Veritas NetBackup Support for Azure VMware Solutions

Purpose

This article provides information about support for Azure VMware Solutions (AVS) Private Cloud using NetBackup 8.2 and later versions. For details on all NetBackup features for VMware, see the *NetBackup version 8.3 VMware Administrator's Guide* and *Web UI VMware Administrator's Guide*.

Solution Architecture

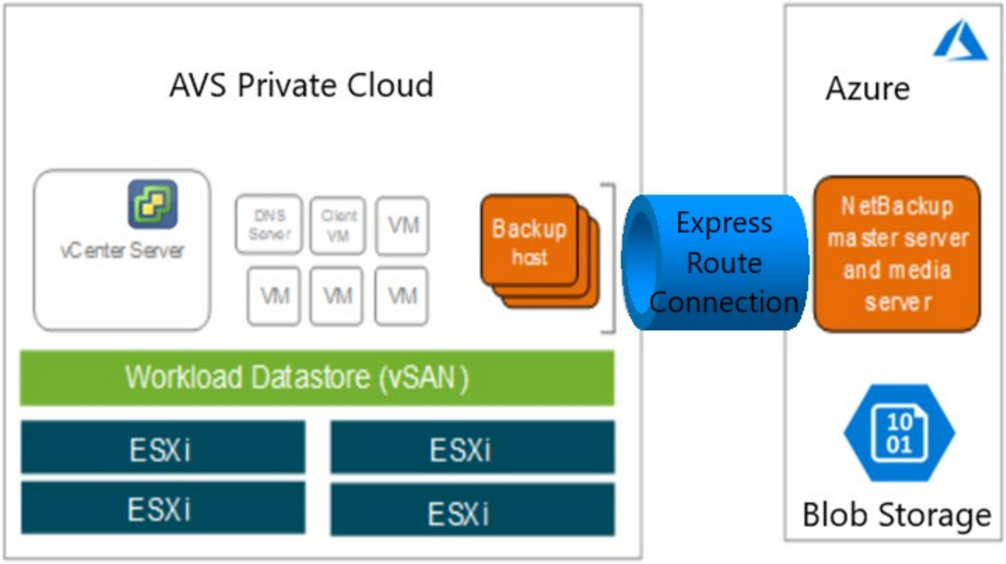
NetBackup uses a master server and optional media servers to protect virtual machines hosted in VMware private clouds. Microsoft recommends the HotAdd transport mode for efficient backup and restoration of VMs in a vSAN datastore in AVS. The HotAdd transport mode requires a backup host (proxy) to be installed in a VM. The backup host in the VM performs the backup and restore processing and can be either a NetBackup client, media server, or a NetBackup Virtual Appliance NBVA). Additional NetBackup media servers or proxy hosts can be scaled up or down when needed.

Note the following requirements and recommendations:

- The backup host must reside on a VMware cluster that has access to the vSAN datastore where vmdk files are deployed.
- The HotAdd transport mode is the preferred transport mode for AVS private cloud.
- VMware recommends that backups are not stored in the vSAN datastore.

The AVS Private Cloud and the rest of the Azure infrastructure can be linked using an ExpressRoute connection. Two simple NetBackup architectures are available to suit a variety of deployment scenarios.

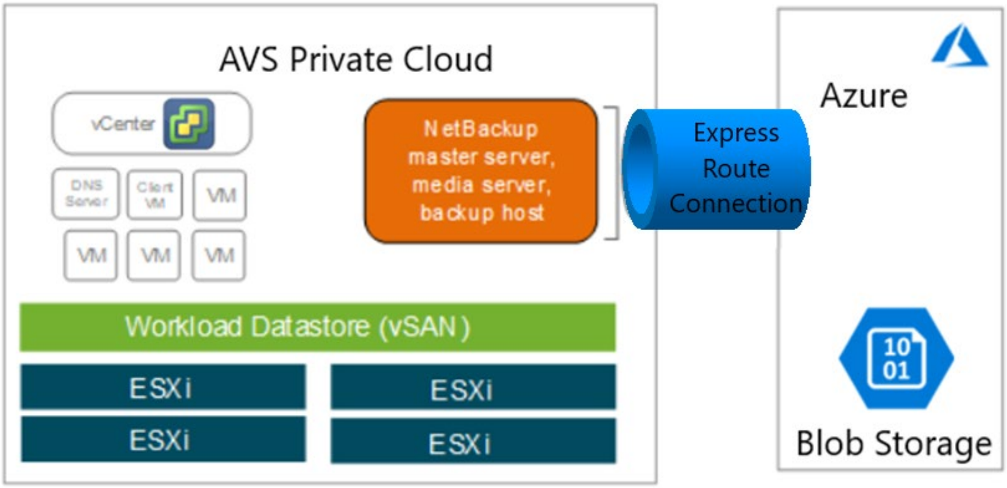
Architecture 1: NetBackup servers installed in Azure with a backup host in Private Cloud



The NetBackup master server and optional media server are installed in the Azure Virtual Network (VNet). In this architecture, the only resources required within the private cloud is a proxy or backup host – the proxy host may be set up as a NetBackup client, media server software, or a NetBackup Virtual Appliance (NBVA) in a guest VM. Enabling Accelerator attribute significantly reduces the amount of data sent into Azure (VNet). This architecture is beneficial when AVS Private Cloud resources are limited or when the NetBackup servers in Azure are also utilized to protect other Azure workloads.

A single NetBackup 8.3 Deduplication media server can also be configured to support multiple storage targets, including one local storage target, and zero or more cloud storage targets. You can move data to local and multiple cloud targets simultaneously with isolation and support for multiple tenants. The cloud targets can also be added on-demand after deduplication is configured and can be from the same or different providers, either public or private.

