ALTEON VA FOR AZURE GETTING STARTED GUIDE

Document ID: RDWR-ALOS-AZ_GSG2306

June 2023

Copyright Notices

The programs included in this product are subject to a restricted use license and can only be used in conjunction with this application.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL, please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgment:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS”' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

This product contains the Rijndael cipher

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimized ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

The OnDemand Switch may use software components licensed under the GNU General Public License Agreement Version 2 (GPL v.2) including LinuxBios and Filo open source projects. The source code of the LinuxBios and Filo is available from Radware upon request. A copy of the license can be viewed at: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

This code is hereby placed in the public domain.

This product contains code developed by the OpenBSD Project

Copyright ©1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

TABLE OF CONTENTS

CHAPTER 1 – PREFACE

This guide describes the getting-started process of the Alteon Virtual Appliance (VA) platform for the Microsoft Azure cloud.

Microsoft Azure is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers.

It eliminates the need to invest up front in hardware and enables organizations to develop and deploy applications faster. Organizations use the Azure cloud to launch virtual machine instances as needed, configure security and networking, and manage storage.

For detailed information regarding the Azure cloud, refer to the Microsoft Azure documentation at `https://azure.microsoft.com`.

Who Should Use This Book

This guide is intended for network administrators maintaining applications in the Microsoft Azure cloud. It assumes familiarity with Microsoft Azure services, as well as general inter-networking technologies and concepts.

Related Documentation

Alteon Application Switches have the following related documentation, which is required to regularly manage the Azure Alteon VA, in addition to the specifics pertaining to Alteon's integration into the Azure cloud:

- Alteon Application Switch Operating System Command Reference
- Alteon Web Based Management Application Guide
- Alteon Command Line Interface Application Guide
- Alteon Application Switch Troubleshooting Guide

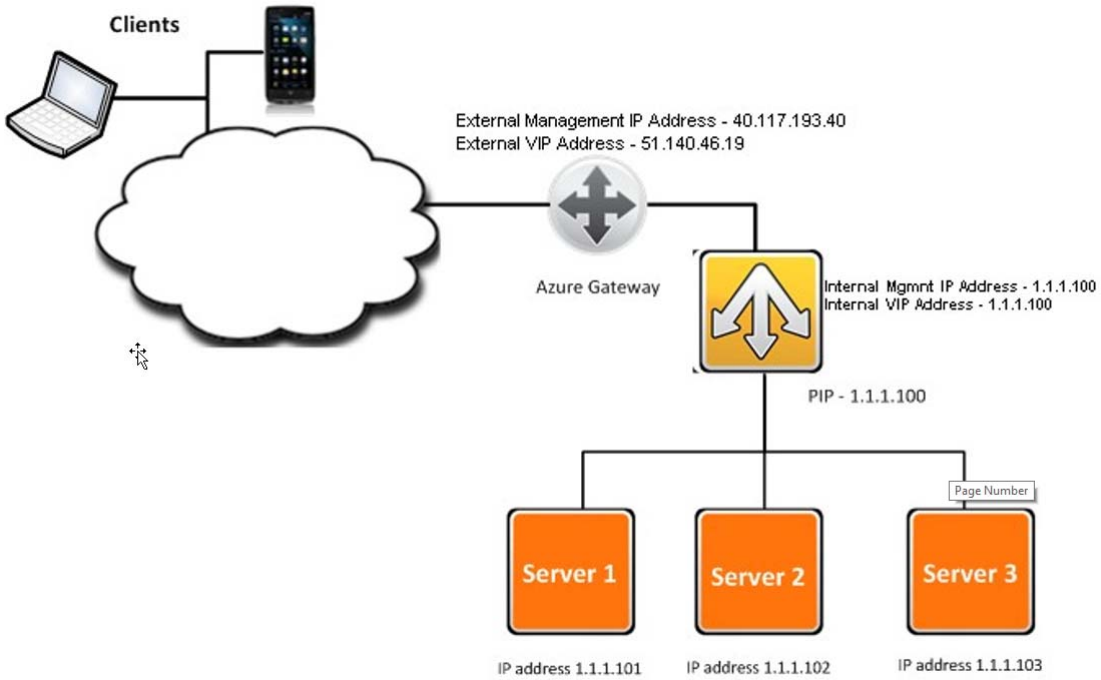
Prerequisites

- Knowledge of Microsoft Azure and deploying VMs on the Microsoft Azure cloud.
- Knowledge of Alteon Application Switch operating system.
- An existing Microsoft Azure account.

The Alteon VA Platform on Microsoft Azure

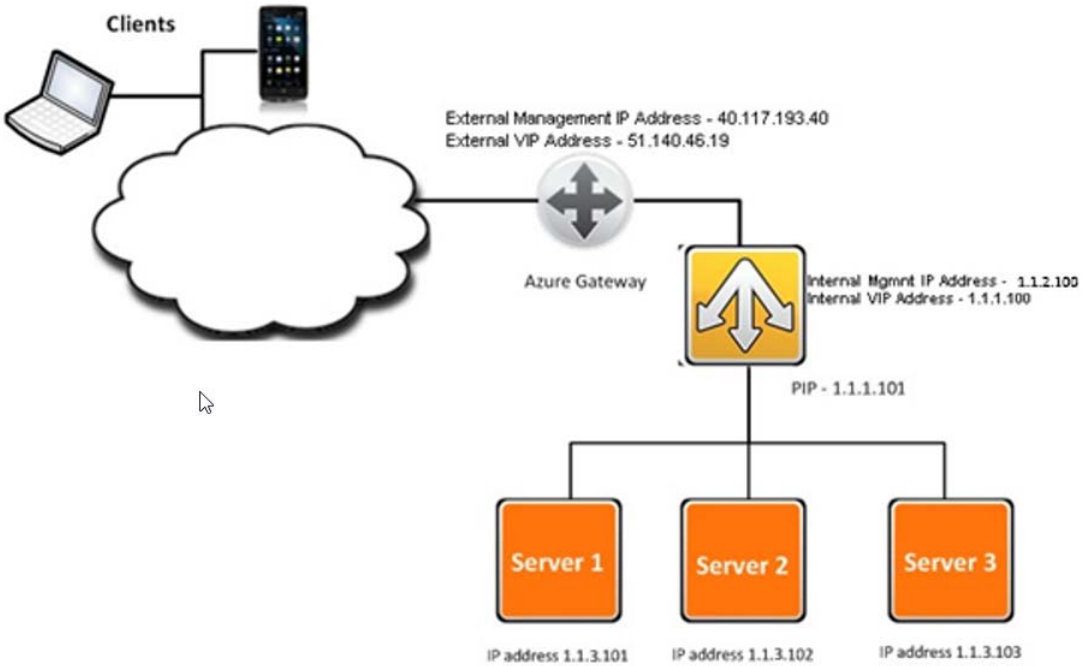
Alteon VA for Microsoft Azure cloud allows running your enterprise applications while tapping into Microsoft Azure computing resources and providing a common application delivery platform for your applications. Leveraging the common Alteon operating system across Microsoft Azure cloud and the enterprise data-center, enables faster application development cycles and improved economies for disaster recovery and seasonal application capacity scalability requirements. The figures below show a reference Alteon VA deployment on Microsoft Azure cloud in a single and in a multiple IP address mode.

Figure 1: Alteon VA configured to run in a single IP address mode



As shown in the figure above, the Alteon VA instance on Microsoft Azure cloud hosts a single IP address (1.1.1.100) for management, VIP and the PIP. For simplicity, and in order to avoid additional configuration, it is mandatory to configure a PIP when operating the Alteon VA on Azure.

Figure 2: Alteon VA configured to run in a multiple IP address mode



As shown in the figure above, the Alteon VA instance running on Microsoft Azure cloud is connected to two networks 1.1.2.0/24 as the management network and 1.1.1.0/24 as the data network. A different IP address is configured for the management interface, PIP and VIPs.

It is mandatory to configure a PIP when operating the Alteon VA on Azure.

CHAPTER 2 – DEPLOYING ALTEON VA ON THE AZURE CLOUD

This section describes deploying Alteon VA on the Azure cloud, and includes the following sections:

Minimum Requirements

The following table details the minimum hardware requirements for the various Alteon configurations:

Configuration	vCPU	GB RAM	GB Disk Space	Notes
Small Footprint (L4 SLB)	1	2	10	With this minimum footprint, Alteon VA can be deployed in Azure on small footprint instances, such as A1V2. This footprint can be used for workloads requiring only basic Level 4 load balancing. This supports reduced configuration capacity (1024 real servers, 4096 run-time health checks, 75 filters, and 128k L4 session entries).
Default	1	2.5	14	This is the default footprint of the Alteon VA image. It is recommended to increase the number of vCPUs to 2, especially in DPDK mode.
Recommended	2	4	14	This is the recommended minimal footprint for a full-featured Alteon ADC without integrated WAF. One vCPU is allocated for the management processor (MP) and one for the traffic processor (SP). With this footprint Alteon can be used for advanced Layer 7 processing as well as for capabilities that require DPDK, such as jumbo frames, and IPv6 BGP.
Alteon with integrated WAF (AppWall)	3	8	14	This is the recommended minimal footprint for a full featured Alteon ADC with integrated WAF. 1 vCPU and 4GB RAM can be allocated to AppWall, the rest to Alteon (1 MP + 1 SP).

Configuration	vCPU	GB RAM	GB Disk Space	Notes
Multiple SP Alteon	-	2 per SP	14	When configuring more than 1 vCPU, one is allocated for the MP and the rest for the SPs.

Notes

1. Additional factors that impact minimum RAM and disk:
   - If the allocated RAM is lower than 4 GB RAM the maximum number of virtual interfaces supported is 3. The first interface is used for management access and the rest are used for data.
   - If the allocated RAM is 4GB or higher, the maximum number of virtual interfaces supported is 8 for Azure environment.
   - To enable EAAF/IP reputation feature, you should add 1 GB to the RAM size and 4 GB to the disk size.
2. In order to minimize the latency while writing to the hard disk, it is recommended to use the Alteon VA local disk VM, and not a remote drive.
3. DPDK is automatically enabled for RAM size of 3GB or higher. It can be disabled manually, however, there are several capabilities, such as multiple SP support, jumbo frames, that are only available when DPDK is enabled.

High Performing System Requirements

You can achieve higher performance with Alteon VA by using NICs that support SRIOV and allocating multiple traffic processors (SPs).

Multiple SP capability is supported on Azure - when running on instances with accelerated network.

For further details refer to `https://learn.microsoft.com/en-us/azure/virtual-network/accelerated-networking-overview`

The maximum number of SPs that can be used depends on the number of DPDK queues available. In case of SRIOV this number is 2.

To overcome this limitation, you can define Traffic Distribution vCPUs (TDs). These TDs distribute the traffic to the SPs according to the number of cores allocated for Alteon processing, extending the CPU power for SSL offloading and Layer 7 processing.

When provisioning an Alteon VA with two vCPUs or more on a server with accelerated network, TD is enabled by default.

Single/Multiple Address Mode

Alteon VA when running on Microsoft Azure cloud can be configured either in a single IP address mode or in a multiple IP addresses mode (the common mode of work of an ordinary Alteon device). If you are using Alteon VA to manage a single service (single VIP) it is recommend to run in a single IP address mode.

