Buying and Configuring a StoneFly Cloud Drive from the Azure Marketplace

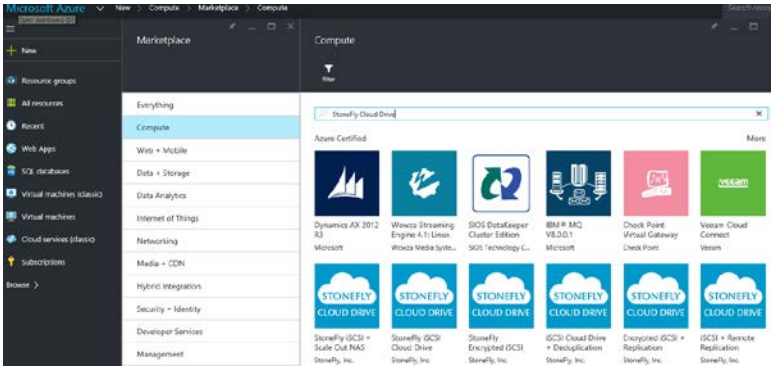
Last Updated: 2015/11/10

What follows is the procedure to purchase and properly configure a StoneFly Cloud Drive Virtual Machine from the Microsoft Azure Marketplace. StoneFly Cloud Drives implement StoneFly's Storage Concentrator™ Virtual Machine (SCVM™) technology to create a Virtual SAN appliance in the cloud.

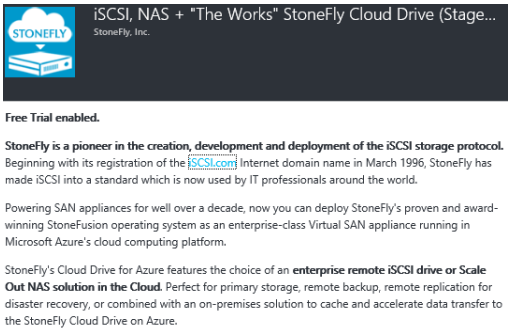
1. Sign in to the Microsoft Azure account portal at https://portal.azure.com. Select the "+ New" button at the top left of the page. Then select "Compute" -> "Marketplace".

   You can scroll through the Marketplace VM's, or search by name. Note that not all of the available "StoneFly Cloud Drive" VM's are shown when browsing in this manner; the rest can be found by clicking on the "More" link across from the "Linux based" label. Or type "stonefly" in the search box to bring up all of the StoneFly Cloud Drive VMs.

   Visit http://stonefly.com/products/cloud/azure/comparisonmatrix.asp to help make your decision on which StoneFly Cloud Drive is right for your business. Then carefully choose the desired StoneFly Cloud Drive product from the assortment listed. Please note that the features cannot easily be changed after purchase.



2. Select the “StoneFly Cloud Drive” VM with the features you desire by clicking on it.



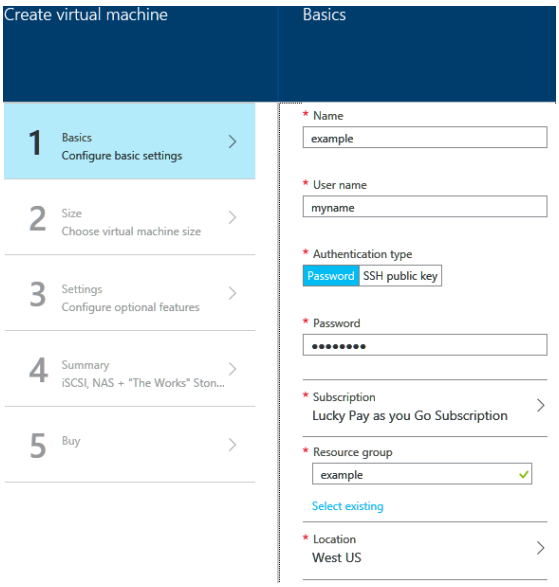
3. After reviewing the product description, click on the “Create” button at the bottom. The “Create virtual machine” and “Basics” windows will open up.

   Fill in and select the required fields. Note that the ‘Name’ field should be limited to a maximum length of 14 characters and it cannot be changed later.

   The “User name” and “Password” settings do not matter as this account is disabled after the StoneFly Cloud Drive VM is created. The StoneFly Cloud Drive VM is managed using a browser session to a URL created as follows: https://<public-dns-name>

   If you have other Azure cloud hosted VM’s or StoneFly Cloud Drive VM’s 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 the page when ready.

