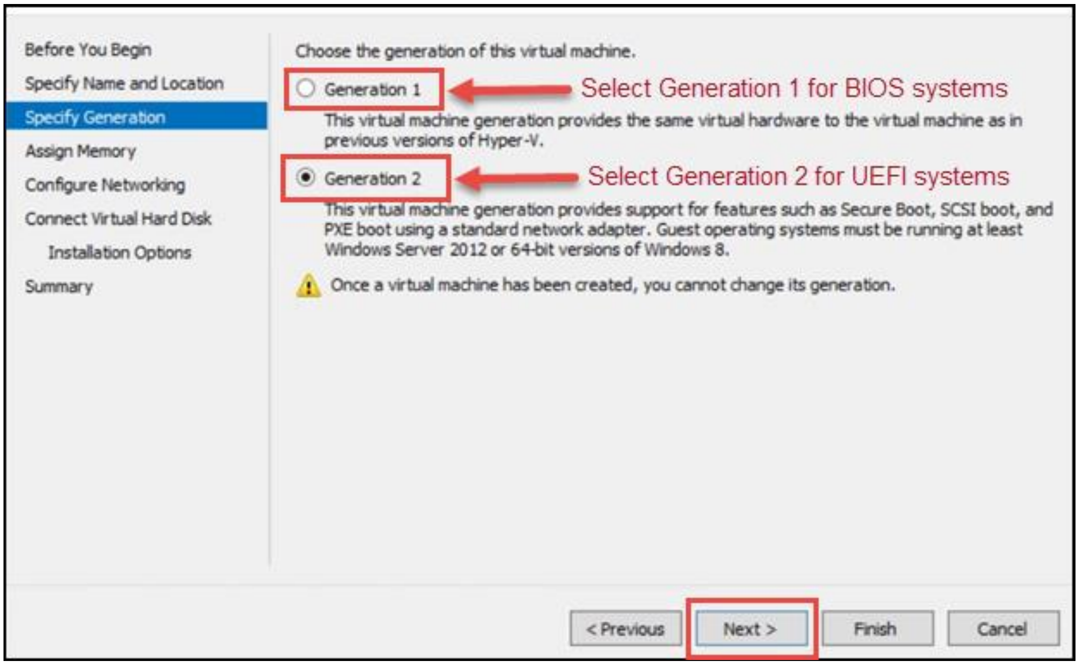
☐ Store the virtual machine in a different location

Location: X:\VMs\ Browse...

⚠ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

4. Select the radio button that corresponds to the generation of your virtual machine:
    - For BIOS systems, choose *Generation 1.*
    - For UEFI systems, choose *Generation 2.*

    Then select **Next**.



Choose the generation of this virtual machine.

○ Generation 1 ← Select Generation 1 for BIOS systems

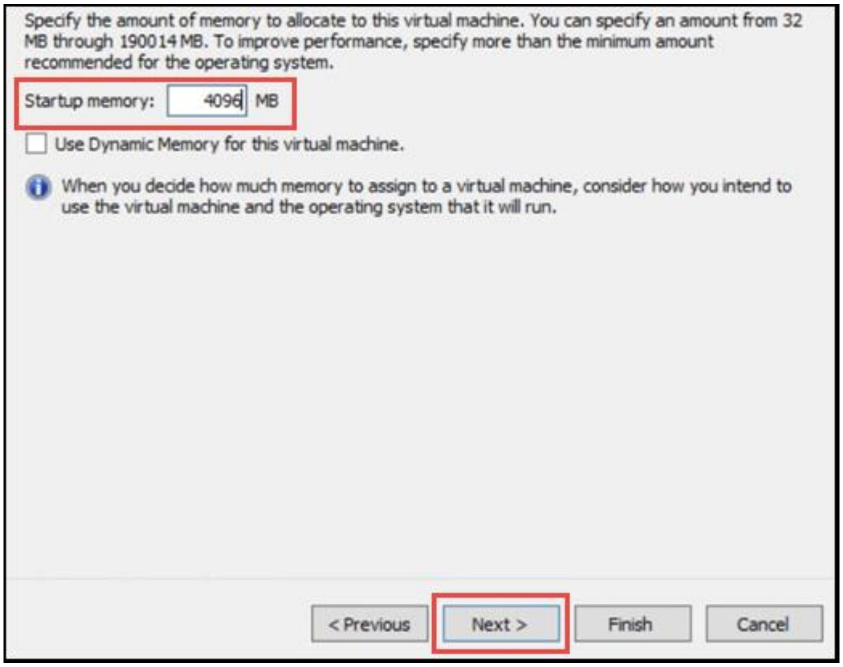
This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.