When working in a single IP address mode, the system automatically configures itself to direct the management traffic to the management process. Virtual services and PIPs will also be automatically assigned the virtual machine IP address, with no further need to configure it. However, it is also possible to configure additional VIPs for more services.

Alteon VA can also operate in a Single IP mode with separate management network (NIC), when an additional NIC is added to the VA. In this case the public IP on the data network is used for Interface address, VIP address and PIP address.

When running in the Azure cloud, the Alteon VA is configured by default to run in basic single IP address mode.

In order for an Alteon VA to run in multiple IP mode, in addition to adding more NICs to the VA, you also need to configure Alteon to work in multiple IP address mode. For details see Deploying Alteon VA with multiple NICs.

Note: When the Alteon VA is not configured to work in a Single IP address mode but just a single network interface is attached to the VM running the Alteon VA, on every login to the system you will receive a notification message in the Web UI and will be prompted on the CLI to switch to Single IP address mode.

IPv6 Support

Alteon VA supports IPv6, however Azure support for IPv6 is limited. On a network interface you can only configure one private IPv6 address, and only as secondary IP address.

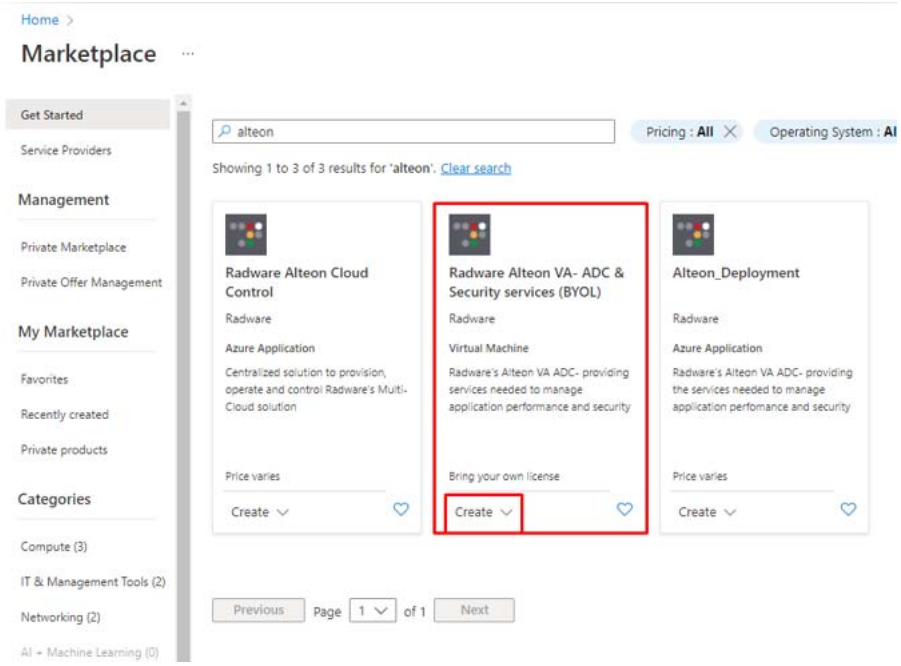
For details see `https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-network-interface-addresses?tabs=nic-address-portal#ipv6`

Deploying Alteon VA

In order to deploy the Alteon VA on the Azure cloud, you first need to log in to the Microsoft Azure portal at **`https://portal.azure.com/`**.

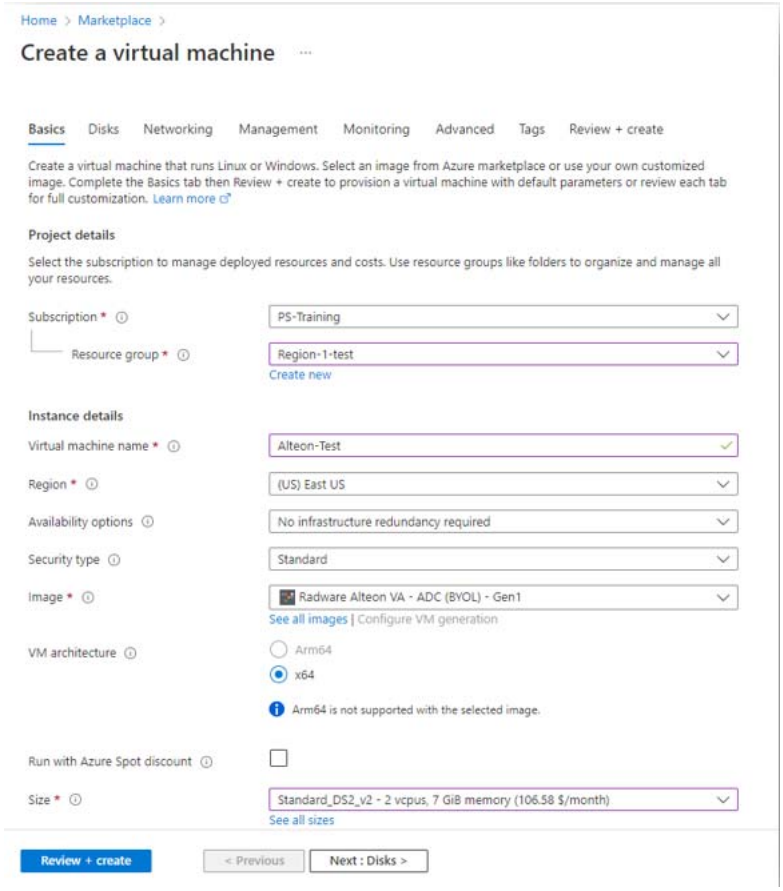
To deploy Alteon VA on the Azure cloud

1. Once logged in to your Azure account, access the marketplace, search for **Alteon**, and create a new Alteon instance from the *Radware Alteon VA- ADC & Security services (BYOL)* template.



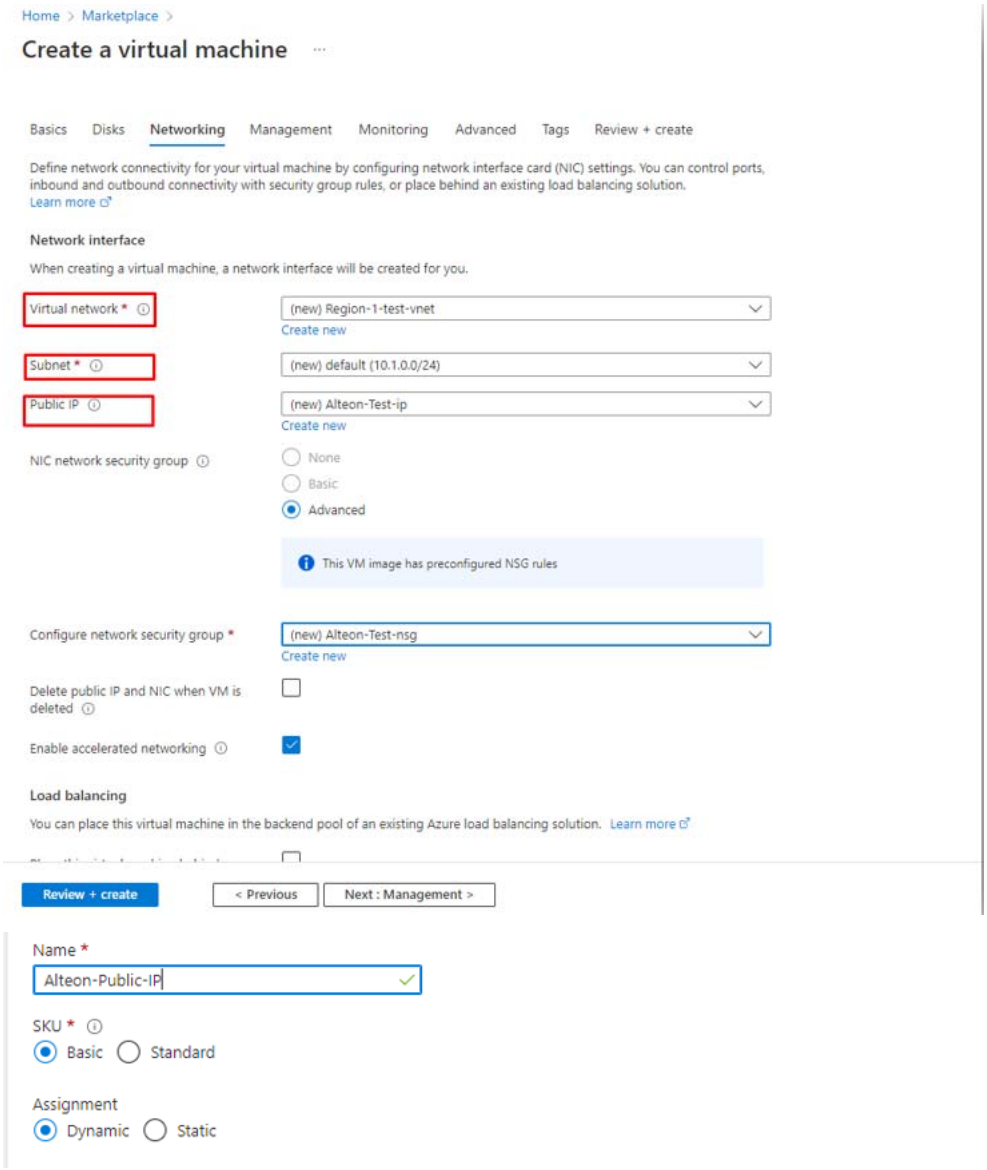
2. Provide the project details - Resource group, Virtual machine name, Region, Size, and click **Next**.

   Providing the authentication type is not required as Alteon has default credentials.



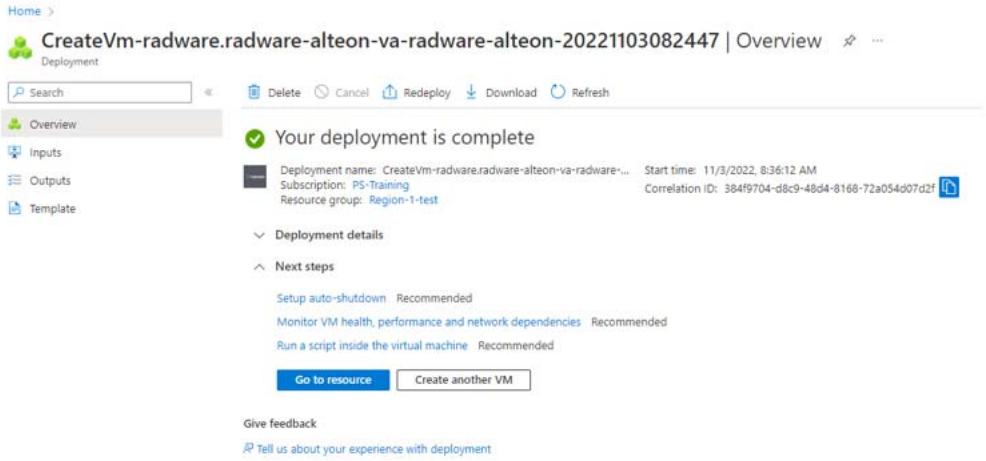
3. In the *Networking* tab, create or set your own virtual network, subnet, and public IP address (for public access).