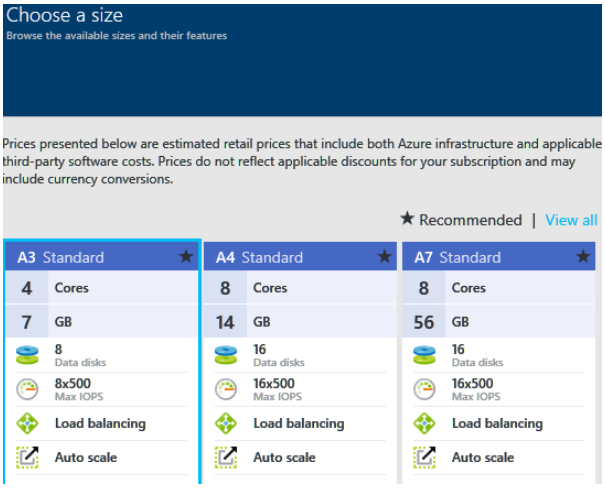


4. You will need to select the size of your StoneFly Cloud Drive VM. Although machine sizes are based on CPU core count, the amount of RAM and the maximum number of "Data disks" are more significant to the StoneFly Cloud Drive VM. Note that in Azure, each data disk can have a maximum size of about 1 TB, so a machine size of "A3 Standard" would be able to have a maximum of 8 TB of storage, and "A4 Standard" would be able to have a maximum of 16TB of storage.

   The size must be "A2" or higher in order for the StoneFly Cloud Drive VM to operate. If selecting a StoneFly Cloud Drive that supports NAS Volumes, the size must be "A3" or higher to afford more memory and CPUs. The "Standard" machine type should be used if NAS Volumes are planned; otherwise a "Basic" machine type can be used.

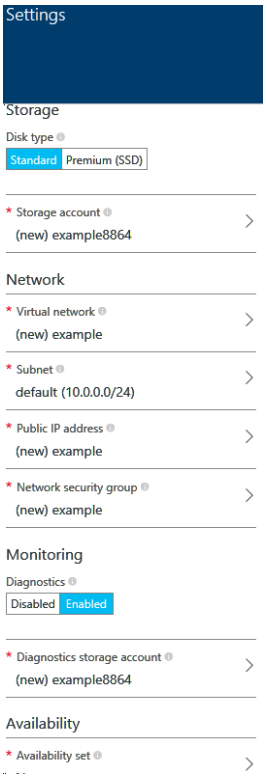
   It is sometimes possible to change the machine size of an existing StoneFly Cloud Drive VM, but only within the same family, e.g. "A# Standard", and only within the limits.

5. Only a few recommended machine sizes are shown, but many other sizes are available and can be seen by clicking on "View All". Select the desired machine size by clicking on it, and then click on the "Select" button at the bottom of the page.



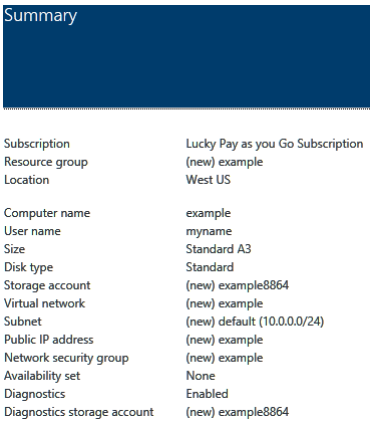
6. You will then be presented with the “Settings” window in order to configure optional features. Use the defaults, or make changes as necessary.

   Note that if you have other Microsoft Azure cloud hosted VM’s or StoneFly Cloud Drive VM’s that you expect to interoperate with; it is recommended that they share the same Virtual Network. Click on the “OK” button at the bottom of the page when done.

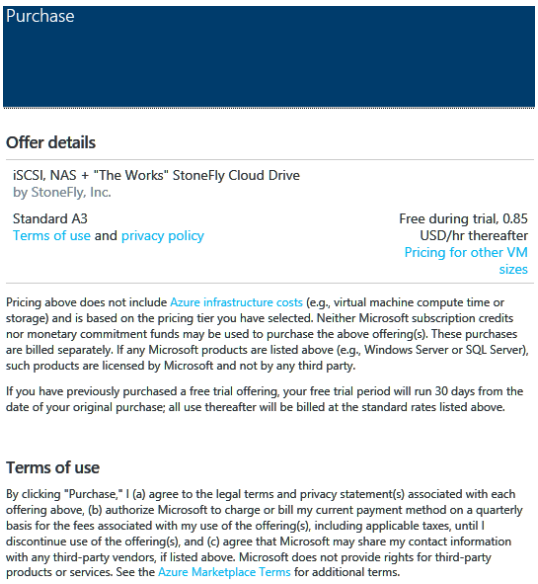


7. The “Summary” window should now appear. If everything is correct, click on “OK”. Otherwise click on the steps above to make any needed changes.