● Generation 2 ← Select Generation 2 for UEFI systems

This virtual machine generation provides support for features such as Secure Boot, SCSI boot, and PXE boot using a standard network adapter. Guest operating systems must be running at least Windows Server 2012 or 64-bit versions of Windows 8.

⚠ Once a virtual machine has been created, you cannot change its generation.

5. Enter the amount of memory and click **Next**.



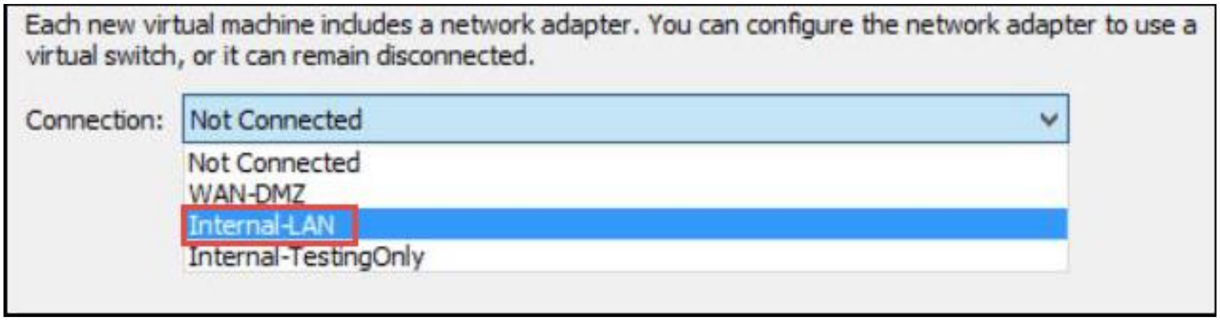
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 190014 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 4096 MB

□ Use Dynamic Memory for this virtual machine.

ⓘ When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

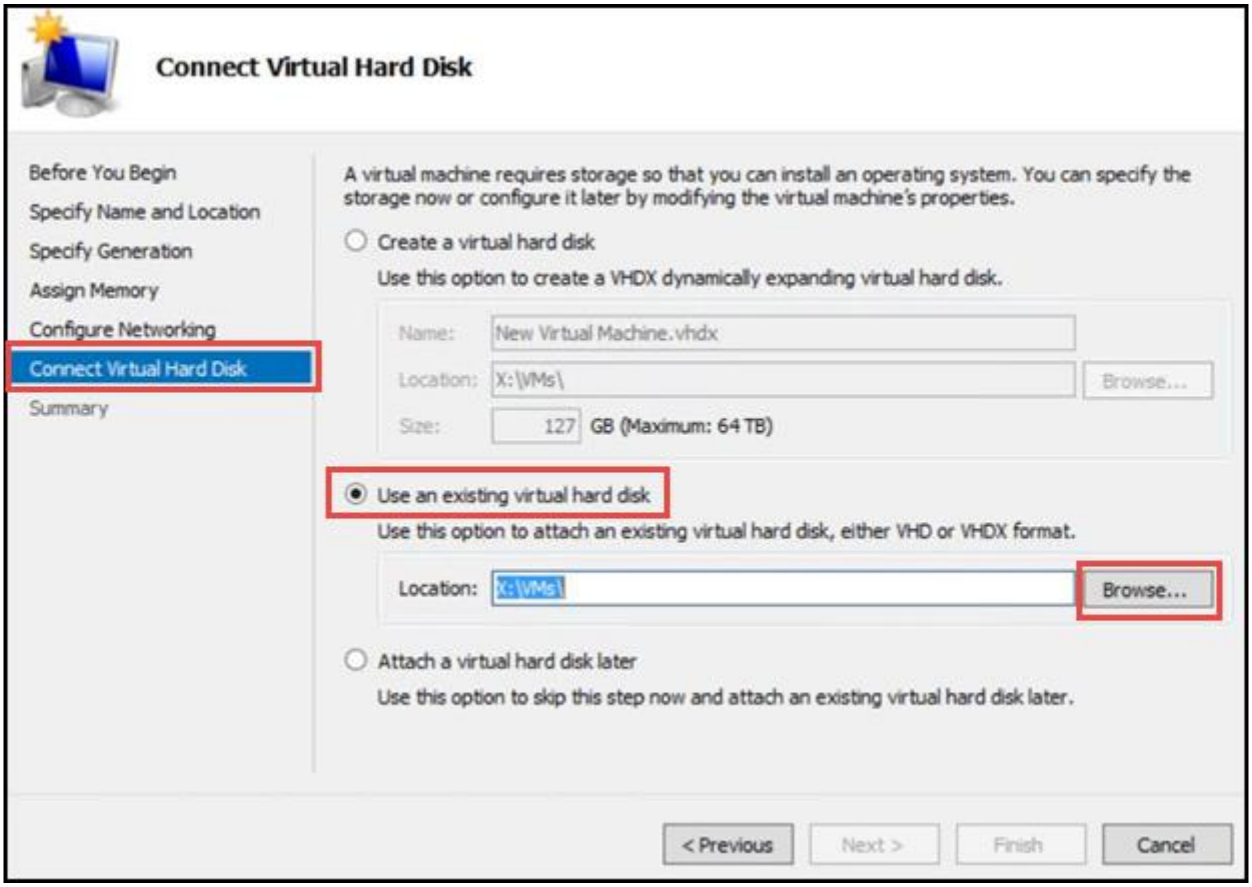
6. Select the network connection and click **Next.**



