Veeam Cloud Connect for the Enterprise using StoneFly Cloud Drive with Scale Out NAS Storage on Microsoft Azure

September 2016
Introduction

NOTE: This document is for IT administrators who are responsible for setting up and managing data Availability infrastructures that include Veeam® Backup & Replication™, with Veeam Cloud Connect for the Enterprise, and who intend to leverage StoneFly Scale Out NAS Cloud Storage hosted on Microsoft Azure. It is assumed that the reader is generally familiar with Veeam Backup & Replication and Microsoft Azure. For your convenience, we have provided both the StoneFly deployment guide, – and the Veeam Cloud Connect for the Enterprise deployment guides in their entirety.

The challenge

Veeam Cloud Connect for the Enterprise offers a turnkey solution for enterprises to connect their on-premises, Veeam Backup & Replication archives to Microsoft Azure. The Certified Veeam VM in the Microsoft Azure Marketplace is limited in its storage capacity, which for many customers makes it necessary to implement additional Scale Out storage solutions.

The solution

Based on the many requests for additional storage space, methods, or other solutions to add flexibility to the storage options available to the enterprise customer in Microsoft Azure, Veeam has partnered with StoneFly to offer state-of-the-art storage options leveraging StoneFly’s Scale Out NAS Cloud Storage. By combining Veeam and StoneFly solutions, customers can bypass the capacity size constraints within Azure, quickly and easily add more capacity without sacrificing performance or throughput, and best of all, manage multiple Cloud Drive nodes with just a single interface.

Configuration steps

1. Install On-premises Veeam Infrastructure (Veeam Availability Suite™ or Veeam Backup & Replication Enterprise Plus edition)
   - Licensed through traditional Veeam Resellers

2. Provision in Microsoft Azure Marketplace — StoneFly Scale Out NAS Cloud Storage
   - Licensed within Microsoft Azure Marketplace
   - Azure VM (Minimum A3 license)

   - BYOL acquired through traditional licensing partner (or demo license)
   - Azure VM (Minimum A3 license)
   - Configure connection to StoneFly Scale Out NAS Cloud Storage
The entire configuration process can be completed in less than 60 minutes, assuming that the on-premises Veeam infrastructure is already in place. Detailed step-by-step configuration instructions for Veeam Cloud Connect for Enterprise and StoneFly Scale Out NAS Cloud Storage are listed here.

For additional information about Veeam Cloud Connect for Enterprise, see:

For additional information on StoneFly Scale Out NAS Cloud Storage, see:


This document contains

StoneFly Cloud Drive deployment guide ................................................................. 4
Deploying Veeam Cloud Connect for the Enterprise on Microsoft Azure user guide ...................... 24
StoneFly Cloud Drive deployment guide

StoneFly Scale Out NAS Cloud Storage hosted on Microsoft Azure

Copyright 2006 — 2016 StoneFly, Inc.

All rights are reserved. No part of this document may be photocopied or reproduced without the prior written consent of StoneFly.

The information contained in this document is subject to change without notice. StoneFly shall not be liable for errors contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.


Other brands and their products are trademarks or registered trademarks of their respective holders.
Contents

1. Overview ............................................................................................................. 6

2. Deploying a StoneFly Cloud Drive Virtual Machine ........................................... 6
   2.1. Select StoneFly Scale Out NAS VM in Azure Marketplace .............................. 6
   2.2. Start Create .................................................................................................. 6
   2.3. Create Basics ............................................................................................... 7
   2.4. Select Machine Size ..................................................................................... 7
   2.5. Settings ........................................................................................................ 9
   2.6. Summary ..................................................................................................... 9
   2.7. Purchase ...................................................................................................... 10

3. Configure StoneFly Cloud Drive VM settings in the Microsoft Azure Portal ........ 10
   3.1. Public DNS name ........................................................................................ 10
   3.2. Add Data Disks ............................................................................................ 11

4. Configure StoneFly Scale Out NAS Enterprise Cloud Storage ............................. 12
   4.1. Initial login .................................................................................................. 12
   4.2. User Access for Cloud Drive management interface ....................................... 13
       4.2.1. Defaults ............................................................................................... 13
       4.2.2. Modify Cloud Drive Management Interface user access .......................... 13
       4.2.3. Add Management Interface users ......................................................... 13
   4.3. NTP ............................................................................................................ 14
   4.4. Data Port IP settings .................................................................................... 14
   4.5. Discover and use resources ......................................................................... 15
   4.6. Create NAS Segments ............................................................................... 16
   4.7. Join a Scale Out NAS Configuration ............................................................ 17
   4.8. NAS volumes ............................................................................................... 19
       4.8.1. Allocate NAS volumes .......................................................................... 19
       4.8.2. Expand NAS volumes ......................................................................... 20
       4.8.3. NAS Volumes Summary ..................................................................... 21
   4.9. CIFS Users ................................................................................................. 22
       4.9.2. CIFS User Access ............................................................................... 22

5. Volume Access .................................................................................................... 23

About StoneFly .......................................................................................................... 23
1. Overview

1.1. Purpose

The purpose of this document is to guide the user through the steps required to deploy a StoneFly Scale Out NAS Enterprise Cloud Drive virtual machine in the Microsoft Azure Cloud. This guide should be used in conjunction with the StoneFly Cloud Drive User’s Guide which can be viewed or downloaded here: http://www.stonefly.com/PDF/StoneFlyCloudDrive_ScaleOutNAS_UsersGuide.pdf

2. Deploying a StoneFly Cloud Drive Virtual Machine

2.1. Select StoneFly Scale Out NAS VM in Azure Marketplace


Type stonefly in the search box and hit Enter. Select StoneFly Scale Out NAS Cloud Storage.

2.2. Start Create

Review the product description then click on the Create button at the bottom. The Create virtual machine and Basics window panes will open.
2.3. Create Basics

Fill in the required fields.