Note: Ensure that for the public IP address you create a new public IP address of type **Basic**.



4. Default values are for the rest of the configuration, but you can edit them if required.

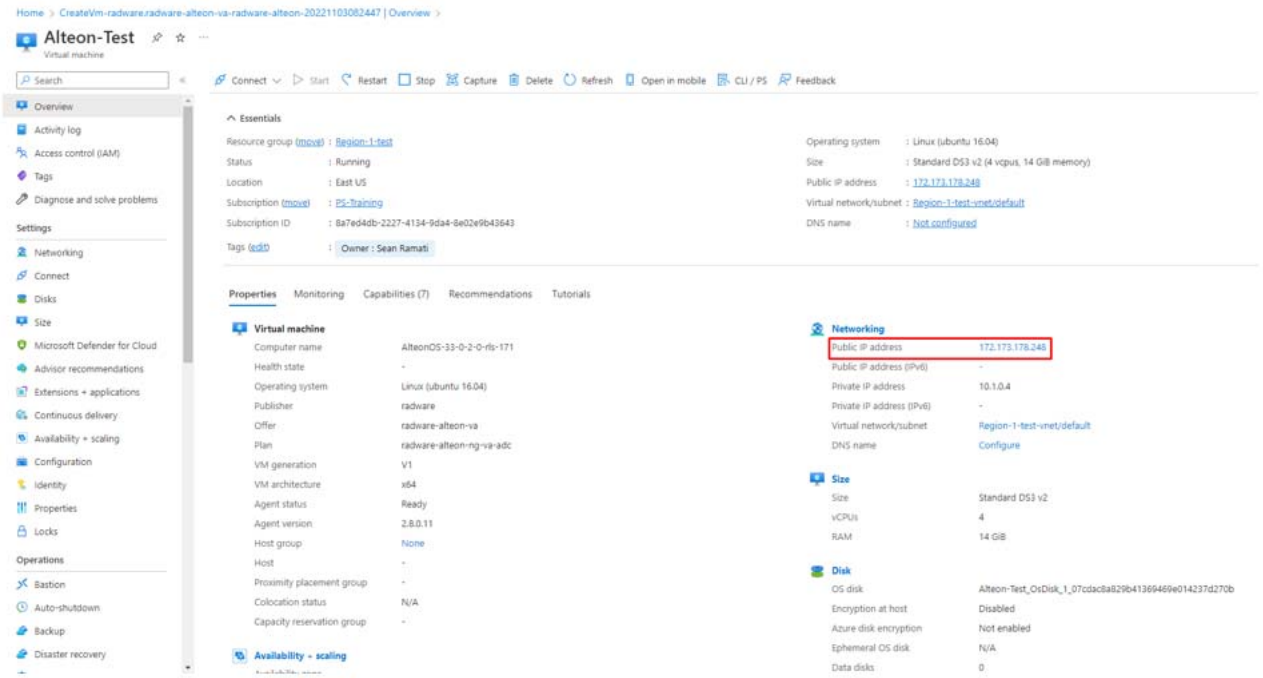
5. Review the configuration and create the virtual machine. After the deployment has been completed, click **Go to resource**.



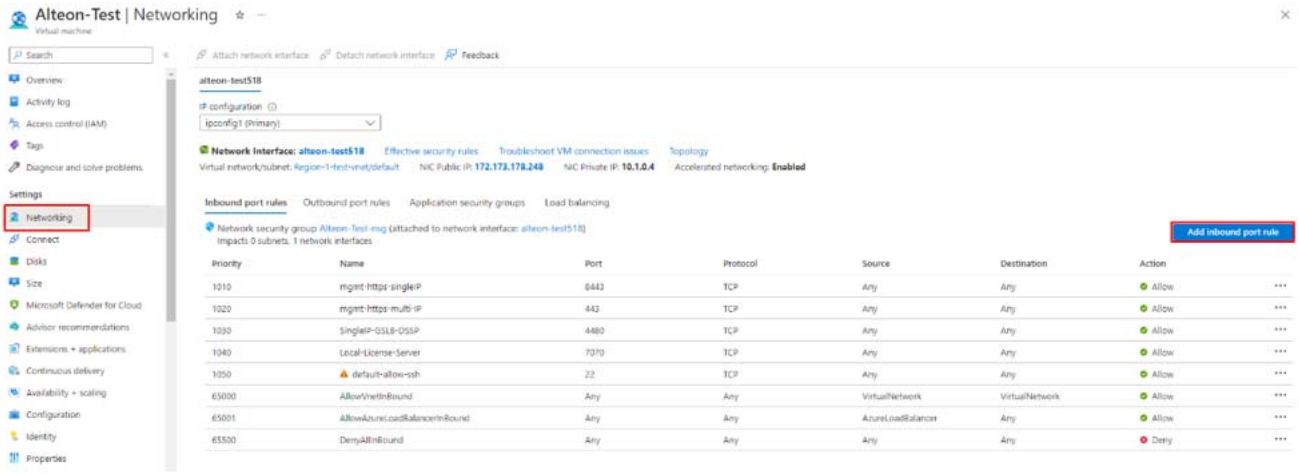
6. The *Virtual Machine Overview* tab includes the public IP address configured for the Alteon device.

   By default, the Alteon instance on Azure comes up in a single IP address mode. Where the public IP address is used as:

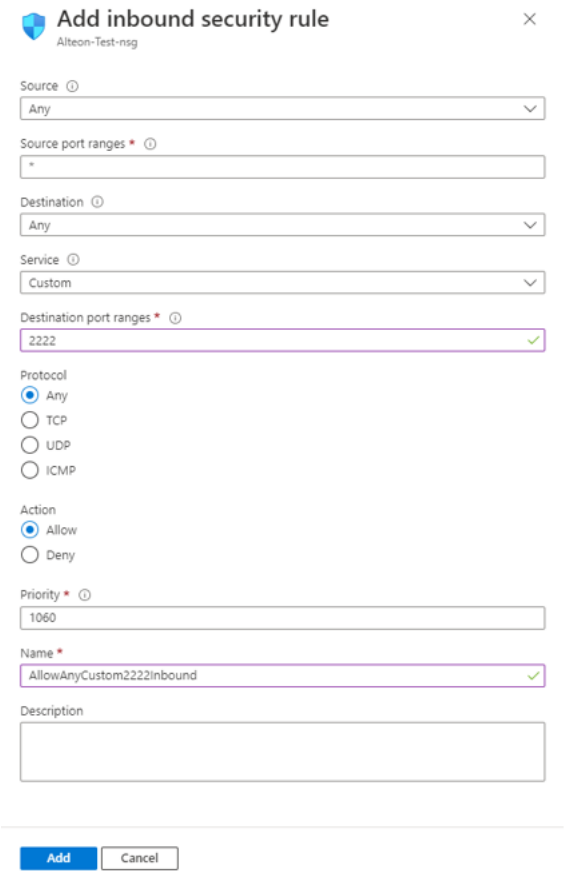
   — Management address
   — Interface address
   — VIP address
   — PIP address



7. Go to the *Networking* tab and check if the I*nbound port rules port 8443* (WBM access) and *port 2222* (SSH access) are defined.



8. If either of these ports is missing, add them to have full access to the virtual machine.



9. Connect to the Alteon device via WBM (**`https://<public-IP>:8443`**) or via SSH (**`<Public-IP>, port 2222`**).

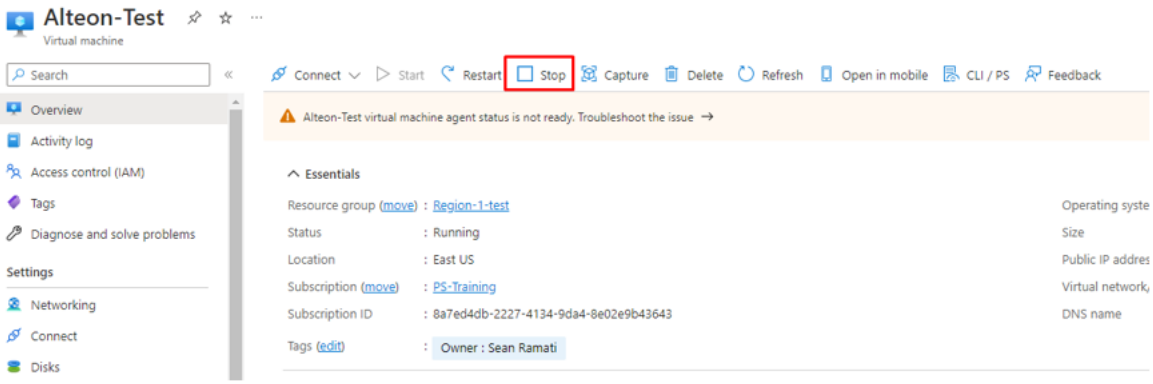
   The default credentials are **`admin`**, **`R@dware12345`**

Deploying Alteon VA with Multiple NICs

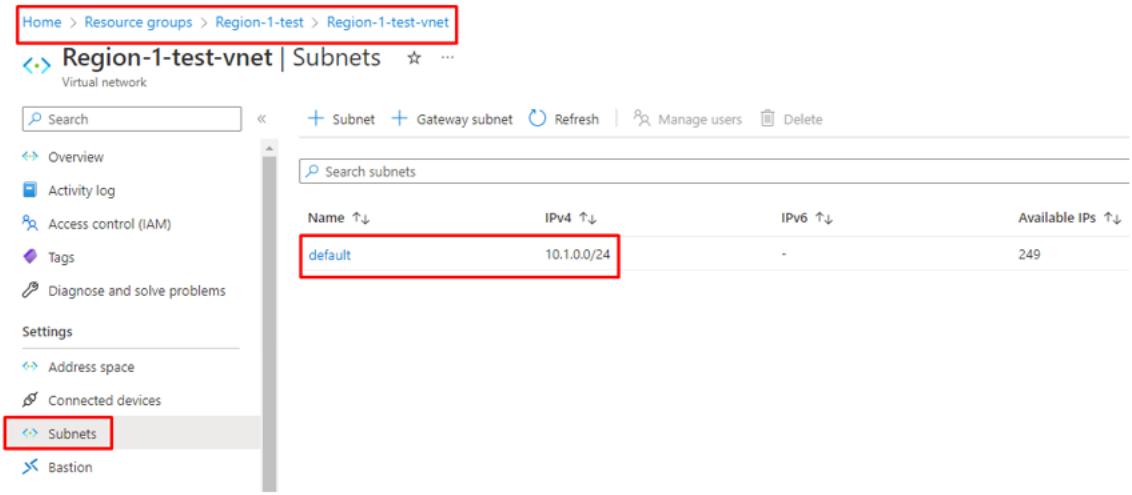
On Azure, the Alteon device works in single-IP mode with one NIC for management and data by default.

