UVM Appliance – Azure
Quick Start Guide
Table of Contents

Introduction .................................................................................................................................................. 3
Prerequisites ............................................................................................................................................... 3
  License Keys ......................................................................................................................................... 3
UVM Instances ........................................................................................................................................ 3
Running an Azure Virtual Machine ........................................................................................................ 3
In Azure .................................................................................................................................................... 3
Configuring Security – Firewall ............................................................................................................... 5
VPN Access ............................................................................................................................................. 5
UVM Appliance Configuration Wizard .................................................................................................... 6
Introduction

This guide provides important information that will help you get started with your UVM appliance instance available from the Azure Marketplace.

Prerequisites

License Keys

You must already have license keys for the BeyondTrust solutions that you want to use.

Contact BeyondTrust to get the license keys. You will use the keys later when you go through the configuration wizard on the UVM instance.

UVM Instances

There are two recommended UVM instances available through the Azure marketplace.

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>vCPU</th>
<th>Memory</th>
<th>SSD Storage</th>
<th>Dedicated EBS Bandwidth (Mbps)</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS4_V2</td>
<td>8</td>
<td>28 GB</td>
<td>56 GB</td>
<td>1000</td>
<td>1 to 10,000</td>
</tr>
<tr>
<td>DS5_V2</td>
<td>16</td>
<td>56 GB</td>
<td>112 GB</td>
<td>2000</td>
<td>10,000 to 20,000</td>
</tr>
</tbody>
</table>

Running an Azure Virtual Machine

For complete details about how to run an Azure machine, you can review the Azure documentation:


In Azure

1. Select Virtual Machines from the menu on the left.
2. Select Add. Enter BeyondInsight in the Search box.

3. Select a deployment model and click Create. The following section goes through the five steps to complete your purchase.

   **Step 1:** Configure Basic Settings.
   - Enter a name, VM Disc Type, create a User Name and Password. You can create a new resource group or choose an existing one. Select a location and click OK.
**Step 2:** Choose a Size. It is recommended that you choose a UVM size from the Recommended systems.  

**Step 3:** Configure optional settings.  

<table>
<thead>
<tr>
<th>Create virtual machine</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Basic Disk</td>
<td></td>
</tr>
<tr>
<td>2 Size: Disk</td>
<td></td>
</tr>
<tr>
<td>3 Settings: Configure optional features</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Managed Disks.** Click **Yes** to automatically manage the availability of disks to provide data redundancy and fault tolerance without creating and managing storage accounts on your own. Managed disks may not be available in all regions.  
- **Virtual Network.** Virtual networks are logically isolated from each other in Azure. You can configure their IP address ranges, subnets, route tables, gateways and security settings, much like a traditional network in your data center. Virtual machines on the same virtual network can access each other by default.  
- **Subnet.** A subnet is a range of IP addresses in your virtual network, which can be used to isolate virtual machines from each other or from the Internet.  
- **Public IP Address.** Use a public IP address to communicate with the virtual machine from outside the virtual network. Choose Dynamic or Static and give it a name.  
- **Extensions.** Extensions are not currently supported.  
- **High Availability.** Select **None.**  
- **Monitoring.** Enable this feature to capture serial console output and screenshots of the virtual machine running on a host to help diagnose startup issues.  
- **Select OK.**  

**Step 4:** A summary of the configuration settings is displayed. Click **OK** to confirm.  

**Step 5:** Click **Purchase** to complete your order.  

4. It will take several minutes for the machine to deploy. After the machine deploys select **Informational** from the options under the Notifications tab.
Configuring Security – Firewall

When you run the instance you want be sure to configure your firewall. When you initially run the instance, the 3389 port is open to all IP addresses. Change the firewall settings to reflect your IP address only. For security purposes, limit your Internet exposure to only your IP address.

VPN Access

It is recommended that you use a VPN connection when you are using your UVM appliance instance. For security reasons, accessing your assets through VPN is recommended. Use the following link for configuring the VPN Tunnel in Azure:

UVM Appliance Configuration Wizard

You must configure your UVM appliance using the UVM Configuration wizard.

1. You can run software updates for the UVM-20 if updates are available. Click Update Now or Skip This Step. All products that need a license are not updated at this time and will need to be updated after running the Configuration wizard.

2. After updates are completed you can go to the Configuration wizard.

3. Click Start the Configuration Wizard.
4. Read the license agreement, and then click I Agree.
   You must accept the licensing agreement for the installation to continue.
5. On the Network Settings page, provide the following details:
   Network State

6. **Click Next.** On the Registration Information, enter the name, organization, and address information.

7. **Click Next.** On the BeyondTrust Licenses page, enter the license keys.

   If you selected No internet connection is step 7, see Offline Licensing.

   - **Client Portal Login** - You can choose to retrieve license keys automatically from the BeyondTrust client portal. Enter your username and password, and then click **Retrieve Serial Numbers**.
   - **Serial Numbers** - Enter the serial number provided when you purchased the product. To access your serial number, log on to the client portal, and select Product Licensing > Managing Your Serial Numbers. Click **Get Offline License** and follow the instructions on obtaining the license key offline. Manually enter the license key once it is received.

8. **On the User Credentials page, enter the following passwords:**

   - **Administrator password** - This password enables you to access the appliance. The email address will receive UVM reports, alerts, and alerts on hardware events.
   - **Central Policy Server password** - This password is used by Central Policy, to deploy Retina Protection agents and to run Retina scans.
   - **BeyondInsight user name and password.**
9. Click **Next**.
10. On the Machine Configuration page:
   - Enter the time zone information, and date and time.
   - Select an auto synchronization setting.
11. Click **Next**. On the Review page verify the information. Click **Change** to adjust settings.
12. To save the settings to a configuration file, click **Download Configuration File**. If for any reason you need to go through the configuration for the appliance again, you can upload the configuration file to apply your settings.
13. Click **Next**, and then click **Proceed to the Roles Configuration**.
14. If the roles configuration is correct, then click **The Current Roles Configuration Looks Good**, otherwise click **Go to The Roles Editor**.
   a. In the Roles Editor change the role settings you need, apply your changes and when complete click **Close Roles Editor**.
15. If the BeyondInsight license includes PowerBroker Password Safe, then you can configure High Availability now. Otherwise, configure HA on the High Availability page later.
16. Click **Start Appliance**. The configuration completes and the browser opens to the Diagnostics logon page.
17. Restart the UVM after configuration so the scanner can start.