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

7. Pick **Use existing virtual hard disk** and then click **Browse**



Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: New Virtual Machine.vhdx

Location: X:\VMs\ Browse...

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

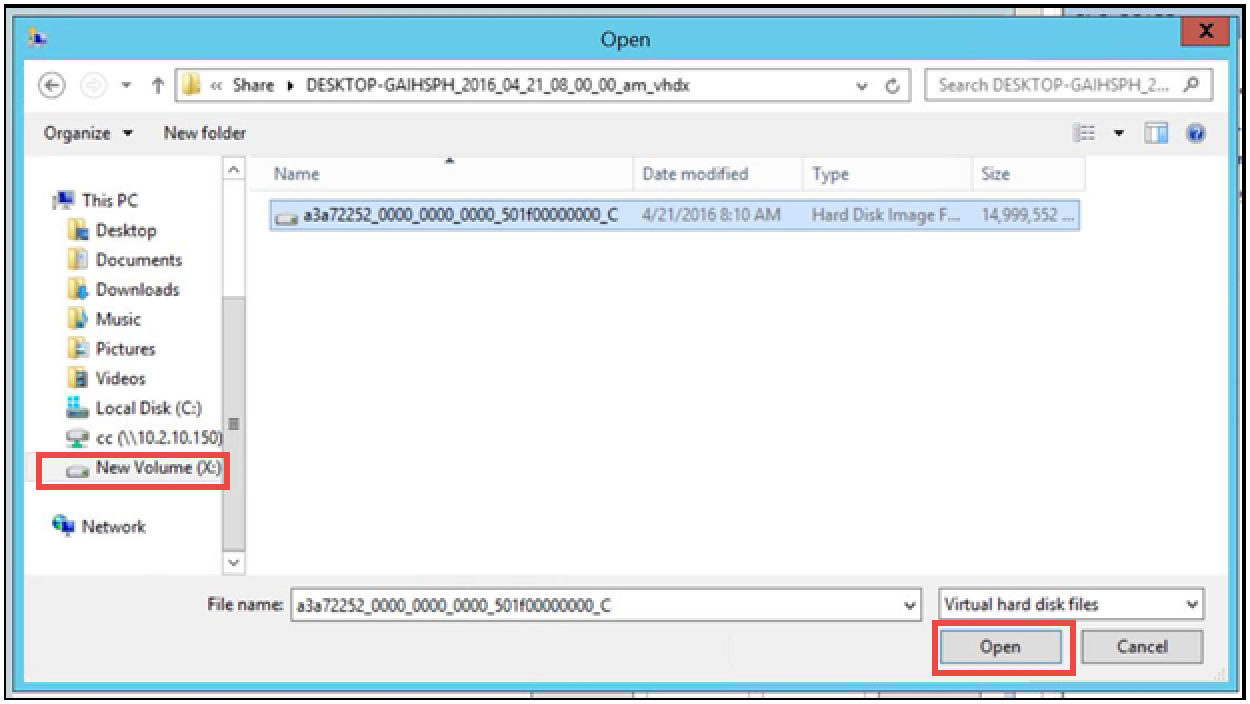
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: X:\VMs\ Browse...