Do not use more than 12 characters for the VM Name field or the StoneFly Cloud Drive will not be able to join the Scale Out. The VM Name cannot be changed later.

The User name and Password settings do not matter as this account is disabled after the StoneFly Cloud Drive Virtual Machine is created.

The StoneFly Cloud Drive Virtual Machine is managed using a browser session to a URL with the format of https://<public-dns-name>.

If you have other Azure Cloud-hosted virtual machines or StoneFly Cloud Drives in Azure that you expect to interoperate with, it is recommended that they share the same Subscription, Resource group and Location.

Click on the OK button at the bottom of page when ready. The Choose a size window will open.

2.4. Select Machine Size

The common recommended sizes will be shown on the Choose a size screen. Other sizes are available by clicking View all.

The machine size selected must be A3 or higher (4 Cores + 7 GB Memory). The number of data disks will depend on your total space requirements.
Each Azure data disk has a maximum size of 1023 GB. An A3 Standard VM supports up to 8 Azure data disks for a maximum of 8 TB per machine. An A4 Standard VM supports up to 16 Azure data disks for a maximum of 16 TB per machine. The machine size can be changed later if needed.

Select the desired machine size, then click the **Select** button at the bottom of page. The **Settings** page will open.
2.5. Settings

On the Settings pane, use the defaults or make changes as necessary. If there are other virtual machines that are expected to interoperate with this StoneFly Cloud Drive, then it is recommended that they share the same Virtual Network.

Click on the OK button at the bottom of the page when finished. The Summary window will open.

2.6. Summary

On the Summary page, check all of the settings listed and correct them if necessary.

Click the OK button at the bottom of the page once you have determined that all settings are correct. The Purchase page will open.
2.7. Purchase

Read the Offer details, and then click on the Purchase button at the bottom of the page. Once the Purchase button is clicked, the Create page will open. If more StoneFly Cloud Drive Virtual Machines will be created at this time, then continue with creating using the steps in this section. If this is the only StoneFly Cloud Drive Virtual Machine to be created, then close the window and click on the Virtual machines icon on the left side of the screen.

The new StoneFly Cloud Drive Virtual Machine will be listed with a status of Creating. Click on the Refresh icon if it does not already appear on the list. After several minutes, the status will change to Running. Continue on to Chapter 3 to configure the new StoneFly Scale Out NAS Enterprise Cloud Drive Virtual Machine in the Microsoft Azure Cloud.

3. Configure StoneFly Cloud Drive VM settings in the Microsoft Azure Portal

3.1. Public DNS name

Click on the new StoneFly Cloud Drive Virtual Machine in Azure. The Virtual machine pane will open showing the Essentials section. Click on the hyperlink for the Public IP address/DNS name label field.

The Public IP address and Settings pane will open. Click on Configuration in the Settings pane. The Configuration pane will open.
Fill in the **DNS name label** in the **Configuration** pane and then click on **Save**. To simplify management, we recommend that the DNS name label matches the name you assigned to the VM in Section 2.3 and that it is no longer than 12 characters.

The new StoneFly Scale Out NAS Enterprise Cloud Drive Virtual Machine in the Microsoft Azure Cloud can now be accessed using the equivalent to this link, *but don’t go there just yet — we still need to attach disks. Proceed to the next step: https://DNSNameLabel.AzureDataCenterName.cloudapp.azure.com*

### 3.2. Add Data Disks

Scroll left to return to the **Virtual machine** and click on **All settings** in the **Essentials** section. The **Settings** pane will open.

Click on **Disks** in the **Settings** pane and the **Disks** pane will open.

Click on **Attach new** in the **Disks** pane and the **Attach new disk** pane will open.

Select **Read/Write** for **Host caching** in the **Attach new disk** pane. Edit other fields as necessary, then click on the **OK** button at the bottom of the pane.

Repeat adding additional disks as needed (up to 8/16/32/64 disks as permitted by the Azure machine size you purchased). Make sure to wait until each disk is successfully attached before attempting to add the next disk.

Repeat these steps as needed for each of the StoneFly Cloud Drive Virtual Machines you purchased.
4. Configure StoneFly Scale Out NAS Enterprise Cloud Storage

4.1. Initial login

We are now ready to login to the StoneFly Scale Out NAS Cloud Drive. You can easily find your custom URL for your StoneFly Cloud Drive VM by returning to the Essentials pane in Azure and clicking on the hyperlink for the Public IP address/DNS name label field to reopen the Public IP address pane. Copy the DNS name field that appears in that Public IP address pane.

Open a web browser, enter https:// and paste the DNS name we just copied to the clipboard in Azure and hit Enter. Your link should appear in the following format:

https://DNSNameLabel.AzureDataCenterName.cloudapp.azure.com

Enter the User ID and Password using the default case-sensitive credentials as follows, and then click the Enter button:

User ID: stonefly
Password: stonefly

Once logged in, you will be taken to the StoneFly Cloud Drive home page.
4.2. User Access for Cloud Drive management interface

4.2.1. Defaults

Navigate to the Users → Summary page using the menu bar. The default users will be displayed. There are two types of users: Observer and Administrative. The defaults are demo, which is an Observer account, and stonefly which is an Administrative account. Observer users can only view information. Administrative users can modify all settings.

4.2.2 Modify Cloud Drive Management Interface user access

Navigate to the Users → Detail page using the menu bar. Select the user you wish to modify from the Select User drop down list. Enter a new password in the Password and Confirm Password fields, and then click the Submit button. Passwords are case-sensitive, must be at least six characters and include at least one non-alphabetic character.

It is highly recommended to change the passwords for both default users during this initial login.

