# Contents

1. Executive Summary 3
2. Introduction 3
   2.1 Audience 3
   2.2 Purpose 3
   2.3 Barracuda Backup & Nutanix Technology Alliance 3
3. Barracuda Backup Overview 4
   3.1 Barracuda Backup Appliance Overview 4
   3.2 Barracuda Backup Virtual Appliance (Vx) Overview 4
   3.3 VMware vSphere Support 5
   3.4 Microsoft Hyper-V Support 10
   3.5 Nutanix AHV Support 10
4. Barracuda Backup Virtual Appliance (Vx) Deployment 10
   4.1 System Requirements 10
   4.2 Technical Best Practices 12
   4.3 VMware vSphere Deployment 12
   4.4 Microsoft Hyper-V Deployment 16
   4.5 Firewall Port Configuration 22
   4.6 Configuring the Barracuda Backup Virtual Appliance (Vx) 22
   4.7 Activating the Barracuda Backup Virtual Appliance (Vx) 24
   4.8 Expanding the Capacity of the Barracuda Backup Virtual Appliance (Vx) 24
5. Conclusion 25
1. Executive Summary

Barracuda Backup provides integrated hardware and software solutions that protect physical, virtual, cloud, and SaaS data and applications from cybercriminals, natural disasters, hardware failures, and more. This document makes recommendations for the protection of virtual machines and applications running on a Nutanix platform, as well as the deployment of the Barracuda Backup Virtual Appliance (Vx) in a Nutanix environment.

2. Introduction

2.1 Audience

This document is intended for use by individuals responsible for the architecture, design, management, and support of Barracuda Backup on Nutanix systems. It is assumed that readers of this document are familiar with both Barracuda Backup and Nutanix, and are using this best practice guide to better understand the synergy between the two products.

2.2 Purpose

This document covers the high-level best practices for Barracuda Backup and Barracuda Backup Vx with Nutanix. We will cover Barracuda’s support for VMware vSphere, Microsoft Hyper-V, and how Nutanix AHV virtual machines and applications can be protected. This document will also provide step-by-step instructions for deploying the Barracuda Backup Virtual Appliance (Vx) into a Nutanix environment running VMware vSphere and Microsoft Hyper-V.

2.3 Barracuda Backup & Nutanix Technology Alliance

Barracuda Backup provides an additional layer of protection for virtualized workloads powered by Nutanix. With hypervisor-level snapshots for VMware vSphere, Barracuda Backup makes it easy to protect your data, virtual machines, and applications running on Nutanix. Together, Barracuda Backup and Nutanix provide a complete data protection solution that helps organizations meet their recovery point and recovery time objectives.

<table>
<thead>
<tr>
<th>BENEFIT</th>
<th>NUTANIX</th>
<th>BARRACUDA BACKUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Data Protection w/Snapshots</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Replication to Other Nodes</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Business Continuity / Failover</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Granular File Recovery (Direct Restore)</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Granular Application Recovery</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Offsite (external) Replication</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Long Term Retention</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Tape / Disk Out Capability (Archive)</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Backup, DR, &amp; Archive in the Cloud</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Live VM Recovery for VMware</td>
<td>●</td>
<td></td>
</tr>
</tbody>
</table>

Barracuda Backup 6.4
3. Barracuda Backup Overview

3.1 Barracuda Backup Appliance Overview

Barracuda Backup Appliances provide an integrated, all-in-one data protection solution that includes the necessary compute, local storage, backup software, and offsite storage to fulfill all of your backup requirements. To ease the pain of management and provide access to data at all times, Barracuda Backup is managed by a cloud-hosted, centralized management interface called Barracuda Cloud Control. Barracuda Backup Appliances range in capacity from 1 TB to 112 TB and can protect most environments up to 50 TB with a single device.