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

8. Navigate to x:\share to find the exported hard drive folder, highlight the drive, and click **Open**.

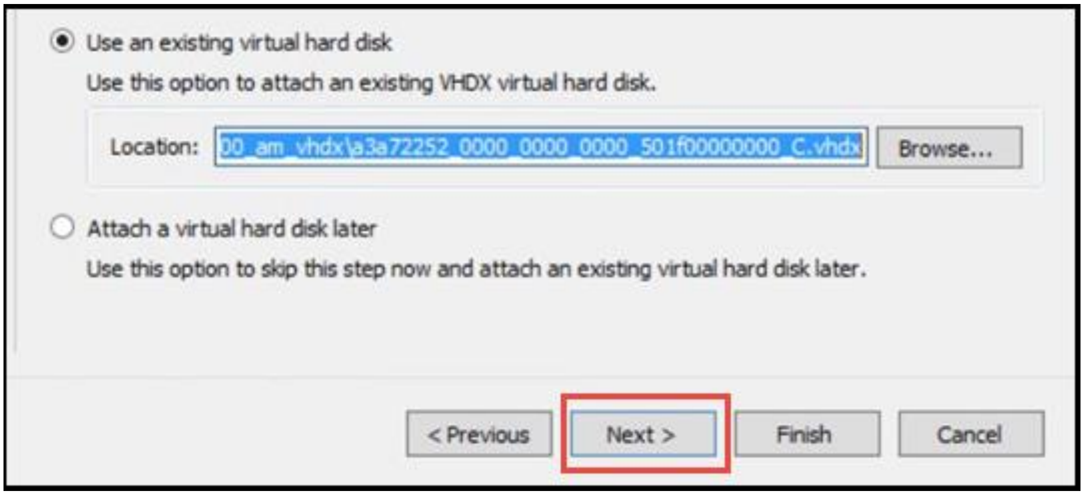


Name	Date modified	Type	Size
a3a72252_0000_0000_0000_501f00000000_C	4/21/2016 8:10 AM	Hard Disk Image F...	14,999,552 ...