To add additional NICs

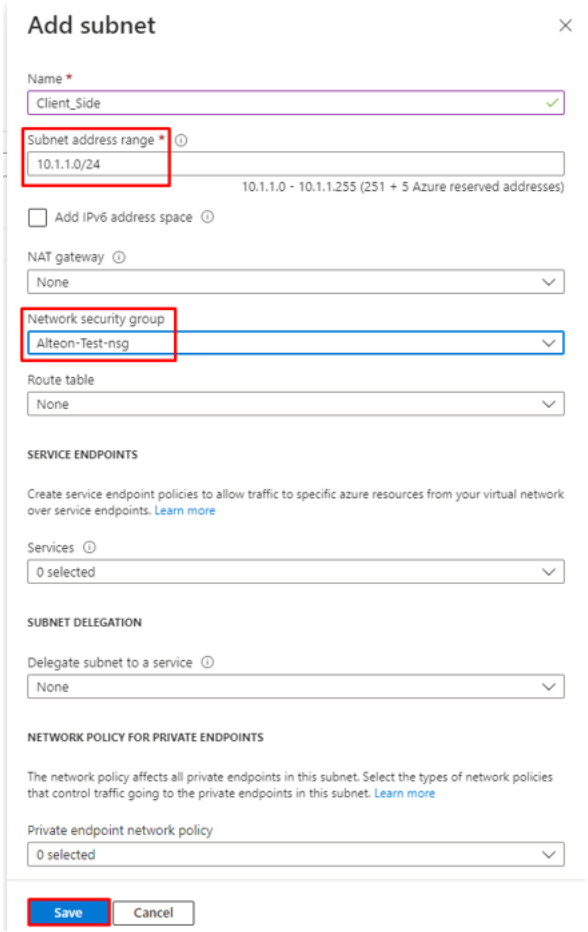
1. Shut down the virtual machine.



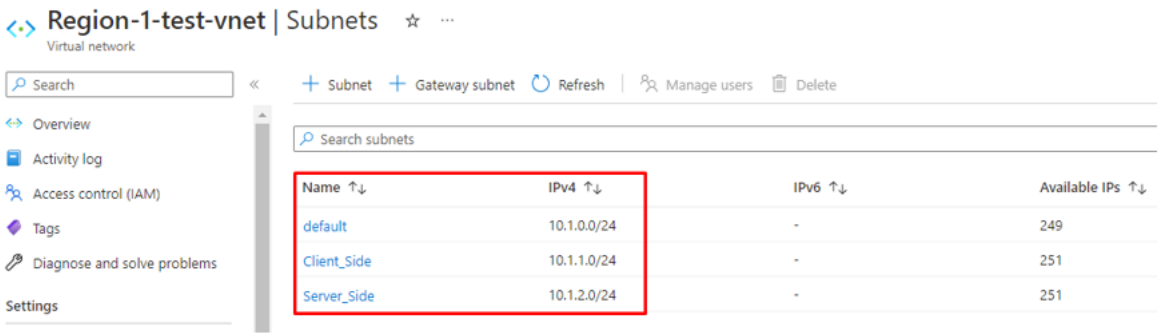
2. Before adding another NIC, to define a separate subnet for the new NIC, go to *Virtual Network* under the resource group and then go to the *Subnets* tab.



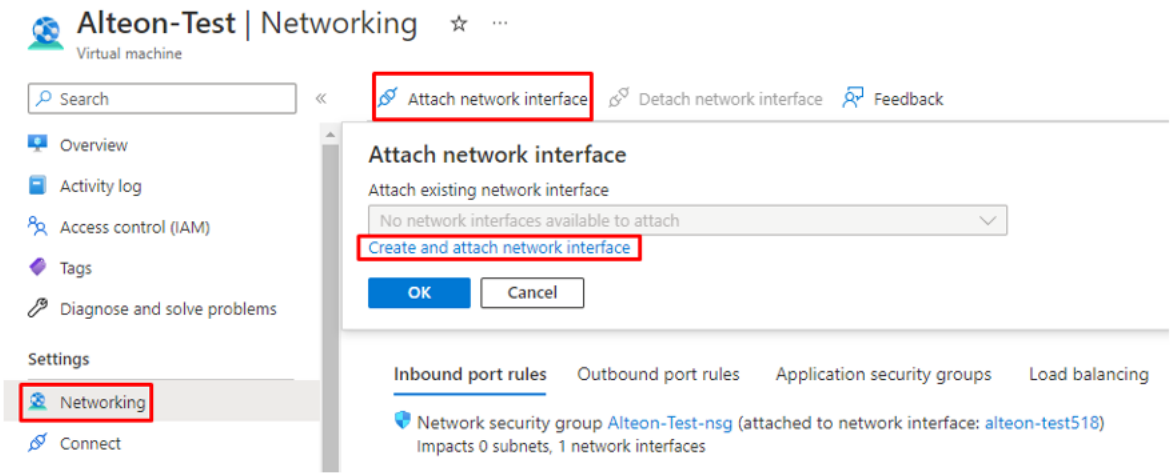
3. Add a new subnet and set the subnet address range and network security group and click **Save**.



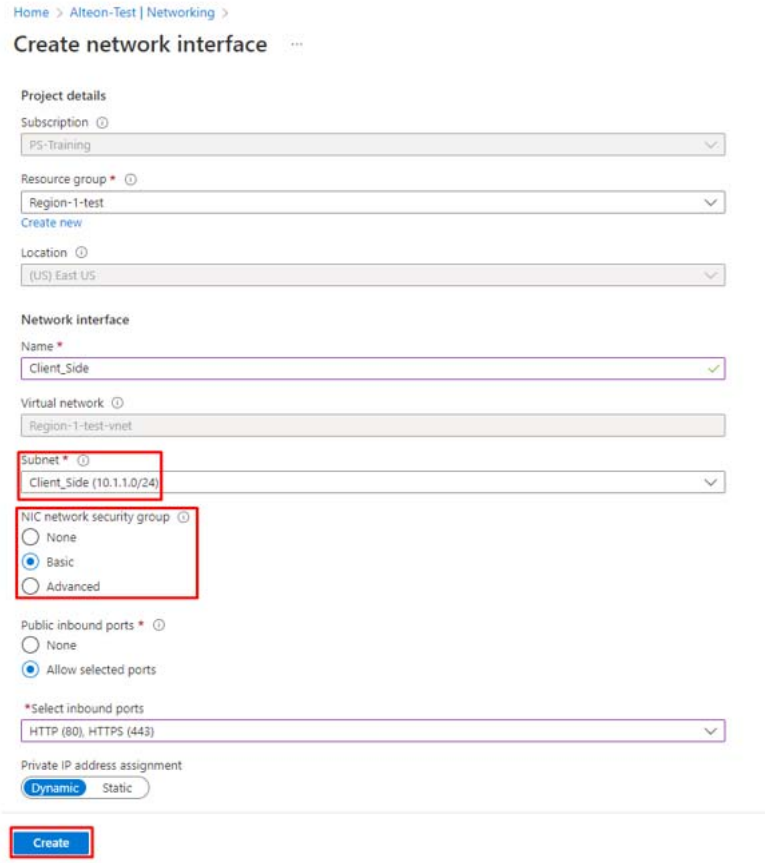
4. After configuring the subnets, you should have a configuration similar to the following:



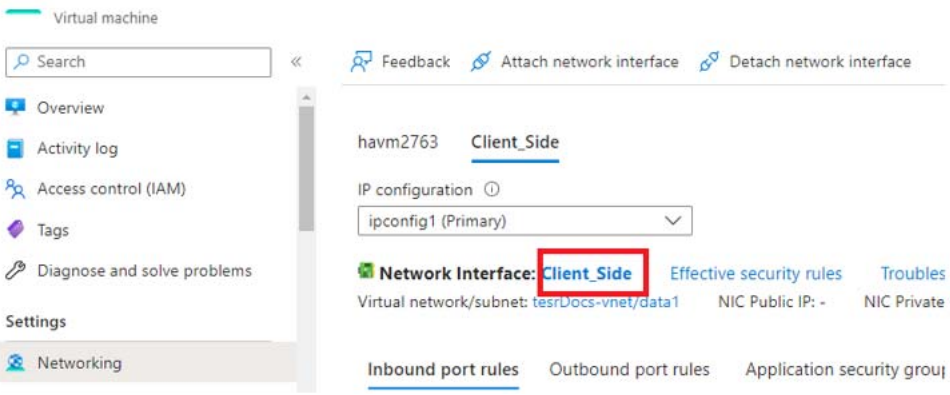
5. Go to the *Networking* tab, select **Attach network interface**, then click **Create and attach network interface**.



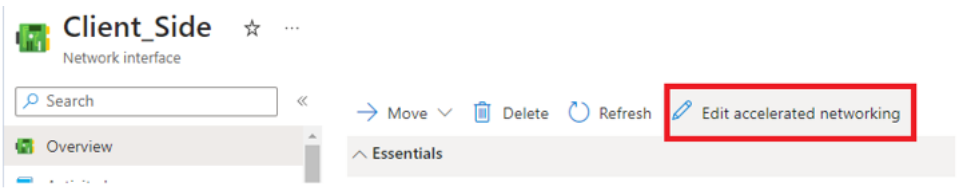
6. Set the name of the NIC and its subnet. In the *NIC network security group*, choose **Basic** or **Advanced** (**None** is not recommended).
When finished, click **Create**.



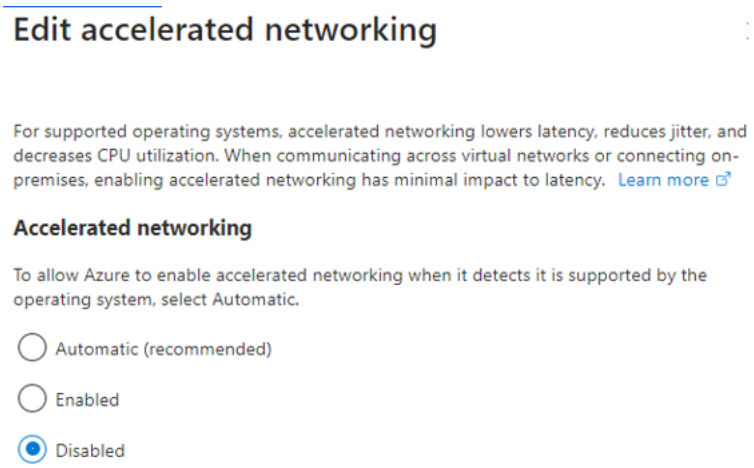
7. If the accelerated networking feature is enabled on the newly created NIC, you must disable it before turning on the Alteon device which is currently configured to boot in single IP address mode. The accelerated networking can be re-enabled after changing the Alteon VM to operate in multiple IP address mode.
   a. To disable accelerated networking, click on the name of the newly added NIC to edit the properties of the NIC



   b. Click **Edit accelerated networking**.



   c. If the feature is in enabled state, change it **disabled** and save the configuration.



8. To create as many NICs as you need, repeat steps 1 and 7 for each NIC.
9. If you have added more than one additional NIC, in order to operate in multiple IP mode:
   a. Turn on the Alteon device.
   b. Access it via SSH (port 2222) and log in (*admin/R@dware12345*).
   c. Run the command **`/c/sys/singleip dis`** to disable single IP mode.
   d. After pressing **Enter** you will be prompted to reboot the Alteon VA.