Architecture 2: NetBackup components deployed within AVS Private Cloud



NetBackup components are installed in the AVS private cloud: a single all-in-one NetBackup deployment can serve the role of master, media, and backup host. Additional backups hosts, CloudCatalyst media servers, or a CloudCatalyst virtual appliance can be configured to deduplicate and store backup data to Blob storage. This architecture suits environments in which the AVS resources can easily accommodate backup services. For details on how to configure NetBackup with Azure storage, see the topic - "Create a cloud storage server" in the *Veritas NetBackup Web UI Administrator's Guide*. Create a protection plan once the storage unit has been created.

Solution Components

The solution comprises of the following components:

- Azure VMware Solutions Private Cloud
- NetBackup version 8.2 or later using a new or existing NetBackup server or client
- NetBackup media server or client as a backup proxy host to communicate with VMware vCenter.
- Instant Access or Universal Shares, new features for NetBackup 8.3 BYO deployments, requires Linux operating system running RedHat 7.6 or 7.7.

NetBackup installation notes and Network Configuration

- Ensure NetBackup can communicate between the master, media server, and any clients as described in the NetBackup 6.x and 7.x and 8.x firewall port requirements article. In general, ports 1556 and 13724 are to be opened bi-directionally between all NetBackup hosts. Ports 10102 and 10082 are to be opened on all NB media servers running the deduplication engine.

- NetBackup Proxy Host communicates with VMware vSphere over Port 443. A typical NetBackup deployment from the Azure marketplace has all the required ports defined within the Network Security Group. The NetBackup 8.3 server deployed using the Azure marketplace template uses RedHat 8.2 for the operating system.
- When deploying Instant Access or Universal Shares, a Media Server Deduplication Pool (MSDP) needs to be configured on a NetBackup server running RedHat 7.6 or 7.7. Ensure that the /mnt folder on the storage server is not mounted by any mount points directly. Mount points may be mounted to its subfolders.
- Some Instant Access features are available in AVS using NetBackup 8.3 BYO servers. The NetBackup media server used for performing live browse (instant access) to download or restore individual files and folders, must be installed and configured using its fully qualified domain name (FQDN). The VxUpdate package that matches the backup (proxy) host's operating system must be added to the NetBackup master server repository.
- When installing the NetBackup master server in either Azure or AVS PRIVATE CLOUD (architecture 1 or 2), use a private DNS name for the master server name. Add the following entries to the hosts file on the master server and the backup host:

  The private IP and the private DNS of the master server.
  The IP and the DNS name of the backup host.

- AVS hostnames have the **avs.azure.com** DNS suffix. When adding vCenter credentials to NetBackup, use the FQDN for the vCenter host. Such hostnames must comply with the **avs.azure.com** DNS suffix.
- Security is an important aspect of your data protection strategy. The NetBackup web user interface provides the ability to apply role-based access control in your NetBackup environment. NetBackup uses SSL certificates to validate inter-host communications. A NetBackup authorization token may be necessary when deploying additional NetBackup servers or clients. See the topic Managing NetBackup security certificates in the *NetBackup Web UI Administrators' Guide*.
- Deploy HotFix Binary ET401300 on NetBackup 8.2 backup hosts. For version 8.3, use HotFix Binary ET4010448. These HotFixes can be obtained from the Veritas Support Download Center. or by contacting Veritas Technical Support. Without this HotFix, snapshot or restore jobs exit with a status code 1 indicating Partial success. This HotFix is not needed if running the latest NetBackup version 8.3.0.1.

    Snapshot Job - *VMware_thaw: Unable to unlock virtual machine: /vmmor/vm-58*
    Restore Job -
    bpvmutil_unlockvmerror_to_monitor: Unable to unlock virtual machine: lnx-vm2

Support considerations

NetBackup currently does not support the following when protecting AVS private clouds:

- The NetBackup vSphere Web Client Plug-in or the NetBackup vSphere Client (HTML5) Plug-in.
- Virtual machine locking or unlocking during backups or restores.

- The “Post vCenter events” option of NetBackup VMware policies.
- The NetBackup Instant Recovery feature for virtual machines, or the Instant Access virtual machines feature of the NetBackup Web User Interface.

Interoperability with VMware Cloud on Azure product features

For a detailed list of VMware versions that NetBackup supports, see the “Virtual Systems Compatibility” section of the *NetBackup Software Compatibility List (SCL)* available here.

- Backup or restore of VM templates are coming soon using the NetBackup web user interface.
- The SAN transport mode is not available. While NBD/NBD-SSL modes may work, Microsoft recommends the HotAdd transport mode for performance considerations.

Technical Support

All Veritas customers with Capacity, Traditional, or NetBackup Enterprise Virtual Client (NEVC) licensing actively under maintenance are supported according to the terms of their Veritas support contract. For further information about NetBackup licensing, see the following or contact a Veritas support representative:

About NetBackup licensing models
Veritas Technical Support

- For further information on the HotAdd transport mode with NetBackup, see Notes on the HotAdd transport mode in the *Veritas NetBackup for VMware Administrator's Guide*.
- For log directories for NetBackup for VMware, see NetBackup logging for VMware in the *Veritas NetBackup for VMware Administrator's Guide*.
- For broader information on NetBackup logging, see Using logs in the *Veritas NetBackup Logging Reference Guide*.
- For additional information on NetBackup, see NetBackup Virtual Data Protection.
- For more information on NetBackup, see Veritas NetBackup.