Some of the advantages of Barracuda Backup include:

- Simple pricing with no per-application or per-server licensing fees
- Cloud-based central management for seamless multisite administration
- Rapid local or remote recovery, preventing data loss and minimizing down time
- Built-in cloud and site-to-site replication prevent data loss in case of disaster
- LiveBoot and Cloud LiveBoot enable rapid recovery of virtual machines
- Cloud-to-Cloud Backup protects Microsoft Office 365 environments from data loss
- Offsite vaulting of historical revisions frees up valuable space on local storage
- Compression and deduplication for up to 50X reduction in storage and bandwidth requirements

3.2 Barracuda Backup Virtual Appliance (Vx) Overview

The Barracuda Backup Virtual Appliance or Vx, is a virtual image of a Barracuda Backup Appliance that can be deployed to a VMware vSphere or Microsoft Hyper-V environment. The software-based solution, once deployed, provides the exact same functionality and features as the Barracuda Backup Appliances. In addition to the advantages provided by a Barracuda Backup Appliance, Barracuda Backup Vx provides two key benefits for customers:

- Barracuda Backup Vx enables customers to deploy the Barracuda Backup product on their own infrastructure, using their own storage.
- Barracuda Backup Vx helps fully virtualized customers more effectively use and deploy Barracuda Backup to protect their virtual environment without having to deploy a dedicated physical Barracuda Backup Appliance.
3.3 VMware vSphere Support

Hypervisor-level snapshots of each guest virtual machine. Barracuda Backup uses the VMware vStorage APIs for Data Protection (VADP) that are included with all licensed vSphere editions for all backup and recovery tasks. Barracuda Backup and Barracuda Backup Vx leverage VMware Changed Block Tracking (CBT) to perform incremental forever backups.

In addition to providing protection for virtual machines running on VMware, the Barracuda Backup Vx can be deployed to and run on it. The Backup Vx image is imported into vSphere where it can be configured like any other virtual machine. Barracuda Backup and Barracuda Backup Vx support the following versions of VMware vSphere:

- vSphere 6.x
- vSphere 5.x

- Free ESXi does not include the VMware vStorage APIs for Data Protection (VADP) and therefore cannot be protected using hypervisor-level snapshots. To protect free ESXi, the Barracuda Backup Agent will need to be installed in each guest VM and each VM will be backed up at the guest level. Barracuda Backup Vx can be deployed to and run on the free version of ESXi, however, the same backup rules apply.
Protecting Nutanix Clusters Running VMware vSphere

1. Within the Barracuda Backup user interface, navigate to the Backup -> Sources page.
2. Click the Add a Computer button.
3. Provide a Computer description. This is just used to identify the system within Barracuda Backup.
4. Specify the Computer name. This can be either the Nutanix vSphere cluster IP address or the Fully Qualified Domain Name (FQDN).
5. Change the Computer type to VMware in the drop-down menu.
6. Enter a username and password to connect to the Nutanix vSphere cluster, then click the Test Credentials button.
7. If you can successfully connect to the Nutanix vSphere cluster, click the Save button.
   **Note:** If you are NOT able to connect using the supplied credentials, you may need to use another account or there could be connection issues between the Barracuda Backup device and the Nutanix vSphere cluster.
8. On the next page, add this source to a new schedule or create a new schedule.
9. Configure your replication, Changed Block Tracking, and Snapshot options, then click the Save button.
10. On the Schedules page, select which datacenters, hosts, or virtual machines will be included in the backup schedule.

![Figure 4: Selecting VMs in a backup schedule](image)

11. Specify the days that the backup schedule will run, then specify the start time.
12. Click the Save button when you are finished setting up the backup schedule.
   **Note:** Multiple schedules can be configured for the same source and can run at different time and day intervals.
13. Back on the Backup -> Sources page, the Nutanix vSphere cluster will look like this:

![Figure 5: Nutanix vSphere cluster as a data source](image)

14. To run a backup manually, navigate to the Backup -> Schedules page and click the Run Backup Now button next to the desired schedule.
15. To view the progress of a running backup job, navigate to the Reports -> Backup page.