10. Wait for the Alteon device to reboot and test your connection via SSH (port 22) or WBM (`https://<alteon-IP>`)
11. To re-enable the accelerated networking on the data NICs, shutdown the Alteon device once again and enable accelerated networking using the azure portal configuration mentioned in step 7 above. Then turn on the device again.

Notes

- If you are configuring the Alteon VA to run in High Availability (HA) mode you should enable the high availability advertisement ports for UDP, port 2090 as inbound and port 2091 as outbound.
- If you are using the Local License Server within your virtual network, you should set the security group rules for the ports that it communicates with the Alteon. If you use the system defaults, the security rules should be: inbound http port 7070.

Obtaining and Installing a License

By default, a new Alteon VA instance has Deliver capabilities license and 1 Mbps throughput license.

There are two options to acquire and install appropriate capabilities and capacity licenses:

- GEL (Global Elastic License) entitlement.

  The Alteon Global Elastic License (GEL) provides an ADC purchasing model that cuts costs eliminates planning risks, ensures complete agility in deploying ADC services wherever and whenever you need them, and with any number of ADC instances you need, limited only by the total ADC capacity you purchased for your entire organization. For instructions on GEL license installation on Alteon see Alteon VA Installation Guide.
- Purchase individual permanent Alteon VA license/s. Combined with the three capabilities packages (Deliver, Perform, Secure), a wide range of throughput license options are available for Alteon VA, starting from 200 Mbps.

Note: Since the Alteon VA license is generated based on the VM MAC or IP addresses, generating the license based on the VM IP address and having the IP address being static, prevents the license from becoming outdated.

To obtain a permanent license, the device management IP address or MAC address is required. Once the Alteon instance is up and the necessary information is available, follow these steps:

To obtain and install a permanent license

1. Log in to Radware Customer portal and select **Tools > VA License Generator**.
2. Search in your VA inventory for the **Serial Number** you want to use for this instance.
3. Click **Generate License**.
4. In the pop-up window enter the MAC address or IP address of the VA instance and click **Generate License**. The list of license strings for this serial number appears.
5. To install the license via Web UI:
   - Login to the Alteon VA instance via HTTPS.
   - Select **System > Licenses**.

- Enter the first license string from the list and click **Set License**.
- Repeat for each license string in the list.

6. To install the license via CLI:
   - Login to the Alteon VA instance via SSH or Telnet.
   - Enter the CLI command /oper/swkey license_string, where *license_string* is the first license string from the list.
   - Repeat for each license string in the list.

Notes

- When deploying a VM from a snapshot, the MAC address of the virtual machine changes and the license becomes invalid. For the VA to operate properly, you must either get a new VA license with the new MAC address or manually set the old MAC address on the new VM.
- If the VA license expires, the SLB traffic will be limited to the default throughput of 1 Mbps, even if there is a separate throughput license with higher limit installed.

CHAPTER 3 – CONSIDERATION FOR CONFIGURING ALTEON VA ON AZURE

Alteon VA for Azure can be accessed through the following user interfaces:

Web Interface

Alteon VA, when running on Microsoft Azure, is configured to have its management controlled through the data path. This is due to the fact that any instance on Microsoft Azure is provided with a single IP address per network interface.

In order to enable load-balancing HTTPS traffic and management access, the HTTPS port for management access is changed to 8443.

To access the Alteon web interface, open your browser and enter the Alteon VA instance IP address with port 8443.

For example, if the Alteon VM IP address is 1.1.1.1, enter `https://1.1.1.1:8443`

To log in, enter the default username and password: **admin**, **R@dware12345**

Note: If you do not intend to load balance HTTPS traffic, you can change the HTTPS port for management purposes to the standard HTTPS port 443 through the Web interface at: **>Configuration>System>Management Access>Management Protocols** or through the CLI command: **/c/sys/access/https/port**.

CLI Interface

To connect to Alteon VA through the command line interface (CLI), connect to Alteon VA port 22 using any terminal emulator supporting SSH (such as PUTTY).

Enter the default username and password: **admin**, **R@dware12345**

The CLI main menu is displayed.

It is strongly recommend you change the password on your first login.

Cloud Init

You can deploy a pre-configured Alteon VA using the cloud-init feature.

Refer to the *Alteon VA Installation Guide* for details of the Alteon VA cloud-init support.

CHAPTER 4 – CONFIGURING ALTEON VA ON THE AZURE CLOUD

This chapter describes how to configure your Alteon VA on the Microsoft Azure cloud.

Enabling HA Mode in the Microsoft Azure Cloud

Alteon VA supports HA mode in the Microsoft Azure cloud.

Notes

- Alteon VA running on the Azure cloud only supports the Switch HA mode.
- Both peers should reside in the same resource group.
- The configuration and backend operations for HA are different in Single IP Address mode and Multiple IP Address mode.

Alteon in the Azure cloud can be configured to work in standard HA mode with a pair of master and backup VA platforms. With one configured as master and the second as backup, they both have a private IP address for internal Azure access. Should the master Alteon VA fail, the backup takes over, replacing the failed platform and becoming the master.

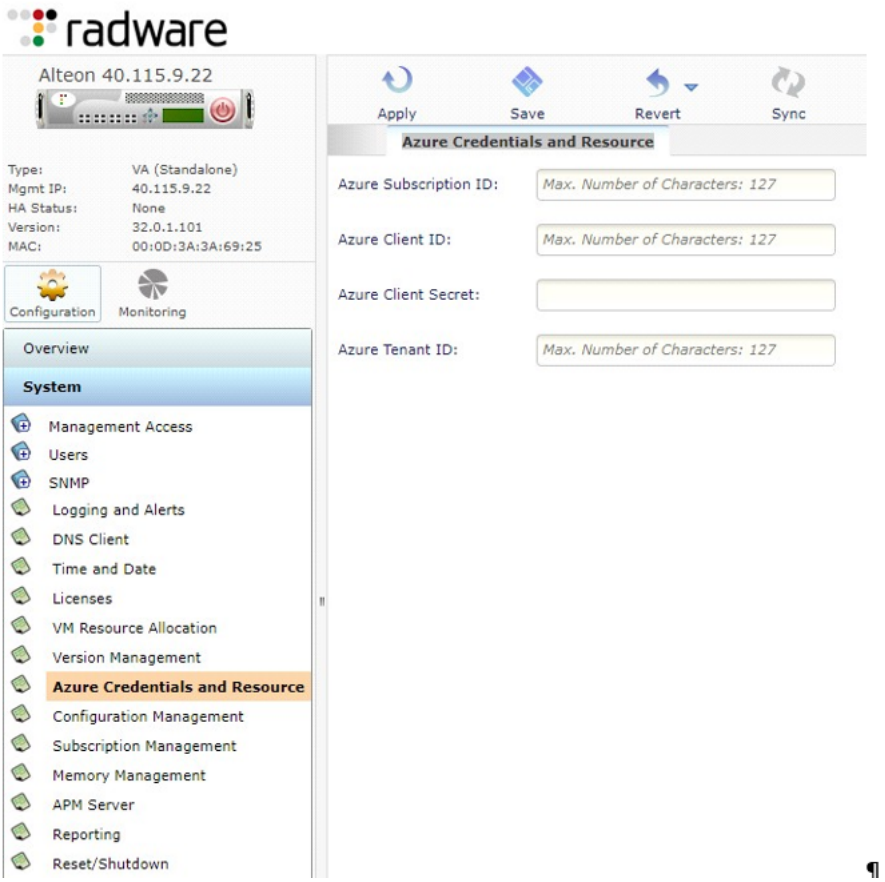
Alteon in the Azure cloud can be configured to work in standard HA mode with a pair of master and backup VA platforms. With one configured as master and the second as backup, they both have private IP addresses for internal Azure access. Should the master Alteon VA fail, the backup takes over, replacing the failed platform and becoming the master.

Based on the address mode (Single IP or Multiple IP), the relevant public IP addresses are also transferred to the new master Alteon VA during fail-over, as explained in detail below.

To enable the transfer of the master public IP address to the backup, Alteon should have access to the Azure account. So, for the Alteon VA to work in HA mode, you must ensure that the Azure credentials are configured on Alteon device. Azure credentials include the following fields: subscription ID, client ID, client secret, and tenant ID.

To retrieve the credentials, See Generating and Retrieving Alteon VA credentials on the Azure Portal, page 45

The Azure credentials are configured in the Web UI at: **Configuration > System > Azure Credentials and Resource**.



Configuring HA mode in Single IP Address Mode

Every Alteon VA running on Azure has its public IP address for access from clients that are outside the Azure cloud, or for accessing the Alteon for management purposes from outside the Azure cloud network. Since the IP addresses tend to change between reboot of the VM, you should configure both the public and private IP addresses to be static.

Since the Azure cloud does not have the provisions to support floating IPs, which is essential in an HA environment, you cannot have two instances with the same IP address, where just one of them will be active. Alteon must therefore transfer the public IP addresses among the VMs.

The primary IP address must be configured to be attached to the public IP address of the master VA of the Alteon VA HA pair and will act as the floating IP address.

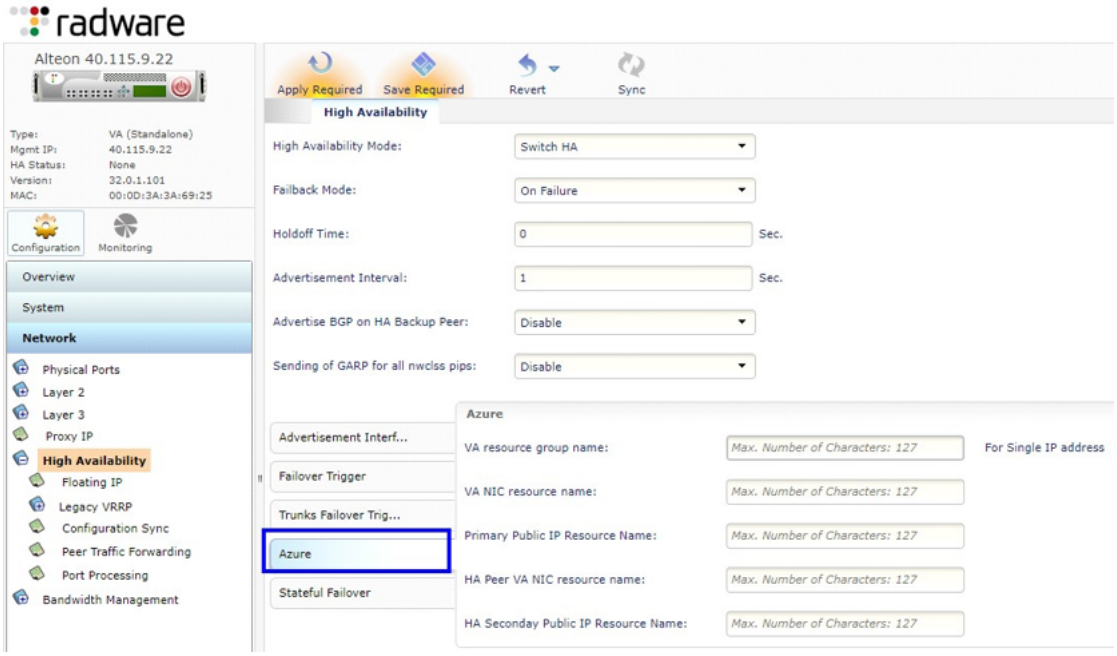
When there is a failure in the master, and a failover to the backup occurs, the public IP addresses are swapped so that the primary IP (the floating IP address), is now attached to the backup (now new master) platform to support the failover.