4.2.3 Add Management Interface users

Navigate to the Users → Add User page using the menu bar. This page is only used for adding users to manage the StoneFly Cloud Drive via the GUI. Adding users for data access is described in Section 4.9. Enter a user name in the Log In field.

Select Administrative (All) or Observer depending on the level of access you wish for the new user to receive for the Administration Level.
An Observer can only display information on the StoneFly Cloud Drive management interface, but cannot change any settings including their own password.

An Administrative users can make any and all changes on the StoneFly Cloud Drive management interface, including passwords for other users.

Create a password and enter it in both the Password and Confirm Password fields.

Click on the Submit button to finish creating the new user’s login.

4.3. NTP

Navigate to the System → Admin → General page using the menu bar.

NTP (Network Time Protocol) is required for StoneFly Cloud Drives with NAS volumes. The Primary NTP Server field is mandatory while the Secondary NTP Server field is optional. A list of public NTP servers can be found here: http://www.pool.ntp.org

If this Cloud Drive is to join a Scale Out NAS configuration, then the same NTP server(s) should be used for all systems in the configuration. Select the Use NTP checkbox and click the Submit button.

4.4. Data Port IP settings

Navigate to the System → Network → Local iSCSI Data Port page using the menu bar. Under Port Forwarding Addresses, enter all three fields as follows:

- Private Internal IP Address: 255.255.255.255
- Public External IP Address: Copy and paste this field from the address bar of your browser. You just need the section after https:// up through the .com, eg. DNSNameLabel.AzureDataCenterName.cloudapp.azure.com
- Public External TCP Port Number: 3260

Click the Submit button to complete the configuration.
4.5. Discover and use resources

Navigate to the Resources → Summary page using the menu bar.

Resources are the Azure disks that have been added to the StoneFly Cloud Drive. Each Azure disk will appear as a separate 1023 GB resource. We will be able to combine these resources in the upcoming steps.

On the initial login, no resources will be displayed until they have been discovered. A discovery will need to be performed any time new resources are added to the StoneFly Cloud Drive.

Click the Discover button and then the OK button on the dialog box to discover the available resources.

The discovered resources should now appear in the Resource Summary section at the bottom of the page.

The Use Type radio button must be set to Managed for each resource before that resource can be used to create volumes.

Click the Submit button to save the changes.
4.6 Create NAS Segments

Navigate to the NAS → Segments → Segment Create page using the menu bar.

A default NAS Segment Name will be displayed. The default name can be used or the name can be edited as desired.

The Notes field can be edited to include the user’s description for this segment.

Enter the Desired NAS Segment Size (GB). This number range from as low as 1, all the way up to the maximum number shown in the Available Space (GB) field.

Note: It is during this step that you will be able to combine the storage capacities of two or more Azure disks into a single usable unit (up to a maximum of 8 with A3 machines, a maximum of 16 with A4 machines, and 32 or 64 with some of the higher-end machines). If you plan to use the StoneFly Cloud Drive with large files greater than 1 TB in size, then please make sure to create a segment that is large enough to contain those large files. The segment size must be greater than the individual file size.

Note: If this segment will be used to expand an existing NAS volume, then it is recommended that the entered segment size match the same sizes of the other segments, which were used for the volume.

Note: No fields can be changed once the segment is created.

Click the Submit button, and then the OK button on the following two dialog boxes to finish configuring the segment. It will take a few minutes for the system to format the segment for use.
It is recommended to reboot the StoneFly Cloud Drive once the first NAS segment has been created. The reboot is only performed the very first time a NAS segment is created. Additional segments do not require a reboot.

To perform the reboot, navigate to the System → Admin → General page and click the Reboot button and then OK on the dialog box. The StoneFly Cloud Drive should be ready within 5 minutes following the reboot. This initial reboot ensures that all settings are updated and ready. Although the login screen reappears immediately in the browser window, you will not be able to login until the reboot is complete.

Click on the orange Alert at the top of the screen. Click the Acknowledgement checkbox and click the Submit button. The system status should return to Good.

### 4.7. Join a Scale Out NAS Configuration

By creating a Scale Out NAS configuration you will be able to join together two or more StoneFly Cloud Drives and pool together the 16 TB/32 TB/64 TB of storage resources that each StoneFly Cloud Drive provides.

**Note:** Before continuing, please make sure that you have performed all of the steps detailed up to this point of this Deployment Guide on every StoneFly Cloud Drive node that will be in the Scale Out. If you will only have one node for your initial configuration, then you can skip ahead to section 4.8.

If this is the first node of a Scale Out NAS configuration, then no action is required. However, if this is node #2, #3, #4, etc. then a Join Scale Out Configuration is required.

Navigate to the System → Information page of the first node or a StoneFly Scale Out NAS Enterprise Cloud Drive that is already in the configuration. Copy the string that appears in the Hostname field.
Navigate to the NAS → Scale Out → Summary page of the second node (or third, or fourth, etc.) and paste the string you copied from the Hostname field of the first node into the Management IP Address field.

Click the Submit button and then the OK button on the dialog box to join.

The next dialog box will notify you whether or not the node was able to join the Scale Out and the reason why if the join was unsuccessful. If the join was unsuccessful, make the corrections noted and resubmit.

If the join was successful, navigate to the NAS → Scale Out → Summary page. A list of nodes that are now part of the Scale Out configuration will be displayed. Repeat this step for each of the Scale Out nodes.
4.8 NAS volumes

To create one large volume across all of the StoneFly Scale Out Cloud Drive nodes, we will first create a volume on the first node, and then expand that volume using segments on the other nodes in the Scale Out.

4.8.1 Allocate NAS volumes

Navigate to the NAS → Volumes → Create New Volume → Allocate page on the first node of the Scale Out (or the only node). Use this page to create a new NAS volume. A default NAS volume Name is entered and can be edited at this time.

