Working with VMware

https://campus.barracuda.com/doc/78155567/

Barracuda Backup uses the VMware vSphere Storage APIs–Data Protection to perform image-level backups of VMware vSphere virtual machines (VMs). If a vCenter server is managing the VMware environment, it is best to configure the data source with the IP address or FQDN of the vCenter server. Configuring the data source using individual ESXi hosts should only be done if a host is standalone or there is no vCenter server managing the environment.

VMware has reported an issue with ESXi version 6.0.x where incorrect changed sectors are returned. When a VM is running ESXi 6.0.x and Changed Block Tracking (CBT) is enabled, some change areas in data are not reported. When this occurs, that data is not recognized as changed and is not backed up; current and past incremental backups are potentially compromised. For more information, see the VMware knowledgebase solution Backing up a Changed Block Tracking enabled virtual machine in ESXi 6.0.x returns incorrect changed sectors (2136854).

This issue is resolved in VMware ESXi 6.0 patch ESXi600-201511001. For more information, see VMware ESXi 6.0, Patch Release ESXi600-201511001 (2137545).

VMware Recovery Licenses

This section describes VMware recovery licenses.

Licenses Required for vStorage APIs for Data Protection

The vStorage APIs for Data Protection (VADP) are included with all licensed vSphere editions including Standard, Enterprise, and Enterprise Plus.

Understanding vStorage APIs for Data Protection

Barracuda Backup can use VADP to back up vSphere VMs without requiring the Backup Agent or processing to be done inside each guest VM on the ESX host. This offloads the backup processing from ESX hosts and reduces cost by allowing each ESX host to run more VMs.

VADP leverages the snapshot capabilities of vSphere, enabling backup across a storage area network (SAN) without requiring VM downtime. This allows backups to be performed at any time without disrupting the VMs or requiring extended backup windows and application downtime.

VMware Data Recovery Backup and Restore Permissions

The tables in this section describe the VMware data recovery backup and restore permissions.

ESX/ESXi Host Machine Permissions

At a minimum, you must have the following permissions assigned to the user role on an ESX/ESXi VM:

Table 1. ESX/ESXi User Role Permissions.

System	Configuration	Disk Change Tracking
VM	Provisioning	• Allow read-only disk access • Allow VM download
VM	Snapshot Management	• Create snapshot • Remove snapshot
Global		• DisableMethods • EnableMethods • Licenses

If you are using SCSI hot-adding on an ESX/ESXi VM, the user role must have the following permissions:

- All of the permissions listed in Table 1, *and*
- The Barracuda Backup must have all of the permissions listed in Table 2

Table 2. Barracuda Backup Minimum Permissions.

System	Configuration	Permissions
Datastore		• Allocate space
VM	Configuration	• Add existing disk • Add new disk • Add or remove device • Change resource • Remove disk • Settings

vCenter Server Role for Backup and Recovery

If you wish to assign privileges to a vCenter Server user or a user in Active Directory (AD), you can create a new user with the VMware vCenter roles.

> The recovery operation requires privileges for operations on hosts, networks, and datastores. You must apply this new role to the Datacenter object or higher in the VMware vCenter Server hierarchy for the user specified in the **VMcuser** option and **Propagate to Child Object** must be turned on when adding the permission.

To create a vCenter Server role for backup and recovery operations, log in to the vCenter Server using the vSphere Client, and add the permissions listed in Table 3:

Table 3. vCenter Server Role Permissions.

Location	Configuration	Permissions
Datastore		• Allocate space • Browse datastore • Low-level file operations
Global		• DisableMethods • EnableMethods • Licenses
Guest Operations[1,2]		• Guest Operation Modifications • Guest Operation Program Execution • Guest Operation Queries
Network		• Assign network
Resource		• Assign VM to
vApp		• Add VM • Assign resource pool • Create

VM	Configuration	• Add existing/new disk • Add/remove device • Advanced • Change CPU count • Change resource • Disk change tracking • Disk Lease • Host USB device • Memory • Modify device setting • Raw device • Reload from path[4] • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual hardware
VM	Inventory	• Create new • Register • Remove • Unregister
VM	Provisioning	• Allow disk access • Allow read-only disk access • Allow VM download
VM[2]	Snapshot Management[2] > State[2]	• Create snapshot • Remove snapshot • Revert to snapshot
VM[3]	State[3]	• Create snapshot • Remove snapshot • Revert to snapshot

Notes:
[1] Guest Operations permissions are necessary *only* if you are using Data Protection for VMware to protect Microsoft Exchange Server or Microsoft SQL Server applications running inside a VM guest.
[2] vSphere 5.0 only.
[3] vSphere 4.0 only.
[4] vCenter Server 4.1 only.

vCenter Server Role for Scheduled Backup Operations Permissions

To add a vCenter Server role for backup operations only, add a role using the vSphere Client, and add the permissions listed in Table 4.