The following information must be configured for transferring the public IPs during failover.

- The resource group of both Alteon platforms (master and backup).
- The NIC resource name of the Alteon instance you are configuring.
- The resource name of the primary public IP address. (Basically, this public IP address acts as the Floating IP address. Always the Master Alteon VA should hold this IP)

- The NIC resource name of the peer Alteon instance.
- The resource name of the secondary public IP address. (This public IP address is attached to backup Alteon VA, through which the backup Alteon can be accessed for management purposes from outside the Azure cloud network.)

The above parameters should be configured, on the primary device, at: **Configuration > Network > High Availability** in the *Azure* tab.



You can enter the CLI command **`info/sys/azureip`** to display the Azure VM public IP information.

After defining the Azure resources on the primary device, the following is performed:

1. The primary public IP address is assigned to the Master Alteon VA VM resources and the secondary public IP address to the backup Alteon VM.
2. Data is synchronized with the peer. The peer will transpose the information between the peer and the VM NIC data.

If a failover occurs, the backup Alteon master swaps the public IP resources of the two Alteon platforms to take control.

For example, for VM1 (Name - Alteon1, Public IP name - Alteon1-IP) and VM2 (Name - Alteon2, Public IP name - Alteon2-IP), where Alteon 1 is currently the master. In the event of a failover, the normal failover process is being processed. In addition, it swaps between the public IP of Alteon1 and of Alteon2.

It will remove Alteon1-IP resource from Alteon1 and remove Alteon2-IP resource from Alteon2. It will then swap the public IP addresses, attach Alteon1-IP resource to Alteon2 and attach Alteon2-IP resource to Alteon1.

Now you can configure the Alteon VA to work in HA. Refer to the *Alteon Application Guide*.

Note: It takes up to 2 minutes for the public IP to transpose in case of failover

Configuring HA mode in Single IP Address Mode with Multiple Virtual Servers

By default, virtual server 1 is automatically configured along with enabling single IP Address mode with the virtual IP address (VIP) same as the IP address of interface 1.

The HA configuration mentioned in the above session is for Single IP Address mode with default configuration.

The limitation with default configuration is that the user cannot modify the VIP address of virtual server 1, as it must be same as the IP address of interface 1. Due to this, the user cannot configure the same VIP address for the Alteon VMs pair in the HA configuration for virtual server 1.

Since the VIP addresses are different, session mirroring is not supported for virtual server 1 in the single IP Address mode.

If session mirroring support is required, additional virtual servers need to be configured manually. In this case, more configuration is required for failing over the new VIPs to the master Alteon device. This is additional to the HA configuration mentioned above for single IP address mode.

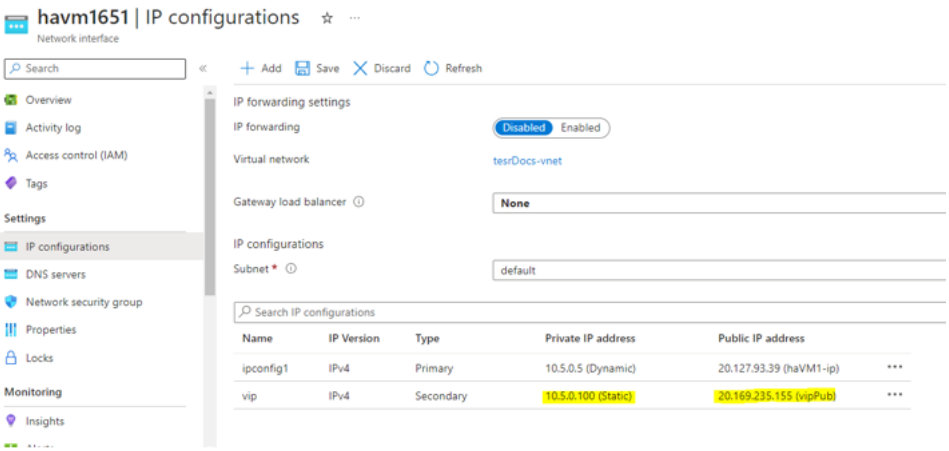
Given below are the extra configuration required for the additional VIPs.

- Configuration in Azure portal:

  Add the below configuration only for the Alteon HA master VM.

  — Add the secondary IP address same as the internal VIP address (statically assigned) to NIC

  — Then attach the VIP public IP to the secondary address



- Configuration in Alteon:

  Web UI support is not available currently for this configuration.

  The following configuration needs to be done using CLI menu:

  — /c/sys/azure/multipha <NIC name>

  pnicid <peer NIC name>

  add <internal IP address>

  — <NIC name> is the NIC resource name of the Alteon instance you are configuring.

  — <peer NIC name> is the NIC resource name of the peer Alteon instance.

  — <internal IP address> is the internal VIP address configured.

  — If more than one VIP is manually configured, the user needs to add all the internal VIPs one by one.

Configuring HA mode in Multiple IP Address Mode

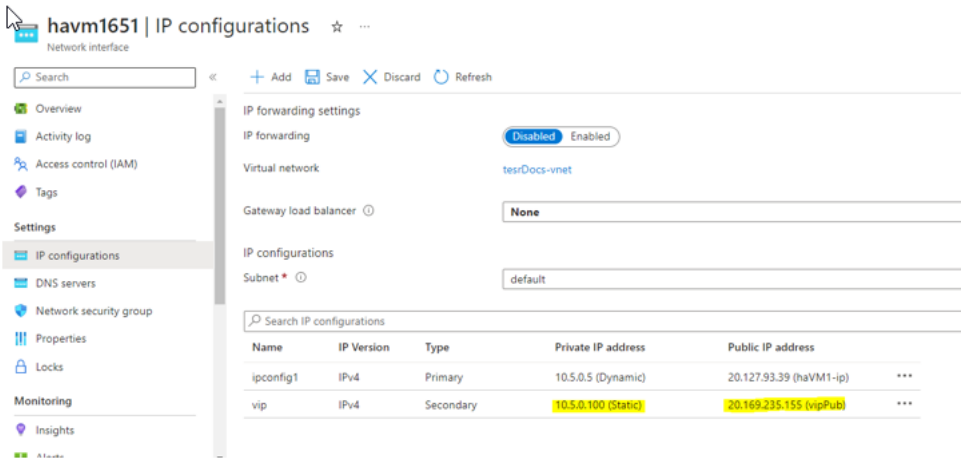
In Multiple IP address mode, the internal IP address and public IP address of all the VIPs are attached only to the data NIC of master Alteon Device.

During the failover process, the pair of internal IP and public IP of VIPs are transferred to the relevant NIC of the new Alteon master device.

Azure credentials must be configured as explained above for transferring the IPs from backup to the master Alteon Device.

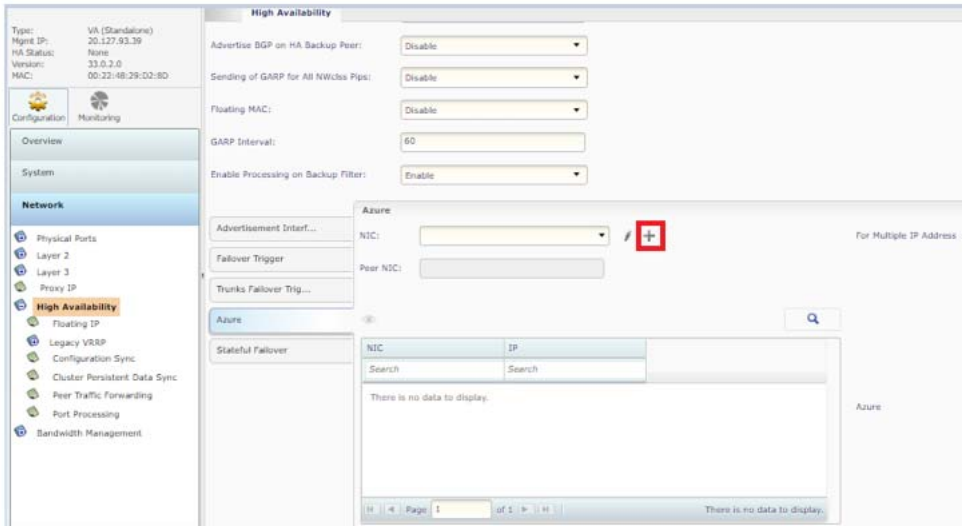
Also given below are the configurations required in Azure portal and in Alteon devices for enabling HA mode in Multiple IP address mode.

- Configuration in Azure portal:
  - Add the configuration only for the Alteon HA master VM.
  - Add the secondary IP address same as the internal VIP address (statically assigned) to relevant data NIC.
  - Then attach the VIP public IP to the secondary address.

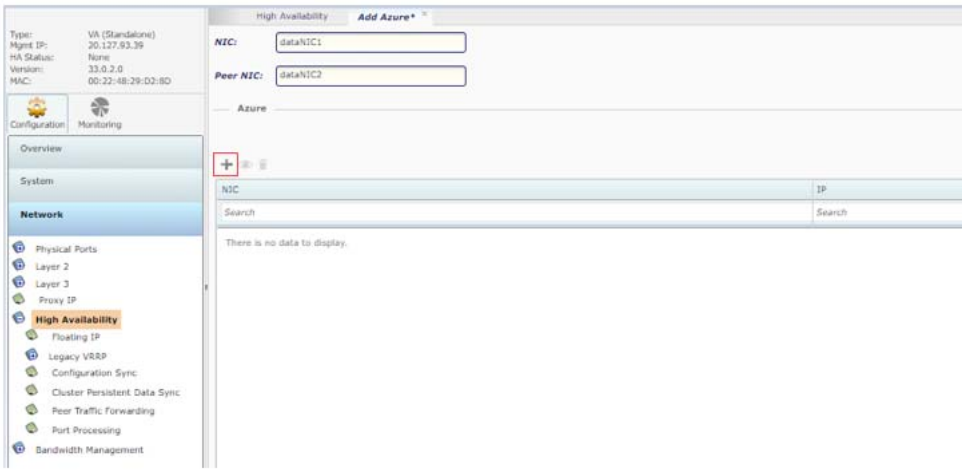


  - If more VIPs are configured in the Alteon device, add all of them as secondary IPs of the NIC and attach relevant public IPs to each internal IPs of VIP.
- Configuration in Alteon:
  - Configure the Azure resource name of the Alteon data NIC.
  - Configure the Azure resource name of the peer Alteon data NIC.
  - Configure the internal IP address of the VIP (since the internal IP and public IP addresses are moved as a pair to the new Alteon Master, configuring only the internal IP is sufficient).
  - If multiple VIPs are configured, add internal IP of all the VIPs.
  - The above parameters should be configured at: **Configuration > Network > High Availability** in the *Azure* tab.