*Note: This name cannot be the same as any existing NAS volume Name on any node within the Scale Out configuration.*

*Note: Once created the NAS volume Name cannot be changed.*

Enter a description in the Notes field to identify this volume.

Select CIFS, NFS, or both CIFS and NFS in the Export As field as desired.

Select the NAS segment you wish to use from the drop down list. The volume will automatically equal the size of the NAS segment that is used to create it.

*Note: If a NAS segment does not exist, then the page will be redirected to the NAS Segment Create page but then returned to the NAS volume Allocation page after the segment is created.*

When the form is completed, click on the Submit button to create the NAS volume.
4.8.2 Expand NAS volumes

If you only have one StoneFly Cloud Drive node, jump to section 4.9.

The following step should be performed on each additional StoneFly Cloud Drive node in the Scale Out to expand the NAS storage volume created on the first node. This step cannot be performed on the first node.

Navigate to the NAS → Volumes → Expand Volume page on the next node in the Scale Out. Use this page to expand the NAS volume created on the first node. An existing NAS volume can be expanded on any StoneFly Cloud Drive node in a Scale Out configuration with available resources available.

It is recommended that all new segments that will be used to expand the NAS volume are configured with sizes that match the existing segments.

Select the NAS volume to be expanded from the Select Volume drop down list then click on the Start button.

The page will refresh to display adding a segment.

Select the new NAS segment to use from the drop down list.

*Note: If a NAS segment does not exist, then the page will be redirected to the NAS Segment Create page but then returned to the Expanded Volume Allocation page after the segment is created.*

When the form is completed, click on the Submit button to expand the NAS Volume.
The page will redirect to the NAS → Volumes → Configure Volume page. Information about the volume will be displayed on this page. Use this page to monitor the progress for the rebalance operation that is performed any time a volume is expanded. The rebalance is performed to maintain an even distribution of data on segments allocated to the NAS volume.

Repeat this step on the next StoneFly Cloud Drive node in the Scale Out configuration to expand the volume across more nodes.

### 4.8.3 NAS Volumes Summary

Navigate to the NAS → Volumes → Summary page on any node. A list of existing volumes will be displayed with information about those volumes. The Size (GB) field should show the new expanded size of the volume across all of the Scale Out nodes.
4.9. **CIFS Users**

NAS volume CIFS user name and password authentication can operate in two modes. The default is the Workgroup mode where the Cloud Drive manages the CIFS user accounts and passwords.

The other CIFS authentication mode is the use of a centralized Windows Active Directory Server (ADS), also known as a Windows Domain Controller. Workgroup users may continue to be used even when the ADS authentication mode is configured.

In a Scale Out NAS configuration, the NAS Server CIFS User Authentication configuration is the same for all of the Scale Out nodes. Changes made to CIFS User Authentication are automatically applied to all Scale Out nodes and the status can be viewed from any node.

To learn about adding Active Directory users, visit section 2.5.22 in the StoneFly Cloud Drive User’s Guide. Adding CIFS Workgroup users is described below.

4.9.1 **Add CIFS User**

Navigate to the NAS → CIFS User → Add/Update User page on any node in the Scale Out. Use this page to add or update a CIFS user. Enter a CIFS User name, a CIFS Password and Confirm CIFS Password. Click the Submit button when all fields are completed. The page will refresh to the User Access page.

4.9.2 **CIFS User Access**

Navigate to the NAS → CIFS User → User Access page on any node in the Scale Out. Select a User and then a Volume from the drop down boxes.

Select the appropriate CIFS Access level (None, Read Only, Read/Write, Read/Write/Admin) for the user. Click the Submit button when complete.

User actions can be performed from any node within a Scale Out configuration and are propagated to all nodes.
5. **Volume Access**

To access a NAS volume from a host use the following format:

```
\DNSNameLabel.AzureDataCenterName.cloudapp.azure.com\NASVolumeName
```

The volume can be accessed by using the Public DNS Name of any node within the Scale Out configuration.

**About StoneFly**

StoneFly, Inc. is a pioneer in the creation, development and deployment of the iSCSI storage protocol. Beginning with its registration of the iSCSI.com Internet domain name in March 1996,

StoneFly has made iSCSI into a standard which is now used by IT professionals around the world.

StoneFly, headquartered in the Silicon Valley, was founded to deliver upon the vision of simple and affordable enterprise-class storage optimization and disaster recovery protection through iSCSI, Fibre Channel SAN and NAS solutions. Advanced storage offerings include Hyper-Converged Unified Storage & Server™ appliances and gateways, Scale Out NAS, Backup, Disaster Recovery, and Enterprise Cloud Storage solutions.

StoneFly is a subsidiary of Dynamic Network Factory, Inc. (DNF), a leading maker of high-performance storage systems. Other divisions include DNF Storage, DNF Security, DNF Defense, and DNF Consulting Services. StoneFly is a member of the Storage Networking Industry Association (SNIA), the founding member of the IP Storage Institute (IPSI), a VMware TAP Elite Partner, a VMware Professional Solution Provider Partner, and a certified Microsoft Azure Marketplace Partner.

To learn more, visit [http://www.StoneFly.com](http://www.StoneFly.com)
Deploying Veeam Cloud Connect for the Enterprise on Microsoft Azure User Guide
# Contents

About this guide ................................................................. 26
Intended audience ............................................................... 26
About Veeam Cloud Connect for the Enterprise ............................... 26
Pre-requisites ................................................................. 26
Azure virtual machine maximum configuration ................................. 26
How to deploy Veeam Cloud Connect for the Enterprise ................. 28
  Step #1: Select the VM image ........................................... 28
  Step #2: Create the Veeam Cloud Connect VM ......................... 29
How to use Veeam Cloud Connect for the Enterprise as a Simple Backup Repository and WAN accelerator ............ 33
  Step #1: Allowing firewall ports .......................................... 34
  Step #2: Adding Veeam Cloud Connect for the Enterprise as a simple backup repository in Veeam Backup & Replication ....................................................... 34
  Step #3: Add Veeam Cloud Connect for the Enterprise as a WAN accelerator in Veeam Backup & Replication .................. 40
  Step #4: Adding StoneFly Cloud Drive as a simple backup repository in Veeam Backup & Replication ................ 43
About Veeam Software ......................................................... 48
About this guide

This user guide provides information on how to deploy Veeam® Cloud Connect (VCC) on Microsoft Azure, using it as both a simple backup repository for off-site backups and as a WAN accelerator.