**Figure 6: Viewing backup reports**

**Recovering VMware vSphere Data, Applications, and Virtual Machines**

Barracuda Backup provides several options for restoring data, applications, and virtual machines originating from VMware vSphere. Complete virtual machine, as well as granular file and folder restoration can be initiated from the Restore -> Restore Browser. From the Restore Browser, select the Nutanix vSphere cluster data source and navigate down to the virtual machines. From there, clicking the Restore link next to a virtual machine launches the virtual machine restore dialog. A virtual machine can be restored to both the original location or an alternate location.

**Figure 7: Recovering a VMware vSphere virtual machine**

Clicking on the name of the virtual machine will allow you to browse inside of that virtual machine image. From there, any file or folder can be downloaded and recovered.

VMware virtual machine instant recovery, called Barracuda LiveBoot, can be performed by navigating to the Restore -> LiveBoot page. The following steps will walk you through the LiveBoot instant recovery process.

1. From the LiveBoot page, click the Add LiveBoot button.

**Figure 8: Barracuda LiveBoot for VMware**
2. Select the virtual machines that you would like to recover from the list, then click **Add**.

![Figure 9: Select VMs for instant recovery](image)

3. To start the virtual machine instant recovery process, click the **Start** button to launch the virtual machine restore dialog.

![Figure 10: View the status of recovered VMs](image)

4. Choose your recovery destination, virtual machine name, and recovery options, then click **Boot**.

![Figure 11: Performing virtual machine instant recovery](image)

5. The Barracuda Backup user interface will provide you with basic statuses of Not Running, Running, Failed, and Stopped. To view more details about the status of the virtual machine instant recovery, log in to your vSphere Web Client and view the **Recent Tasks** pane.

![Figure 12: Recent Tasks in vSphere Web Client](image)
6. Within a few seconds, the recovered virtual machine will be visible within your list of VMs in the vSphere Web Client and will begin the boot process.

![Figure 13: Viewing your recovered virtual machine](image)

7. Open the virtual machine console to view the boot process.

![Figure 14: Connect to and interact with your recovered VM](image)

8. If this is only a recovery test or you have no plans on keeping the recovered virtual machine, click the **Stop** button in the Barracuda Backup LiveBoot page, then click **Destroy**. This will shut down the virtual machine, delete it, and unmount the Barracuda Backup NFS datastore.

![Figure 15: View the status of and control your recovered VMs](image)

9. If you do wish to keep the recovered virtual machine, you can use vMotion to perform a datastore migration or shut the VM down and perform a datastore migration to move the virtual machine disk from the Barracuda Backup device and onto a datastore of your choosing.
3.4 Microsoft Hyper-V Support

Barracuda Backup and Barracuda Backup Vx offer guest-level protection for Microsoft Hyper-V on Nutanix, using the Barracuda Backup Agent for Windows and Linux. Host-based protection is unavailable at this time as the Barracuda Backup Agent for Windows does not support SMB 3.0, which Nutanix uses in the Hyper-V cluster configuration. The following section provides guidance on a Microsoft Hyper-V environment.

In addition to providing protection for guest virtual machines running on Hyper-V, the Barracuda Backup Vx can be deployed to and run on it. The Backup Vx image is imported into Hyper-V where it can be configured like any other virtual machine. Barracuda Backup and Barracuda Backup Vx support the following versions of Microsoft Hyper-V:

- Windows Server Hyper-V 2016
- Windows Server Hyper-V 2012 R2
- Windows Server Hyper-V 2012
- Windows Server Hyper-V 2008 R2
- Windows Server Hyper-V 2008

Recovering Microsoft Hyper-V Data, Applications, and Virtual Machines

Barracuda Backup provides several options for restoring data, applications, and virtual machines originating from Microsoft Hyper-V. Complete virtual machine, as well as granular file and folder restoration can be initiated from the **Restore -> Restore Browser**. Hyper-V virtual machines running Microsoft Windows operating systems can be recovered using Barracuda's Physical-to-Virtual (P2V) ISO, where they can be restored back to a Microsoft Hyper-V or VMware vSphere host. Individual files and folders can be restored or downloaded directly by browsing through the agent source for that virtual machine.