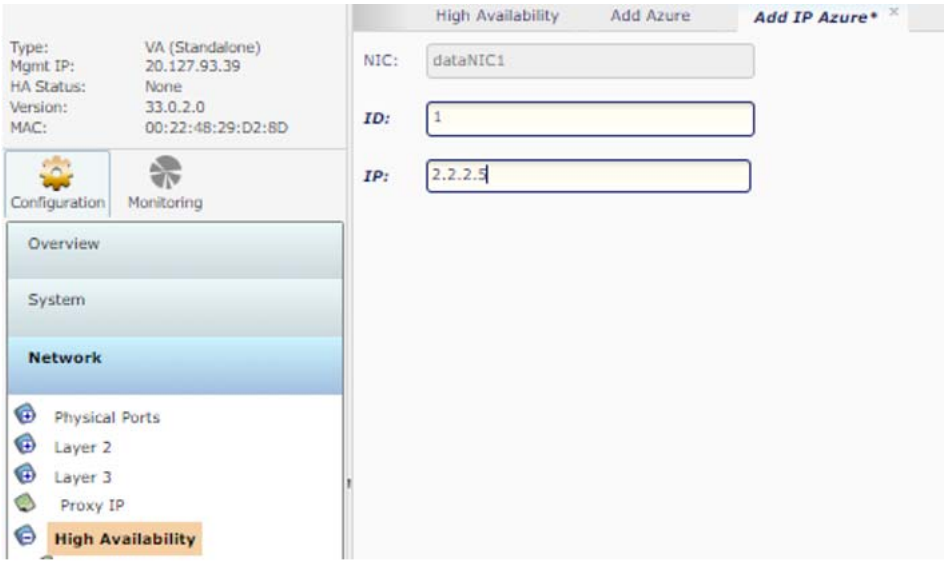
— Add new NIC configuration using the **+** button.



— Enter the NIC resource name and peer NIC resource name. Then click on the + button the add internal VIP addresses associated with the NIC.



— Add internal VIP addresses one by one.



Basic Load Balancing Configuration

Once you access the Web interface (as described above) you can configure your Alteon VA on the Azure cloud to load balance between servers, performing the following steps:

- Configure the real servers
- Configure the servers group
- Configure the virtual servers

The following sections provide a step-by-step guide to perform these configurations.

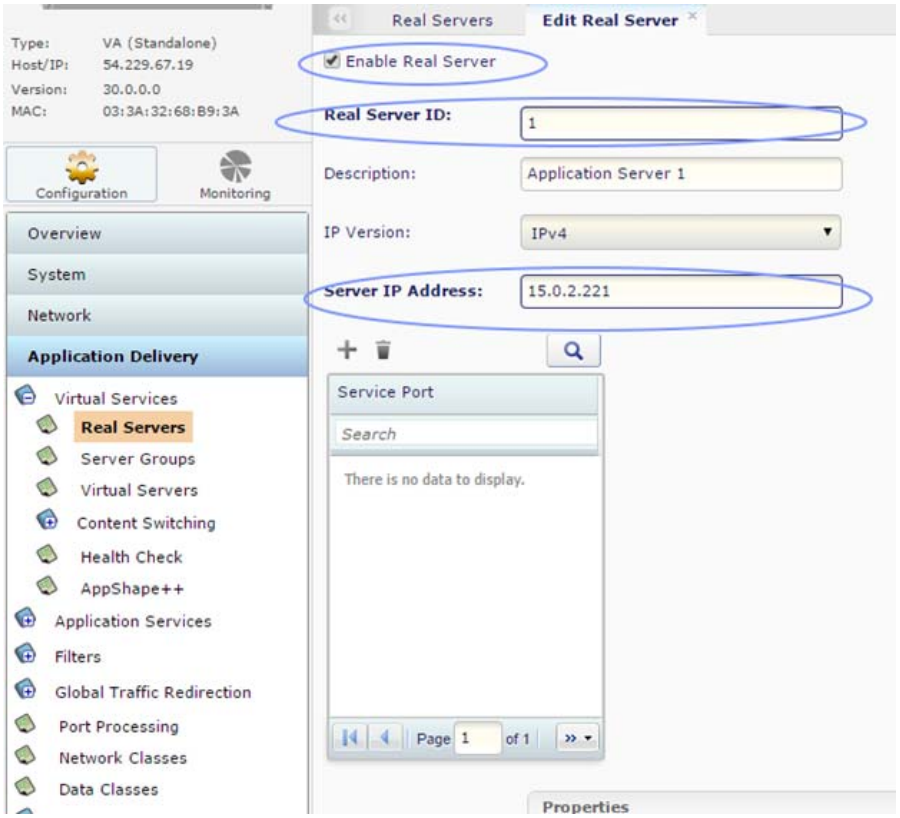
Note: For more enhanced capabilities, refer to the *Alteon Application Guide*.

Configuring the Real Servers

You need to first configure the real servers.

To configure the real server

1. In the Web interface, navigate to: **Configuration > Application Delivery > Real Servers**
2. Enter the real server ID.
3. Enter the real server IP address.
4. Click the checkbox to enable the real server.
5. Define the service ports and the additional parameters as required.
6. Press **Submit**.
7. Repeat all the above steps for all your real servers.

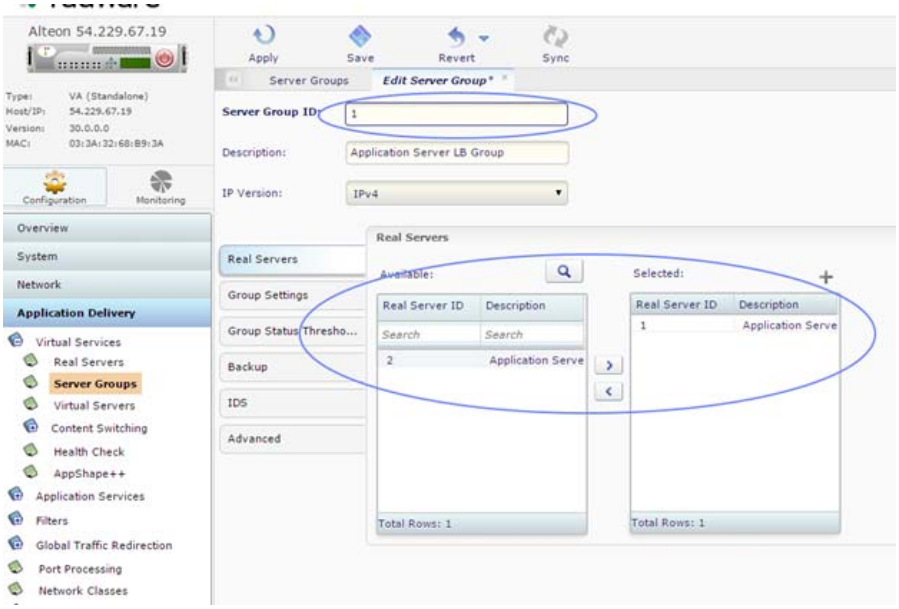


Configuring the Real Server Group

You can now configure the real server group.

To configure the real server group

1. In the Web interface, navigate to: **Configuration > Application Delivery > Server Groups**
2. Click **+** to create a new group.
3. Enter the group ID.
4. Enter the group description.
5. Mark the real servers in the **Available** area on the left and click the right arrow button to select them.
6. If there is a need to change the system defaults, modify any parameters as required.
7. Click **Submit**.

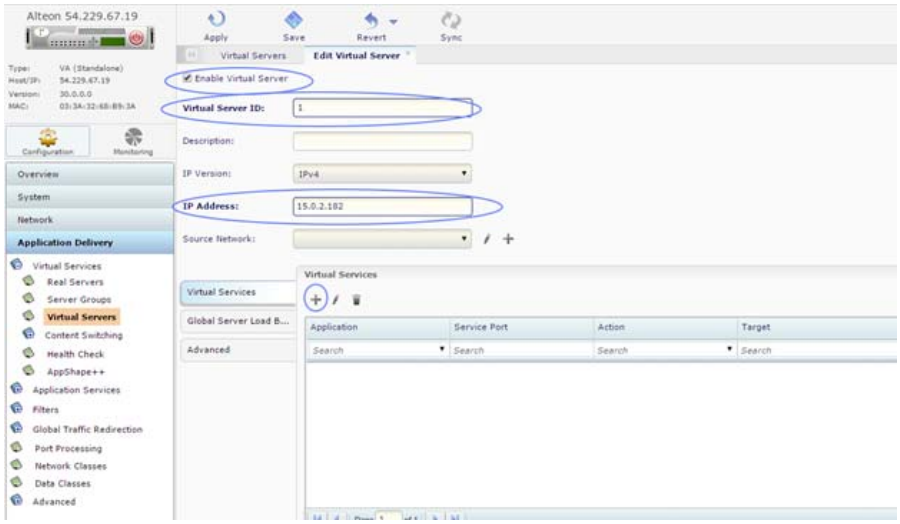


Define the Virtual Server

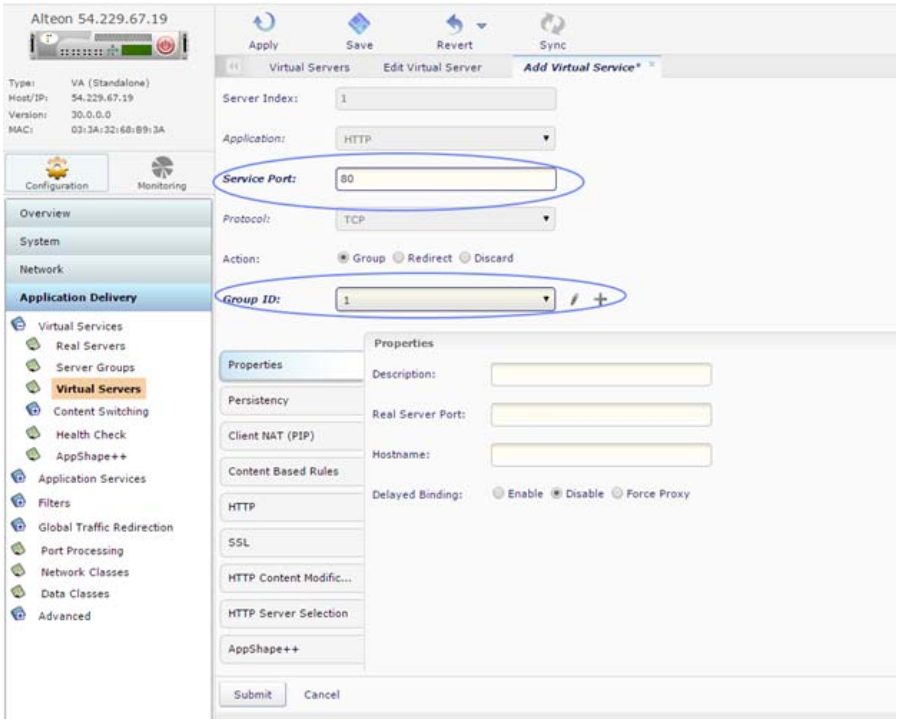
You can now configure the virtual servers.

To configure the virtual server

1. In the Web interface, navigate to: **Configuration > Application Delivery > Virtual Servers**
2. Click **+** to create a new virtual server.
3. Enable the Virtual Server by clicking **Virtual server ID**.
4. Enter the Virtual Sever ID.
5. The virtual server IP address is automatically assigned to be the same as the virtual machine IP address.