Intended audience:

This user guide is for anyone who wants to use Veeam Cloud Connect for Microsoft Azure.

About Veeam Cloud Connect for the Enterprise

Veeam Cloud Connect for the Enterprise (VCC-E) is an easy, efficient way to get backups off site to Azure. Microsoft Azure Marketplace customers can instantly provision cloud backup repositories and automatically move on premises backup archives to Azure. This powerful combination of Microsoft and Veeam provides enterprise customers with cost-effective Azure storage, Plus the granular recovery capabilities of Veeam.

Pre-requisites

Veeam Cloud Connect for the Enterprise is licensed as an annual subscription, per VM and is an add-on purchase to Veeam Availability Suite™ or Veeam Backup & Replication™. Version 8 Update 3 or higher is required for backup.

- It is intended for large deployments of Veeam Availability Suite or Veeam Backup & Replication with a minimum of 100 sockets.
- Customers who do not meet the minimum socket requirement are encouraged to use Veeam Cloud Connect through a Veeam Cloud & Service Provider partner

Utilization of the WAN accelerator requires Veeam Backup & Replication enterprise edition. Further, when using the WAN accelerator configuration, the firewall needs to be configured with additional firewall ports for communications between the VCC server and the Veeam Backup & Replication server.

Azure virtual machine maximum configuration

Microsoft offers Azure virtual machines (VMs) in two tiers (basic and standard) with an array of different sizes (compute, memory, storage and IOPS configurations). Select the right VM size that matches the workload requirements. The selected VM size also determines the price for the use of the VM. Storage cost is priced separately and depends on the space used in the Azure storage account.
## Basic tier VMs

<table>
<thead>
<tr>
<th>Size</th>
<th>CPU cores</th>
<th>Memory</th>
<th>Max disk sizes/Max number of disks (Max Size — 1023 GB)</th>
<th>Max IOPS (300/disk)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>1</td>
<td>768 MB</td>
<td>OS—1023 GB, Temp—20 GB / 1</td>
<td>300</td>
</tr>
<tr>
<td>A1</td>
<td>1</td>
<td>1.75 GB</td>
<td>OS—1023 GB, Temp—40 GB / 2</td>
<td>600</td>
</tr>
<tr>
<td>A2</td>
<td>2</td>
<td>3.5 GB</td>
<td>OS—1023 GB, Temp—60 GB / 4</td>
<td>1200</td>
</tr>
<tr>
<td>A3</td>
<td>4</td>
<td>7 GB</td>
<td>OS—1023 GB, Temp—120 GB / 8</td>
<td>2400</td>
</tr>
<tr>
<td>A4</td>
<td>8</td>
<td>14 GB</td>
<td>OS—1023 GB, Temp—240 GB / 16</td>
<td></td>
</tr>
</tbody>
</table>

## Standard tier VMs

### Standard tier VMs — A Series:

<table>
<thead>
<tr>
<th>Size</th>
<th>CPU cores</th>
<th>Memory</th>
<th>Max disk sizes/Max number of disks (Max Size — 1023 GB)</th>
<th>Max IOPS (500/disk)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>1</td>
<td>768 MB</td>
<td>OS—1023 GB, Temp—20 GB / 1</td>
<td>500</td>
</tr>
<tr>
<td>A1</td>
<td>1</td>
<td>1.75 GB</td>
<td>OS—1023 GB, Temp—70 GB / 2</td>
<td>1000</td>
</tr>
<tr>
<td>A2</td>
<td>2</td>
<td>3.5 GB</td>
<td>OS—1023 GB, Temp—135 GB / 4</td>
<td>2000</td>
</tr>
<tr>
<td>A3</td>
<td>4</td>
<td>7 GB</td>
<td>OS—1023 GB, Temp—285 GB / 8</td>
<td>4000</td>
</tr>
<tr>
<td>A4</td>
<td>8</td>
<td>14 GB</td>
<td>OS—1023 GB, Temp—605 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>A5</td>
<td>2</td>
<td>14 GB</td>
<td>OS—1023 GB, Temp—135 GB / 4</td>
<td>2000</td>
</tr>
<tr>
<td>A6</td>
<td>4</td>
<td>28 GB</td>
<td>OS—1023 GB, Temp—285 GB / 16</td>
<td>4000</td>
</tr>
<tr>
<td>A7</td>
<td>8</td>
<td>56 GB</td>
<td>OS—1023 GB, Temp—605 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>A8</td>
<td>8</td>
<td>56 GB</td>
<td>OS—1023 GB, Temp—382 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>A9</td>
<td>16</td>
<td>112 GB</td>
<td>OS—1023 GB, Temp—382 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>A10</td>
<td>8</td>
<td>56 GB</td>
<td>OS—1023 GB, Temp—382 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>A11</td>
<td>16</td>
<td>112 GB</td>
<td>OS—1023 GB, Temp—382 GB / 16</td>
<td>8000</td>
</tr>
</tbody>
</table>