File name: a3a72252_0000_0000_0000_501f00000000_C

Virtual hard disk files

9. Click **Next**.



● Use an existing virtual hard disk

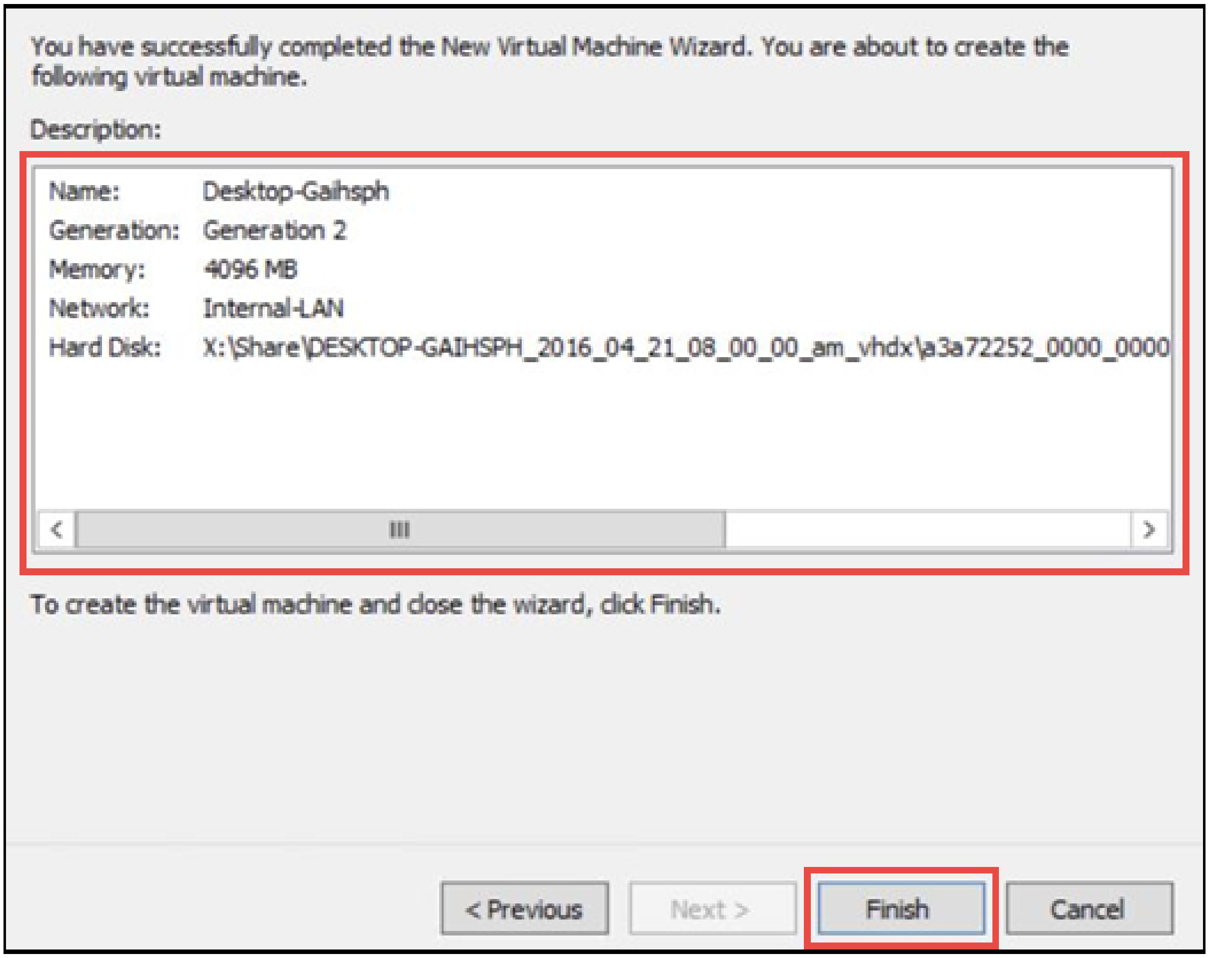
Use this option to attach an existing VHDX virtual hard disk.

Location: 00_am_vhdx\a3a72252_0000_0000_0000_501f00000000_C.vhdx

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

10. Verify the settings and select **Finish.**



You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

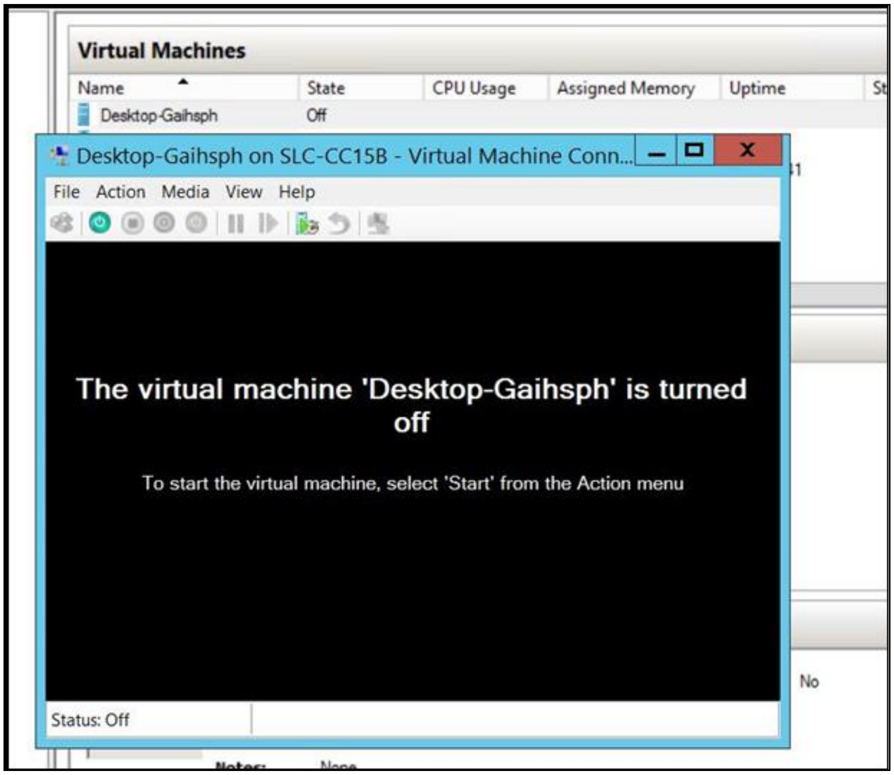
Description:

```
Name:        Desktop-Gaihsph
Generation:  Generation 2
Memory:      4096 MB
Network:     Internal-LAN
Hard Disk:   X:\Share\DESKTOP-GAIHSPH_2016_04_21_08_00_00_am_vhdx\a3a72252_0000_0000
```

To create the virtual machine and close the wizard, click Finish.