You must apply this new role to the target host (ESX/ESXi) object or higher in the VMware vCenter Server hierarchy for the user specified in the **VMcuser** option, and **Propagate to**

Child Object must be turned on when adding the permission.

Table 4. vCenter Server Role for Backup Operations Permissions.

Location	Configuration	Permissions
Global		• DisableMethods • EnableMethods • Licenses
Guest Operations[1][2]		• Guest Operation Modifications • Guest Operation Program Execution • Guest Operation Queries
VM	Configuration	• Disk change tracking • Disk Lease
VM	Provisioning	• Allow read-only disk access • Allow VM download
VM[2]	Snapshot Management[2] > State[2]	• Create snapshot • Remove snapshot
VM[3]	State[3]	• Create snapshot • Remove snapshot
Notes: [1] Guest Operations permissions are necessary *only* if you are using Data Protection for VMware to protect Microsoft Exchange Server or Microsoft SQL Server applications running inside a VM guest. [2] vSphere 5.0 only. [3] vSphere 4.0 only.		

Barracuda Backup Set Up and Restore Permissions

To set up and restore a VMware VM as a data source in the Barracuda Backup web interface, you must have administrator privileges to the VM. Once your credentials are verified and the data source is set up and backups are enabled, use the **Restore** page to restore a VM. For more information on this VMware requirement, refer to the VMware Data Recovery Administration Guide available on the VMware website.

Understanding Which Ports to Open for VMware Accessibility

In order for the Barracuda Backup appliance to access VMware servers, you must open the ports listed in the following tables:

Table 1. Data Recovery.

Port	Details
902	TCP Data Recovery Appliance ESX Host VDR to ESX Communication
22024	TCP Data Recovery vSphere Client Plug-in Data Recovery Appliance Data Recovery Management

Table 2. Ports Related to Non-Data Recovery Features.

Port	Details
22	TCP User VDP ssh (for debugging)
53	UDP VDP DNS server DNS
80	TCP User VDP http
111	TCP, UDP VDP ESXi/ESX rpcbind
443	TCP User VDP https
700	TCP VDP, LDAP Active Directory Loginmgr tool
7778	TCP vCenter VDP VDP, RMI
7779	TCP vCenter VDP VDP, RMI
8509	TCP vCenter VDP Tomcat AJP Connector
8543	TCP User VDP Redirect for Tomcat
8580	TCP vCenter VDP VDP Downloader
9443	TCP vCenter VDP VDP Web Services
27000	TCP VDP vCenter Licensing communication

VMware Support Statement

Barracuda Networks supports Barracuda Backup customers irrespective of whether they are protecting VMware environments. Barracuda Networks supports operating systems, not specific hardware configurations. VMware operates as a hardware abstraction layer.

VMware supports a set of certified operating systems and hardware, and the customer and VMware are responsible for any interactions or issues that arise at the hardware or operating system layer as a result of the customer's use of VMware.
Barracuda Networks does not require customers to recreate and troubleshoot every issue in a non-VMware environment, however, Barracuda Networks does reserve the right to request customers to diagnose certain issues in a native-certified operating system environment, operating without the virtual environment. Barracuda Networks will only make this request when there is reason to believe that the virtual environment is a contributing factor to the issue.

Any time spent on investigation of problems that may, in the sole opinion of Barracuda Networks, be

related to VMware, will be handled in the following fashion:

1. If a problem is encountered backing up a VMware environment, the customer may be required to recreate the problem on a non-VMware server, at which time Barracuda Networks will provide regular support.
2. Regardless of the problem type or source, if the problem is determined to be a non-VMware related issue, time spent on investigation and resolution will be covered as part of regular maintenance, and support will be provided as usual.

Please note that Barracuda Networks only provides technical support to customers who maintain the requisite subscriptions.