   Once all is correct, click on the “OK” button and proceed to the “Buy” step.



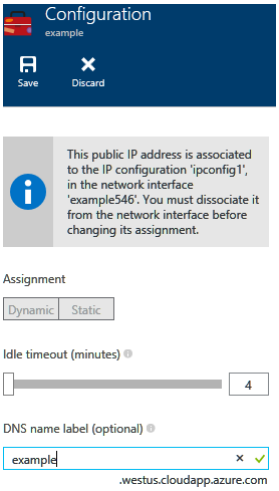
8. Read the “Offer details” on the “Purchase” window, and then click on the “Purchase” button at the bottom of the page.



9. Once the “Purchase” button is selected, the windows should close, and an icon for the new StoneFly Cloud Drive VM will appear with an animated status of “Deploying”. The deploying step can take a number of minutes. When it is ready for use, it will transition to the “Running” state.

   Once the StoneFly Cloud Drive VM is running, you will need to configure its Public DNS name. It is not recommended to use public or private IP addresses since these can change whenever the StoneFly Cloud Drive VM is restarted.

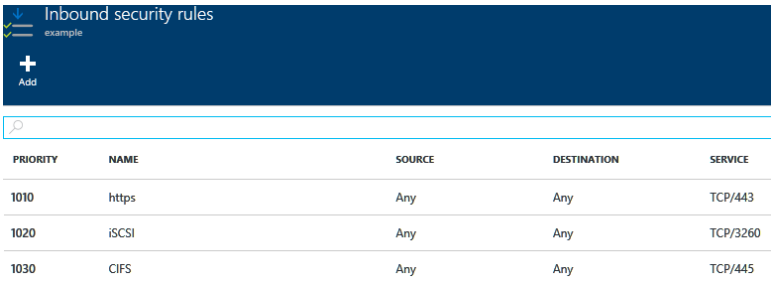
   To initially set the Public DNS name, open the VM “Essentials” window and then click on the “Public IP address” field which should open two other windows. In the “Settings” window, click on “Configuration”, enter the first term of the DNS name you want to use, and then click “Save” at the top of the window. The fully qualified name is determined by the location; in this case, the FQDN is “example.westus.cloudapp.azure.com”.



10. By default, the Azure VM Network Security Group (NSG) security rules make all network ports open and accessible to the world. Unless the entire Azure Service is being protected by a site-to-site Azure VPN, global access is probably not what is desired.

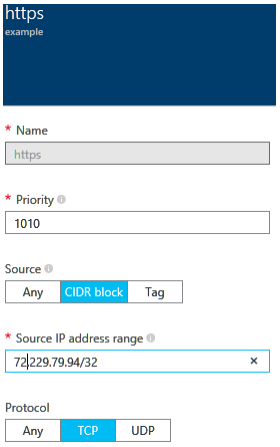
    Access can be restricted by configuring Azure Network Security Group rules to limit access. Before NSG rules can be configured, the client public IP addresses need to be known. These are the IP addresses seen on the public side of a firewall. Browsing to the site http://www.whatismypublicip.com though the firewall will provide this IP address.

    Given the client(s) public IP address, NSG inbound rules can be added for all of the protocol ports by using the Azure Portal GUI Network Security Group "Settings" page. Open the StoneFly Cloud Drive VM "Essentials" window and click on "All settings", then click on "Network interfaces" and select the interface which opens the "Network interface" window. Then click on the "Network security group" name which opens the "Settings" window. From there, click on the "Inbound security rules" to open that window. Each public service port is listed with its security settings:



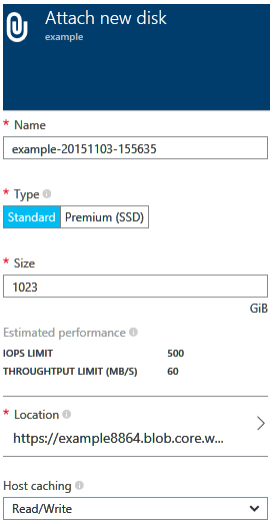
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE
1010	https	Any	Any	TCP/443
1020	iSCSI	Any	Any	TCP/3260
1030	CIFS	Any	Any	TCP/445

11. Click on each protocol listed, one at a time. Click on the "Source" "CIDR block" label, and configure the allowed IP address range in CIDR format, then click "OK" at the bottom of the window. Remember that this needs to be done for all protocols, and that a "Source" of "Any" means unrestricted access.