The VM is ready to boot. If you need to add additional virtual drives or any other system setting changes. right click on the **VM** and click **Settings.**

To power on the VM, double click the **VM** and select the **power** button. The following windows should display:



Virtual Machines

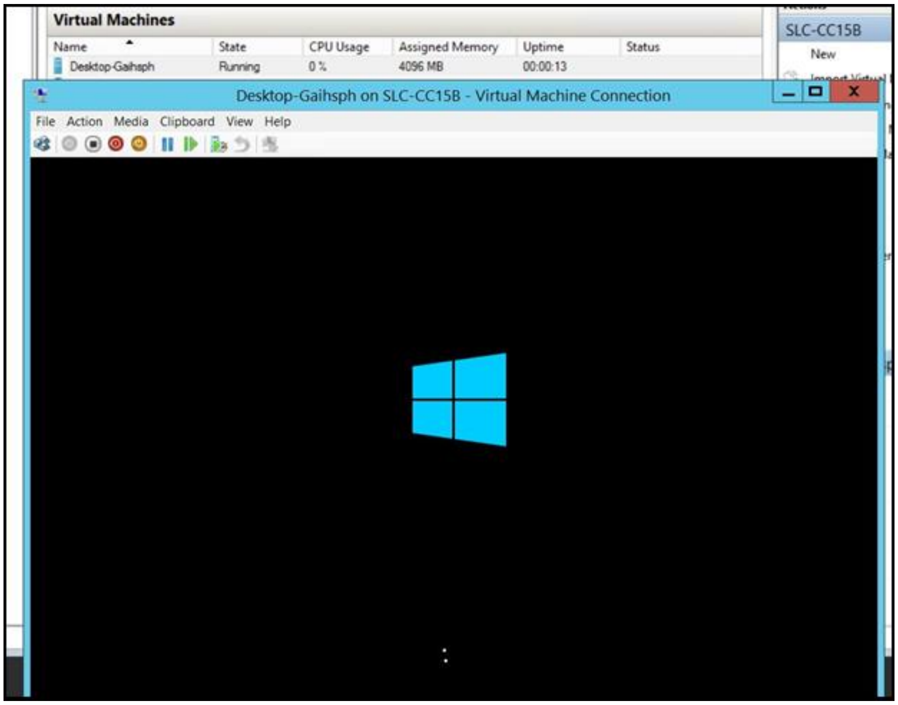
Name	State	CPU Usage	Assigned Memory	Uptime	St
Desktop-Gaihsph	Off				

Desktop-Gaihsph on SLC-CC15B - Virtual Machine Conn...

The virtual machine 'Desktop-Gaihsph' is turned off

To start the virtual machine, select 'Start' from the Action menu

Status: Off



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status
Desktop-Gaihsph	Running	0 %	4096 MB	00:00:13	

Desktop-Gaihsph on SLC-CC15B - Virtual Machine Connection

Cleaning Up

- When you have finished with the eFolder Continuity Cloud, the best practice is to delete any of your data off of the X: drive (using Windows Explorer).
- eFolder will reinitialize the underlying RAID volumes when the node is reprovisioned, zeroing out all data on the volume.
- For especially sensitive data, you may want to securely erase all of the free space on the drive in a way that adheres to DoD standards.
    - To do this, clear the recycle bin; then, open a command prompt and run the command "sdelete -c X:"—this will more securely erase any files you have deleted.
    - Running sdelete may take 24-48 hours, so you should only run it if required by your security procedures.
- To ensure that you are no longer billed for the eFolder Continuity Cloud service, you submit a ticket indicating that you are finished with the node(s) that have been provisioned for you and please notify eFolder that you have done so.
- Once you have submitted this ticket to eFolder indicating that you are finished with the node, you will no longer have access to the machine. eFolder will wipe and reimage the machine from bare metal, so please make sure you have any data that you need before submitting a ticket indicating that you are finished with the nodes.