3.5 Nutanix AHV Support

To protect virtual machines running on Nutanix AHV, Barracuda Backup recommends installing the Barracuda Backup Agents for Windows and Linux inside each guest virtual machine and performing guest-level backup and recovery. At this time, Barracuda Backup does not provide hypervisor-level snapshot support for Nutanix AHV.

While the Barracuda Backup Vx can be deployed to and run successfully on Nutanix AHV, Barracuda does not officially support running the Backup Vx on Nutanix AHV at this time until further testing and validation has been completed.

4. Barracuda Backup Virtual Appliance (Vx) Deployment

4.1 System Requirements

This section of the document provides guidance on designing and deploying Barracuda Backup Vx on VMware vSphere and Microsoft Hyper-V platforms.

**VMware and Hyper-V System Requirements**

Barracuda offers the following types of images for a Barracuda Backup Vx deployment. Follow the instructions for your hypervisor below to deploy the Barracuda Backup Virtual Appliance.

<table>
<thead>
<tr>
<th>IMAGE TYPE</th>
<th>SUPPORTED HYPERVISORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVF</td>
<td>VMware ESX and ESXi (vSphere Hypervisor) versions 5.x and 6.x</td>
</tr>
</tbody>
</table>
CPU and RAM System Requirements
The most common mistake when designing an environment for Barracuda Backup Vx is to size only for capacity as opposed to sizing for capacity and performance. Tasks such as backup, offsite replication, data restoration, and purging can use a significant amount of system resources. When considering a Barracuda Backup virtual deployment, it is best to consider the use cases of the Backup Vx in addition to needed storage.

vCPU Recommendations

<table>
<thead>
<tr>
<th>BACKUP VOLUME</th>
<th>MINIMUM RECOMMENDED vCPUS</th>
<th>HIGH PERFORMANCE RECOMMENDED vCPUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 TO 2 TB</td>
<td>1 vCPU</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>2 TO 6 TB</td>
<td>2 vCPUs</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>6 TO 16 TB</td>
<td>4 vCPUs</td>
<td>8 vCPUs</td>
</tr>
<tr>
<td>16 TO 32 TB</td>
<td>8 vCPUs</td>
<td>16 vCPUs</td>
</tr>
<tr>
<td>32 TO 100 TB</td>
<td>16 vCPUs</td>
<td>32+ vCPUs</td>
</tr>
</tbody>
</table>

Note: When deploying a Receiver Vx (V95), it is acceptable to use roughly 50% of the recommended vCPUs. Less resources can be used since the Receiver Vx will not be backing up or replicating data offsite. In the event of a restore or disaster recovery scenario, more resources can be added to the Receiver Vx to improve performance.

RAM Recommendations

<table>
<thead>
<tr>
<th>BACKUP VOLUME</th>
<th>MINIMUM RECOMMENDED vCPUS</th>
<th>HIGH PERFORMANCE RECOMMENDED vCPUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 TO 1 TB</td>
<td>2 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>1 TO 4 TB</td>
<td>4 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>4 TO 12 TB</td>
<td>8 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>12 TO 16 TB</td>
<td>16 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>16 TO 24 TB</td>
<td>32 GB</td>
<td>64 GB</td>
</tr>
<tr>
<td>24 TO 48 TB</td>
<td>64 GB</td>
<td>128 GB</td>
</tr>
<tr>
<td>48 TO 100 TB</td>
<td>128 GB</td>
<td>256+ GB</td>
</tr>
</tbody>
</table>

Note: When deploying a Receiver Vx (V95), it is acceptable to use roughly 50% of the recommended vCPUs. Less resources can be used since the Receiver Vx will not be backing up or replicating data offsite. In the event of a restore or disaster recovery scenario, more resources can be added to the Receiver Vx to improve performance.