### Standard tier VMs — D Series:

<table>
<thead>
<tr>
<th>Size</th>
<th>CPU cores</th>
<th>Memory</th>
<th>Max disk sizes/Max number of disks (Max Size — 1023 GB)</th>
<th>Max IOPS (500/disk)</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>1</td>
<td>3.5 GB</td>
<td>OS—1023 GB, Temp—50 GB / 2</td>
<td>1000</td>
</tr>
<tr>
<td>D2</td>
<td>2</td>
<td>7 GB</td>
<td>OS—1023 GB, Temp—100 GB / 4</td>
<td>2000</td>
</tr>
<tr>
<td>D3</td>
<td>4</td>
<td>14 GB</td>
<td>OS—1023 GB, Temp—200 GB / 8</td>
<td>4000</td>
</tr>
<tr>
<td>D4</td>
<td>8</td>
<td>28 GB</td>
<td>OS—1023 GB, Temp—400 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>D11</td>
<td>2</td>
<td>14 GB</td>
<td>OS—1023 GB, Temp—100 GB / 4</td>
<td>2000</td>
</tr>
<tr>
<td>D12</td>
<td>4</td>
<td>28 GB</td>
<td>OS—1023 GB, Temp—200 GB / 8</td>
<td>4000</td>
</tr>
<tr>
<td>D13</td>
<td>8</td>
<td>56 GB</td>
<td>OS—1023 GB, Temp—400 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>D14</td>
<td>16</td>
<td>112 GB</td>
<td>OS—1023 GB, Temp—800 GB / 32</td>
<td>16000</td>
</tr>
</tbody>
</table>
Standard tier VMs — DS Series:

<table>
<thead>
<tr>
<th>Size</th>
<th>CPU cores</th>
<th>Memory</th>
<th>Max disk sizes/Max number of disks (Max Size — 1023 GB)</th>
<th>Cache</th>
<th>Max IOPS (500/disk)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS1</td>
<td>1</td>
<td>3.5 GB</td>
<td>OS—1023 GB, Local—7 GB / 2</td>
<td>43 GB</td>
<td>3200</td>
</tr>
<tr>
<td>DS2</td>
<td>2</td>
<td>7 GB</td>
<td>OS—1023 GB, Local—14 GB / 4</td>
<td>86 GB</td>
<td>6400</td>
</tr>
<tr>
<td>DS3</td>
<td>4</td>
<td>14 GB</td>
<td>OS—1023 GB, Local—28 GB / 8</td>
<td>172 GB</td>
<td>12800</td>
</tr>
<tr>
<td>DS4</td>
<td>8</td>
<td>28 GB</td>
<td>OS—1023 GB, Local—56 GB / 16</td>
<td>344 GB</td>
<td>25600</td>
</tr>
<tr>
<td>DS11</td>
<td>2</td>
<td>14 GB</td>
<td>OS—1023 GB, Local—28 GB / 4</td>
<td>72 GB</td>
<td>6400</td>
</tr>
<tr>
<td>DS12</td>
<td>4</td>
<td>28 GB</td>
<td>OS—1023 GB, Local—56 GB / 8</td>
<td>144 GB</td>
<td>12800</td>
</tr>
<tr>
<td>DS13</td>
<td>8</td>
<td>56 GB</td>
<td>OS—1023 GB, Local—112 GB / 16</td>
<td>288 GB</td>
<td>25600</td>
</tr>
<tr>
<td>DS14</td>
<td>16</td>
<td>112 GB</td>
<td>OS—1023 GB, Local—224 GB / 32</td>
<td>576 GB</td>
<td>50000</td>
</tr>
</tbody>
</table>

Standard tier VMs — G Series:

<table>
<thead>
<tr>
<th>Size</th>
<th>CPU cores</th>
<th>Memory</th>
<th>Max disk sizes/Max number of disks (Max Size — 1023 GB)</th>
<th>Max IOPS (500/disk)</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1</td>
<td>2</td>
<td>28 GB</td>
<td>OS—1023 GB, Local—384 GB / 4</td>
<td>2000</td>
</tr>
<tr>
<td>G2</td>
<td>4</td>
<td>56 GB</td>
<td>OS—1023 GB, Local—768 GB / 8</td>
<td>4000</td>
</tr>
<tr>
<td>G3</td>
<td>8</td>
<td>112 GB</td>
<td>OS—1023 GB, Local—1536 GB / 16</td>
<td>8000</td>
</tr>
<tr>
<td>G4</td>
<td>16</td>
<td>224 GB</td>
<td>OS—1023 GB, Local—3072 GB / 32</td>
<td>16000</td>
</tr>
<tr>
<td>G5</td>
<td>32</td>
<td>448 GB</td>
<td>OS—1023 GB, Local—6144 GB / 64</td>
<td>32000</td>
</tr>
</tbody>
</table>

How to deploy Veeam Cloud Connect for the Enterprise

Step #1: Select the VM image


2. On the Hub Menu, click New. In a search bar type Veeam, select Veeam Cloud Connect for the Enterprise.
3. On the **Veeam Cloud Connect for the Enterprise** page, click **Create**.

**Information**

The deployment mode is gray. This is because Microsoft Azure has two deployment models (Classic and Resource Manager), and the Veeam Cloud Connect VM is only available in the Resource Manager model. To know more about the deployment models visit: https://azure.microsoft.com/en-gb/documentation/articles/resource-manager-deployment-model/

**Step #2: Create the Veeam Cloud Connect VM**

Select the image using Azure default settings for most of the configuration to create the VM quickly.

1. On the **Create VM** blade, click **Basics**.
2. Enter a name for the VM. The name cannot contain special characters.
3. Enter the administrative user name and a strong password. The password must be 8 - 123 characters long, and have at least three of the following: One lower case character, one upper case character, one number, and one special character. The user name and password will be needed to log on to the VM.
4. If there is more than one subscription, specify which one is for the new VM, as well as a new or existing resource group and an Azure data center location.
Information

Azure is generally available in 22 regions around the world, and there are plans for an additional five regions. Geographic expansion is a priority for Azure, because it enables customers to achieve higher performance while supporting their requirements and preferences regarding data location.

