

Protecting VMware vSphere

<https://campus.barracuda.com/doc/78156831/>

Barracuda Backup follows the lifecycle policy of each supported vendor and does not support versions that are end of life or end of support as indicated by the product vendor.

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. See also [Storage Pools](#).

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 \(2137545\)](#).

Use the following steps to configure a VMware vSphere data source:

1. Log into Barracuda Backup and select the associated Barracuda Backup device in the left pane or in the devices table (for customers with multiple Barracuda Backup devices).
2. Go to the **Backup > Sources** page, and click **Add a Computer**.
3. Complete the following information on the **Add a Computer** page:
 1. **Computer description**
 2. **Computer name**
4. In the **Computer type** drop-down menu, select **VMware**.
5. In the **VMware Computer Information** section, enter the credentials of the account that Barracuda Backup is to use to connect to the vCenter Server or ESXi host.
As a best practice, use a unique account for this integration point and grant it the least level of privileges required, coordinating with the system administrator. This account requires administrative privileges to the vCenter Server or ESXi host. For additional information, see [Security for Integrating with Other Systems - Best Practices](#).
6. Click **Test Credentials** to verify that Barracuda Backup can successfully communicate with the vCenter Server or ESXi host. If the connection is unsuccessful, verify that the credentials are correct.

7. Once the VMware data source is configured, click **Save**.
8. The **Add Data Source** page displays. Ensure that **Enable CBT** is selected. This allows Barracuda Backup to perform incremental backups of the VMs. Finish configuring the backup schedule name, the offsite replication destination, and click **Save**.

By default, if a snapshot fails when trying to quiesce a VM, Barracuda Backup retries the snapshot without the quiescing option. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. To disable the non-quiesce snapshot behavior, select **Quiesce Only**.
9. Once the data source is configured, the **Schedules** page displays. For more information, see [Backup Scheduling](#).

Independent Disks and Physical RDM

Because snapshots from the hypervisor cannot be performed on Independent Disks and Physical Raw Device Mapping (RDM), the Barracuda Backup Agent must be used on these guest VMs to back up these disks. Virtual RDM does support snapshots and is therefore supported by Barracuda Backup.

VMs with Independent Disks configured are backed up by Barracuda Backup, however, the actual Independent Disk itself is excluded from the backup and an error message displays in the backup report. Independent Disks can be configured to exclude a specific disk of a VM from being backed up.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.