Storage System Requirements
When deploying a Barracuda Backup Virtual Appliance, Barracuda recommends the following storage system requirements:

- Any storage infrastructure consisting of Local/Direct Attached Storage (DAS), Storage Area Network (SAN), and Network Attached Storage (NAS).
- Storage with inadequate throughput, read, and write speeds will cause Barracuda Backup Vx performance to suffer.
- Servers with software RAID, slow Network Attached Storage (NAS), and low-RPM drives will yield poor performance.
4.2 Technical Best Practices

The following are best practices for a successful Barracuda Backup Virtual Appliance deployment:

- Barracuda Backup utilizes memory (RAM) for database queries during backup, restore, and offsite replication. Barracuda highly recommends following the recommended minimum resources for memory in the RAM recommendations table above.
- Barracuda Backup uses CPU resources for hashing blocks during deduplication, compression for offsite replication, and rehydration of data during restoration. Barracuda highly recommends following the recommended minimum resources for vCPUs in the vCPU Recommendations table above.
- At minimum, memory resources should be dedicated (reserved). It is also recommended that the CPU be dedicated to Barracuda Backup Vx, and not shared with other virtual machines on the host. This aligns with VMware and Microsoft’s recommendations for virtualized Microsoft Exchange Server and SQL Server implementations.
- A separate data store is recommended for use with the virtual appliance due to disk I/O constraints or an entirely separate storage server/environment altogether from the production environment.
- Other system components such as network and storage need to be sized accordingly to prevent them from becoming a bottleneck.
- It is important that snapshots are not used on the Barracuda Backup Virtual Appliance. Even if data is not being replicated to the Barracuda Cloud, configuration data is still sent to Barracuda so that the unit can be managed. Reverting to a previous state using snapshots can potentially cause loss of data and unit corruption. Independent disks are the default selection and highly recommended to avoid snapshots.
- All Barracuda Backup Vx disk, vCPUs, and RAM can be adjusted later by shutting down the system properly and making the necessary changes through the hypervisor.

4.3 VMware vSphere Deployment

The following steps demonstrate how to deploy the Barracuda Backup Virtual Appliance to a Nutanix environment running the VMware vSphere hypervisor. The following deployment scenario was done using the VMware vSphere 6.5 Web Client instead of Nutanix Prism, as certain features such as Image Configuration were unavailable during testing.

1. Download and extract the Barracuda Backup Vx .zip archive to a location that can be accessed from a machine using the vSphere Web Client.
2. From the vSphere Web Client, click the Actions drop-down menu and select **Deploy OVF Template**.

![Figure 17: Deploy OVF Template](image)
3. From the Deploy OVF Template wizard, select **Local file**, then click **Browse**.

![Figure 18: Deploy OVF Template wizard](image1)

4. Navigate to the extracted folder that contains the Barracuda Backup Vx files. Select both the `.ovf` file and the `.vmdk` file, then click **Open**.

![Figure 19: Select `.ovf` and `.vmdk` files](image2)

5. From the Deploy OVF Template wizard, complete the following:
   - Virtual machine name and location
   - Host, cluster, or resource pool
   - Storage location and settings
     
     **Note**: Select the disk format as **Thick provision lazy zeroed**. Do **NOT** select Thin provision as the disk format. A dedicated datastore is recommended for Barracuda Backup Vx storage.
   - Destination network

6. Review your settings and click **Finish**.

7. After the template deployment is complete, locate the Barracuda Backup Virtual Appliance in the list of virtual machines.
8. With the Barracuda Backup Virtual Appliance powered off, right-click the appliance and choose Edit Settings.

9. Edit the CPU and Memory, using the vCPU and RAM Recommendations tables above for reference.

10. Edit the Hard disk 1 size.

11. Change the Disk Mode to Independent – Persistent.

   **Note:** Changing the Disk Mode to Independent (Persistent) will prevent snapshots from taking place for this disk. Taking snapshots and reverting to a previous point in time can cause data loss.

12. Review your virtual hardware settings carefully, then click OK.
13. Power **ON** the Barracuda Backup Virtual Appliance, then open the virtual machine console.

![Figure 22: Barracuda Backup Vx installation](image)

14. If you have added additional storage to Hard disk 1 or added a new hard disk, choose **Yes** to format the new disk space. This may take several minutes to complete, depending on the amount of disk space.

![Figure 23: Format additional disk space](image)

15. Once the setup and formatting is complete, the Barracuda Backup Virtual Appliance will reboot and display the System Configuration page.