The location (i.e. nearest Azure data center) field is very important for the VM performance. To find the best location, please go to [http://azurespeedtest.azurewebsites.net/](http://azurespeedtest.azurewebsites.net/). West Europe is the nearest Azure data center in this example.

5. Click **Size** and select an appropriate VM size. Each size specifies the number of compute cores, memory and other features, such as support for Premium Storage, which will affect the price. Azure recommends certain sizes automatically, depending on the image chosen.
6. Click **Settings** to see storage and networking settings for the new VM. Generally, accepting the default settings is appropriate for a first VM.

![Virtual Machine Settings](image)

- **Storage**
  - Disk type: Standard
  - Premium (SSD)

- **Network**
  - Virtual network: (new) test
  - Subnet: (default) 10.9.0.0/24
  - Public IP address: (new) test
  - Network security group: (new) test

7. Click **Summary** to review the configuration choices. To review or update the settings, click **Create**.

![Virtual Machine Summary](image)

8. Track progress under **Virtual Machines** in the hub menu while Azure creates the VM.
9. Once deployment is done, click the VM on the dashboard, or click on Virtual Machines and select it from the list.

10. Click Connect on the VM blade.
How to use Veeam Cloud Connect for the Enterprise as a Simple Backup Repository and WAN accelerator

The following steps prepare the Veeam Cloud Connect VM as a simple backup repository and WAN accelerator:

1. Allow firewall ports for communication between Veeam Cloud Connect and the Veeam Backup & Replication server
2. Add Veeam Cloud Connect for the Enterprise as a Windows server
3. Configure the Veeam Cloud Connect windows server as a simple backup repository
4. Configure the Veeam Cloud Connect windows server as a WAN accelerator

**Network configuration:**

To use Veeam Cloud Connect as a simple backup repository and a WAN accelerator, the following ports need to be allowed in the network security group:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>135</td>
<td>TCP, UDP</td>
<td>Ports required for deploying Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>137</td>
<td>TCP, UDP</td>
<td>Ports required for deploying Veeam Backup &amp; Replication components.</td>
</tr>
<tr>
<td>138</td>
<td>TCP, UDP</td>
<td>Ports required for deploying Veeam Backup &amp; Replication components.</td>
</tr>
<tr>
<td>139</td>
<td>TCP, UDP</td>
<td>Ports required for deploying Veeam Backup &amp; Replication components.</td>
</tr>
<tr>
<td>445</td>
<td>TCP, UDP</td>
<td>Ports required for deploying Veeam Backup &amp; Replication components.</td>
</tr>
<tr>
<td>2500-5000</td>
<td>TCP, UDP</td>
<td>Default range of ports used as transmission channels for jobs. One port from this range is assigned for every TCP connection that a job uses.</td>
</tr>
<tr>
<td>6160</td>
<td>TCP</td>
<td>Default port used by the Veeam installer service.</td>
</tr>
<tr>
<td>6162</td>
<td>TCP</td>
<td>Default port used by the Veeam data mover service.</td>
</tr>
<tr>
<td>6163</td>
<td>TCP</td>
<td>Default port used to communicate with Veeam Hyper-V.</td>
</tr>
<tr>
<td>6164</td>
<td>TCP</td>
<td>Controlling port for RPC calls.</td>
</tr>
<tr>
<td>6165</td>
<td>TCP</td>
<td>Default port used for data transfer between WAN accelerators. Ensure this port is open in firewall between sites where WAN accelerators are deployed.</td>
</tr>
</tbody>
</table>
Step #1: Allowing firewall ports

1. Go to Virtual Machine > Click Settings > Setting blade > Network Interface > Select Network Interface > Network Security Group > Inbound security rule.

2. Add Inbound security rule and allow firewall ports mentioned above.

Information:

By default, all inbound and outbound ports are blocked in Azure. Once the network security group is configured, it can be used for other VMs.

Step #2: Adding Veeam Cloud Connect for the Enterprise as a simple backup repository in Veeam Backup & Replication

Open the Veeam Backup & Replication Console, then click the Backup Infrastructure, then right-click Backup Repositories, and then click Add Repository on the ribbon.
Specify the Backup Repository Name and Description

At the Name step of the wizard, specify a name and description for the backup repository.

1. In the Name field, specify a name for the backup repository.

2. In the Description field, provide a description for future reference. The default description contains information about the user who added the backup repository, and the date and time when the backup repository was added.

Choose type of Backup Repository

At the Type step of the wizard, select the type of the backup repository.

- Microsoft Windows server with local or directly attached storage.

When adding a Microsoft Windows server as a backup repository, Veeam Backup & Replication deploys the target data mover service on the Microsoft Windows server. The data mover service is responsible for transporting VM data over the network.
Specify the server

Click Add New to open the New Windows Server or wizard, and enter the VCC-E IP Address or DNS Name:

Credentials:

At the Credentials step of the wizard, specify credentials for the Microsoft Windows server.

1. From the Credentials list, select credentials for the account that has administrator privileges on the Microsoft Windows server. If credentials are not already set up, click the Manage accounts link or click Add on the right to add the credentials. For more information, see Managing Credentials.

Veeam Backup & Replication will use the provided credentials to deploy the following components on the added server:

- Veeam installer service
- Veeam data mover service (Transport)
Review

At the **Review** step of the wizard, review which Veeam Backup & Replication components are already installed on the server, and which components will be installed.

1. Review the components.
2. Click **Next** to add the Microsoft Windows server to the backup infrastructure.

Apply

At the **Apply** step of the wizard, complete the procedure of adding the Microsoft Windows server.