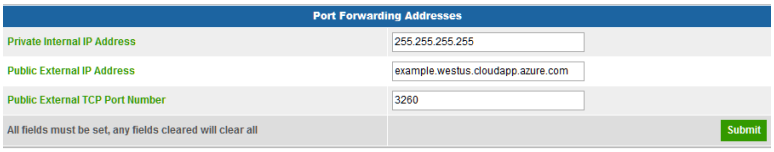
12. By default, the StoneFly Cloud Drive VM for Microsoft Azure configuration assumes that all network service ports may want to be used publically, outside of the Azure cloud. If this is not the case, then the default NSG rules for those not needed should be deleted.

13. One or more storage virtual disks need to be added to the StoneFly Cloud Drive VM. Each may be up to 1023 GB in size, and there can be a maximum of 16 virtual disks per StoneFly Cloud Drive VM, for the largest Azure machine sizes. Open the StoneFly Cloud Drive VM "Essentials" window, click on "All settings", click on "Disks", and then click on the "Add new" button at the top of the "Disks" window. Make sure to change "Host caching" to "Read/Write" on each.



14. Because the StoneFly Cloud Drive VM is located behind the Azure cloud firewall, iSCSI discovery from an external client will not work because the StoneFly Cloud Drive VM's internal IP addresses are not accessible from the outside of the Azure Virtual Network that the StoneFly Cloud Drive VM is located in. To provide external access, the StoneFly Cloud Drive VM must be configured with the public IP address and iSCSI TCP port used to reach it in its "Port Forwarding Addresses" settings.

    Connect to the StoneFly Cloud Drive VM GUI using the cloud service public DNS name, and the StoneFly Cloud Drive VM's TCP port number you specified for the HTTPS service (if not the default), and then log in. For example, https://example.westus.cloudapp.azure.com. Go to the StoneFly Cloud Drive VM's "System -> Network -> Local iSCSI Data Port Settings" GUI page, and configure the "Port Forwarding Addresses" section. Note that for the Azure network, the "Private Internal IP Address" should always be set to "255.255.255.255", and the "Public External TCP Port Number" should usually be set to the default, "3260".



15. It is recommended that when iSCSI is enabled for use through the public network interface, that iSCSI CHAP security be used as an additional measure to control access between host and the target. This is set up when the StoneFly Cloud Drive's target volume ACL's are set up.

16. The Azure specific StoneFly Cloud Drive VM configuration steps are now complete. Continue to configure and manage the StoneFly Cloud Drive VM for Microsoft Azure as you would any StoneFly SAN Appliance. Please refer to the StoneFly Storage Concentrator User's Guide and online help. The StoneFly User's Guide can be obtained by registering your StoneFly Cloud Drive subscription here: http://stonefly.com/products/cloud/azure/register.asp

17. Note that any client/host or other StoneFly Cloud Drive VM network reference to StoneFly Cloud Drive VM for Microsoft Azure **must** be in terms of the public DNS name, and not the currently assigned DHCP IP address. Every time that the StoneFly Cloud Drive VM is restarted, it will be assigned a new IP address.

18. When using the CIFS protocol (provided by select StoneFly Cloud Drives that include NAS volumes) from outside of the Azure cloud, it is common for ISP's to completely block the use of the CIFS network port 443 by default. Because Windows clients cannot easily be made to use an alternate port, it may be necessary to request the ISP to remove their blocking, assuming that an adequate firewall exists to protect your network.

19. It is **strongly** recommended that the default passwords for the default StoneFly Cloud Drive browser GUI accounts 'stonefly', and 'demo' be changed. This can be changed from the GUI Users page.

20. It is also strongly recommended that the "Console Password" be changed from the default. This can be done on the StoneFly Cloud Drive browser GUI System -> Admin -> General page, in the "Console Password" section.

21. These default accounts and passwords are published in user documentation, and are common to all installed StoneFly Cloud Drives. StoneFly Cloud Drive VM's for Microsoft Azure are potentially open to access by anyone in the world when neither an Azure VPN nor Network Security Group Source CDIR access rules are used.

End of document.

StoneFly, Inc.
Support@StoneFly.com
www.StoneFly.com
www.iSCSI.com
(510) 265-1616