![Figure 24: System Configuration](image)

To continue with your Barracuda Backup Vx configuration and activation, jump to "4.6 Configuring the Barracuda Backup Virtual Appliance (Vx)".
4.4 Microsoft Hyper-V Deployment

The following steps demonstrate how to deploy the Barracuda Backup Virtual Appliance to a Nutanix environment running the Microsoft Hyper-V hypervisor. The following deployment scenario was done using Microsoft System Center 2016 Virtual Machine Manager (SCVMM) instead of Nutanix Prism, as certain features such as Image Configuration were unavailable during testing.

1. Download and extract the Barracuda Backup Vx.zip archive to a location that can be accessed from a machine using SCVMM or Hyper-V Manager.
2. Add or Import the Barracuda Backup Vx.vhd to the SCVMM library or use the Import Virtual Machine tool in Hyper-V Manager.

3. In SCVMM, select Create Virtual Machine.
4. In the Create Virtual Machine wizard, choose “Use an existing virtual machine, VM template, or virtual hard disk”, then click **Browse**.

5. Select the Barracuda Backup Vx.vhd from the list, then click **OK**.

![Select Virtual Machine Source](image)

*Figure 27: Select virtual machine source*

6. Click **Next** on the Select Source page of the wizard to continue.
7. Specify a name and description for the Barracuda Backup Vx on the Specify Virtual Machine Identity page.

8. From the Configure Hardware page, specify the CPU and Memory, using the vCPU and RAM Recommendations tables above for reference.

9. Click New and choose Disk from the drop-down menu.
10. In the Disk settings, choose "Create a new virtual hard disk", then specify the preferred disk size.

Note: When sizing the hard disk, try to size for about double the amount of raw data that will be initially protected. This will provide enough storage for retention and data growth. Additional disks can be added to the Barracuda Backup Virtual Appliance. Additional disks or storage will be recognized during the system boot process.

![Figure 29: Virtual hardware configuration](image)
11. In the Advanced section, select Checkpoints. Ensure that "Enable checkpoints" is NOT selected. 

**Note:** Disabling checkpoints will prevent snapshots/checkpoints from taking place on the Barracuda Backup Vx virtual machine. Taking snapshots/checkpoints and reverting to a previous point in time can cause data loss.

![Configure Hardware](image)

*Figure 30: Disabling checkpoints*

12. Review your virtual hardware settings carefully, then click **Next**.
13. On the Select Destination page, choose ‘Place the virtual machine on a host’, then click Next.

![Select Destination](image)

**Figure 31: Select virtual machine destination**

14. In the next several sections of the wizard, choose a host to deploy the virtual machine to, configure the virtual machine and disk storage location, and choose your startup options.

15. Carefully review your virtual machine configuration, then click Create.

16. Power ON the Barracuda Backup Virtual Appliance, then open the virtual machine console.

17. If you have added a new disk or additional storage to a hard disk, choose Yes to format the new disk space. This may take several minutes to complete, depending on the amount of disk space.

![Format additional disk space](image)

**Figure 32: Format additional disk space**
18. Once the setup and formatting is complete, the Barracuda Backup Virtual Appliance will reboot and display the System Configuration page.

To continue with your Barracuda Backup Vx configuration and activation, jump to "4.6 Configuring the Barracuda Backup Virtual Appliance (Vx)".

### 4.5 Firewall Port Configuration

For security purposes, your Barracuda Backup Virtual Appliance should be located behind a corporate firewall. If this is the case, make sure that the following ports are open to ensure proper operation of your Barracuda Backup Vx.