1. Review details of the Microsoft Windows server.
2. Click **Next**, then click **Finish** to exit the wizard.
Specify disk for backup

Click **Populate** to see a list of disk storages connected to the server, their capacity and free space, and then select the disk for backups.
Specify Mount Server Settings

At the mount server step of the wizard, select the mount server to be used for file-level and application items restore.

1. From the Mount Server list, select a server that you want to use as a mount server. The mount server is required for file-level and application items restore. During the restore process, Veeam Backup & Replication will mount the VM disks from the backup file residing on the backup repository to the mount server. As a result, VM data will not have to travel over the network, which will reduce the load on the network and speed up the restore process.

2. Uncheck vPower NFS Service, as it will not be used for the cloud repository.

Review Properties and Components

At the Review step of the wizard, review the details of the backup repository and specify importing settings.

Finish working with wizard

At the Apply step of the wizard, complete the procedure of backup repository configuration.
1. Wait for the backup repository to be to the backup infrastructure. The process may take several minutes.

2. Review details for the added backup repository.

3. Click **Finish** to exit the wizard.

Step #3: Add Veeam Cloud Connect for the Enterprise as a WAN accelerator in Veeam Backup & Replication:

**Configuring WAN accelerators**

Configure a pair of WAN accelerators in the backup infrastructure to optimize the VM traffic going over the WAN during remote jobs.

To launch the **New WAN Accelerator wizard**, do one of the following:

- Open the **Backup Infrastructure** view, in the inventory pane and select **WAN Accelerators**. Then, click **Add WAN Accelerator** on the ribbon.

- Open the **Backup Infrastructure** view, in the inventory pane then right-click **WAN Accelerators** and select **Add WAN Accelerator**.
Choose the Server

At the Server step of the wizard, select a VCC-E server to use as a WAN accelerator. Define the port and connection settings for this server.

1. From the Choose server list, select a VCC-E Server added to the backup infrastructure. If the server is not yet added to the backup infrastructure, click Add New to open the New Windows Server wizard. Provide a description for future reference in the Description field.

It is recommended to describe the added WAN accelerator as the source or target. When creating a remote job, this hint will be displayed in brackets next to the WAN accelerator name. This helps to choose the necessary WAN accelerator for use on the source or target side.

2. In the Traffic port field, specify the number of the port over which the WAN accelerators must communicate with each other. Port 6165 is used by default.

3. In the Streams field, specify the number of connections that must be used to transmit data between WAN accelerators. Five connections are used by default.

This setting applies only to the source WAN accelerator. The greater the number of streams, the more bandwidth resources Veeam Backup & Replication will use. A great number of streams engage more CPU and memory resources of the source WAN accelerator.

Define Cache Location and Size

At the Cache step of the wizard, define settings for the folder where service files and global cache data will be stored.

In the Folder field, specify a path to the folder in which service files (for source and target WAN accelerators) and global cache data (for target WAN accelerator) must be stored. When selecting a
folder on the target WAN accelerator, make sure that there is enough space for storing global cache data.

1. [For the target WAN accelerator] In the **Cache size field**, specify the size for the global cache. The global cache size is specified per source WAN accelerator. If one target WAN accelerator is used with several source WAN accelerators, the specified amount of space will be allocated to every source WAN accelerator and the size of the global cache will increase proportionally. For more information, see **WAN Accelerator Sizing**.

![New WAN Accelerator](image)

**Finish Working with the wizard**

At the **Apply** step of the wizard, complete the WAN accelerator configuration.

1. Wait for the WAN accelerator to be added to the backup infrastructure.
2. Click **Next**, then click **Finish** to exit the wizard.

![Apply](image)
Veeam Cloud Connect for the Enterprise as a simple backup repository and a WAN accelerator has been successfully deployed and configured.

**Step #4: Adding StoneFly Cloud Drive as a simple backup repository in Veeam Backup & Replication:**

To access a NAS volume from a host use `\<Public DNS Name>`\<NAS volume Name>`. Volume can be accessed by using the Public DNS Name of any node within the Scale Out configuration.

Open Veeam Backup & Replication software. Select Backup Repositories, then right-click in the NAME column to select Add Backup Repository. Click on Add Backup Repository and the New Backup Repository Name window will open.
Enter a name for the repository. **Click Next** when ready to continue. The **New Backup Repository Type** window will open.

Select **Shared folder** then click **Next** when you are ready to continue. The **New Backup Repository Share** window will open.
Enter in the Shared folder field the access point: `\<Public DNS Name>\<NAS volume Name>`. Click the This share requires access credentials check box then click Add. The Credentials window will open.

Enter Username and Password then click OK. The New Backup Repository Share window will open. The User Name and Password will be the CIFS User information setup on the StoneFly Cloud VM for the volume being added.

Supply Share information
Add the path to repository and then click **Next**.

Specify the Server, then click **Next**.

Review the settings, and then click **Finish**.
Confirm the completion of the **New Repository** creation wizard.
About Veeam Software

Veeam recognizes the new challenges companies across the globe face in enabling the Always-On Business™, a business that must operate 24.7.365. To address this, Veeam has pioneered a new market of Availability for the Always-On Enterprise™ by helping organizations meet recovery time and point objectives (RTPO™) of less than 15 minutes for all applications and data, through a fundamentally new kind of solution that delivers high-speed recovery, data loss avoidance, verified protection, leveraged data and complete visibility. Veeam Availability Suite, which includes Veeam Backup & Replication, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs.

Founded in 2006, Veeam currently has 41,000 ProPartners and more than 205,000 customers worldwide. Veeam’s global headquarters are located in Baar, Switzerland, and the company has offices throughout the world. To learn more, visit http://www.veeam.com.
ANNOUNCING

Disaster recovery orchestration for the Enterprise

NEW Veeam Availability Orchestrator

70% of Fortune 500 are Available.
24.7.365

AVAILABILITY for the Always-On Enterprise™