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>DIRECTION</th>
<th>USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP &amp; UDP</td>
<td>OUTBOUND</td>
<td>Health Monitoring</td>
</tr>
<tr>
<td>443</td>
<td>TCP &amp; UDP</td>
<td>OUTBOUND</td>
<td>Health Monitoring</td>
</tr>
<tr>
<td>1194</td>
<td>TCP &amp; UDP</td>
<td>OUTBOUND</td>
<td>Configuration/Management</td>
</tr>
<tr>
<td>5120</td>
<td>TCP &amp; UDP</td>
<td>OUTBOUND</td>
<td>Barracuda Backup Agents</td>
</tr>
<tr>
<td>5121-5129</td>
<td>TCP &amp; UDP</td>
<td>OUTBOUND</td>
<td>Offsite Replication</td>
</tr>
</tbody>
</table>

### 4.6 Configuring the Barracuda Backup Virtual Appliance (Vx)

Once you have deployed the Barracuda Backup Vx to either VMware vSphere or Microsoft Hyper-V, you will need to provision it, using the license you should have received via email or from the website when you downloaded the Barracuda Backup Vx images. If you do not have a 15-digit license token, please contact your Barracuda sales representative or request an evaluation at barracuda.com.

1. From the System Configuration screen, use keyboard arrows to select **TCP/IP Configuration**.
2. Specify your network settings, then use your arrows to **Save** the changes. Once the new settings have taken effect, the Network Status for Local and Internet will show as "Up". Cloud will remain "Down" until the Barracuda Backup Vx has been linked to a Barracuda Cloud Control Account. For instructions on linking a device to a BCC account, click here.
3. Once the Network Status for Local and Internet show as "Up", use keyboard arrows to select **Licensing**.

4. In the Token field, enter the unique token provided to you by Barracuda Networks, then **Save**.

5. Provided the Barracuda Backup Vx has an Internet connection, it will contact Barracuda Networks and fetch the associated model and serial number. Type **YES** and press **Enter** to apply the license.

6. Once applied, the license will be installed. When prompted, press **Enter** to reboot.
7. Once the Barracuda Backup Vx reboots, you should see the following information on the System Configuration screen:

- Serial #
- Firmware version
- Network Status – Local: Up
- Network Status – Internet: Up
- Network Status – Cloud: Down

Continue to the section Activating the Barracuda Backup Virtual Appliance Vx to link your Barracuda Backup Vx to Barracuda Cloud Control and change the Network Status – Cloud to “Up”.

4.7 Activating the Barracuda Backup Virtual Appliance (Vx)

Refer to the Barracuda Campus article “How to Install the Barracuda Backup Appliance” and follow the instructions under Activate Backup Product and Create a Barracuda Cloud Control Account if you do not already have a Barracuda Cloud Control account.

Once the Barracuda Backup Vx is linked to your Barracuda Cloud Control account, the Network Status – Cloud will change to “Up”.

![System Configuration](image)

*Figure 37: Fully configured and activated*

4.8 Expanding the Capacity of the Barracuda Backup Virtual Appliance (Vx)

Throughout the lifecycle of the Barracuda Backup Vx, you will most likely need to edit the CPU, RAM, or disk space. To expand the capacity or change the CPU, RAM, or other virtual hardware settings, perform the following steps.

1. Power down the Barracuda Backup Vx.
2. Right-click on the Barracuda Backup Vx and choose **Edit Settings**.
3. Edit the CPU, RAM, Hard Disks, or other virtual hardware settings.
4. Click **OK** to apply your changes.
5. **Conclusion**

Barracuda Backup provides Nutanix customers with a cloud-first approach to backup and recovery. Fully tested and validated on Nutanix clusters running VMware vSphere, Barracuda Backup can both protect virtual machines and be deployed as a virtual appliance within VMware vSphere. Barracuda Backup also supports the protection of virtual machines running on both Microsoft Hyper-V and Nutanix AHV, with the ability to be deployed as a virtual appliance on Hyper-V. The combined solution of Nutanix and Barracuda Backup gives customers the peace of mind that their data, applications, and virtual machines are fully protected and always available.

---

**About Nutanix**

Nutanix makes datacenter infrastructure invisible by delivering an Enterprise Cloud that enables IT to focus on the applications and services that power their business. Go beyond hyperconverged infrastructure with one OS, one click™. Learn more at www.nutanix.com or follow up on Twitter @nutanix.

**About Barracuda Networks**

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda’s customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda Networks, Barracuda and the Barracuda Networks logo are registered trademarks or trademarks of Barracuda Networks, Inc. in the U.S. and other countries.