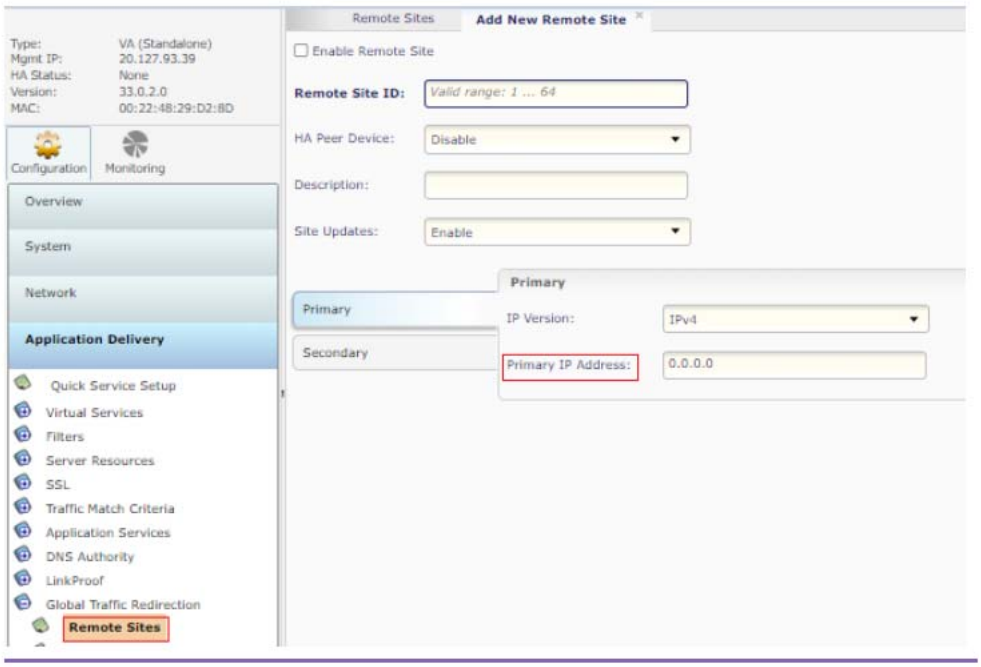
6. In the *Virtual Services* tab, click **+** to add a real servers group.
7. Enter the service port.
8. From the group ID drop down list, select the real servers group.
9. If you need to change the system defaults, modify any parameters as required.
10. Click **Submit**.



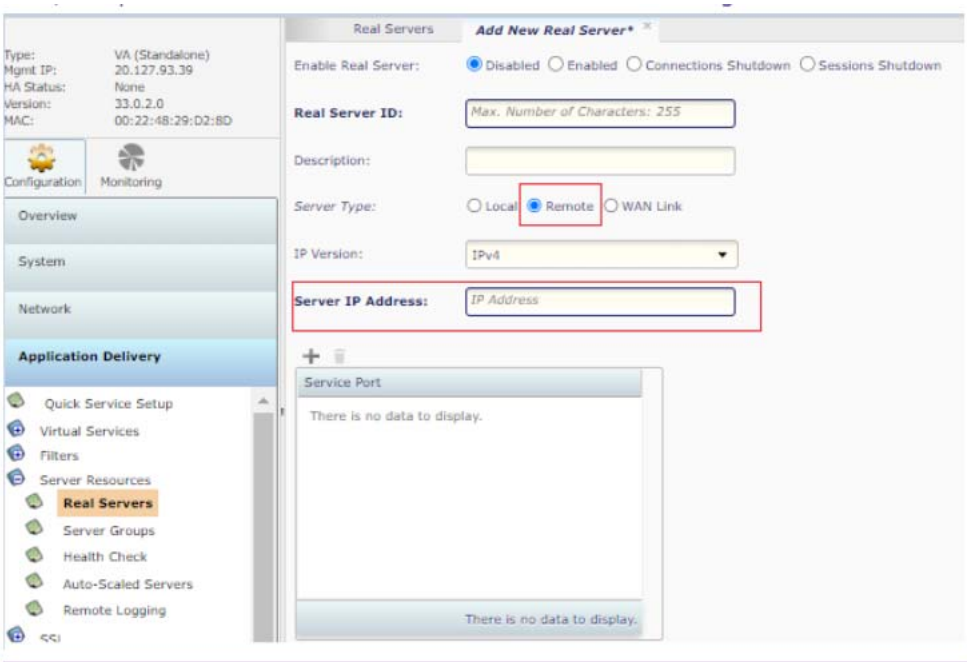
11. Click **Apply** to apply all the above changes.

GSLB Configuration

The public IP address of the remote VIP must be configured as the remote site address (for both primary and secondary switch IP address of the remote site) for the GSLB



Also, the public IP address of the remote VIP must be configured as the remote real server address.



GSLB Configuration for Single IP Address mode

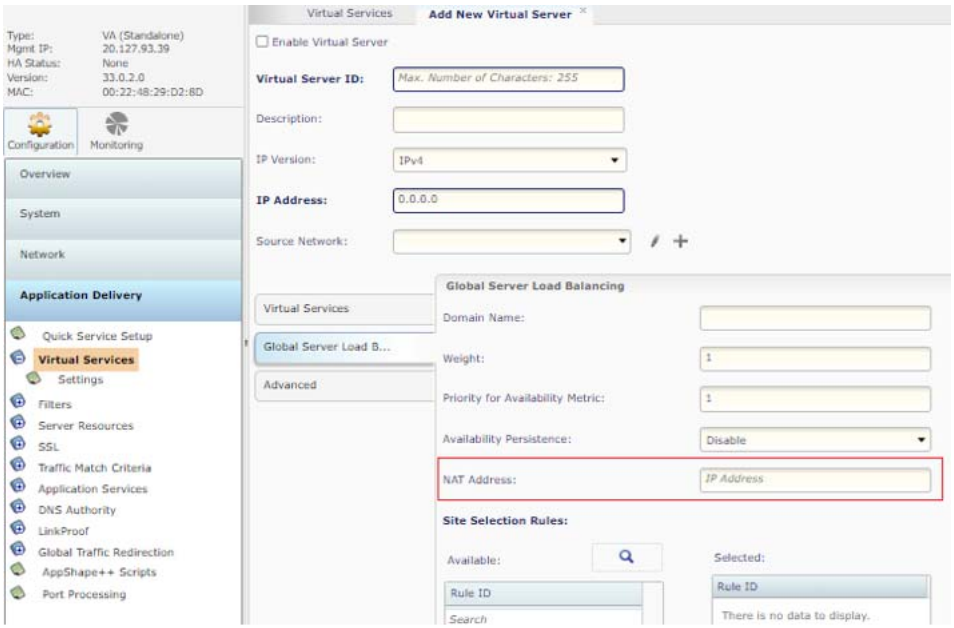
Following are the specific changes added in Single IP address mode for supporting the GSLB.

- The port for DSSP messages is changed from port 80 to port 4480 internally.
- For a DNS query, if the local VIP is found as the best site, the DNS response is modified to use public IP instead of the internal IP address.
- The public IP of the local VIP is automatically fetched from the Azure portal. To fetch the IP from the portal, the Azure credentials and resource names must be configured as described in session for *Configuring HA mode in Single IP Address Mode*.
- There is no separate configuration for GSLB. The same parameters configured for HA are used for fetching the public IP.
- However, the peer NIC resource name and resource name for secondary public IP address are not used for GSLB.

GSLB Configuration for Multiple IP Address mode

The following is the only specific configuration needed for Alteon device running in Multiple IP address mode in Azure for supporting GSLB.

The public IP of the VIP must be configured as the NAT address.



CHAPTER 5 – SPECIAL CONSIDERATION FOR SINGLE IP ADDRESS MODE

Azure virtual machines are associated with a single IP address. As a result, there are some special considerations that should be taken into account when deploying Alteon VA on Azure.

Configuring Virtual Services

There is no limitation on load balancing for more than one application as long as every application is using a different service port.

In case you need to load balance several applications using the same port (for example web application using port 80) you should:

- Configure one virtual service.
- Configure a real server group for every application.
- Assign a content class based on the application domain name, or URL to redirect the traffic to the appropriate service group. For further information on configuring content groups refer to the *Alteon Application Guide*.

HTTPS

In order to enable load-balancing HTTPS traffic and management access, the HTTPS port for management access is changed to 8443.

To access the Alteon web interface, enter the Alteon VA instance IP address with port 8443.

For example, if the Alteon VM IP address is 1.1.1.1, enter **`https://1.1.1.1:8443`**

If you do not intend to load balance HTTPS traffic, you can change the HTTPS port for management purposes to the standard HTTPS port 443.

Reserved Ports

Alteon VA reserves some ports for internal usage.

You cannot load balance services running on the following ports: 123, 161, 3121, 2090, and 2091.

The following services use predefined ports and you cannot load balance services using the same ports as the services without changing the Alteon VA settings. If you do need to load balance services using these ports, you can change the ports that Alteon uses for these services through the user interface.

The following are the services and their predefined ports:

- HTTPS - port 8443 (to enable load balancing of HTTPS traffic)
- SSH - port 22
- Telnet - port 23
- DPM - port 3030

When you configure the Alteon to respond to health checks on specific ports (using the command: /cfg/sys/health) these ports cannot be used for load balancing services.

CHAPTER 6 – LIMITATION ON ALTEON VA SERVICES

The current release of the Alteon VA on Microsoft Azure cloud provides the same functionality as the Standard Alteon VA, such as: basic and advanced content-aware server load balancing, content modifications, SSL offload, and application security (WAF, API protection, BoT manager, IP intelligence).

Non-Supported Features

The following features are not supported by this release on the Azure cloud.

- Traffic Steering

Limitations

The following are the known limitations for this release related to the Alteon VA on the Azure cloud.

For the entire limitation list for any Alteon version, please refer to the relevant *Alteon Installation Guide*.

Item	Description	Bug ID
1.	The Alteon VA in Azure Cloud boots by default with a single IP address even if the VM has more NICs. In order to switch to a multiple-IP addresses configuration, disable the singleip mode using the /c/sys/singleip command.	DE19291
3.	Session mirroring is not supported when pbind is enabled (when the Alteon is configured to run in a multiple IP address mode).	DE36033
4.	The management interface does not support a NIC with accelerated network configured.	DE53182

APPENDIX A – RETRIEVING AZURE CREDENTIALS

In order for the Alteon to support HA and GSLB on the Azure cloud, it must access the Azure portal in order to remove the IP addresses between the Alteon VA instances.

For Alteon to access the Azure portal and perform the required activities, you must provide/create the proper credentials.

For this purpose you must register Alteon on the Azure portal as an application and assign it the proper roles through the Azure Active Directory.

Note: For other options to register applications on Azure portal refer to https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-integrating-applications

Generating and Retrieving Alteon VA credentials on the Azure Portal

This section describes the process to retrieve the following Azure credentials, which further needs to be entered to the Alton VA through the WebUI or using CLI commands.

- Azure Subscription ID
- Azure Tenant ID
- Azure Client ID
- Azure Client Secret

Prerequisites

Prerequisites include:

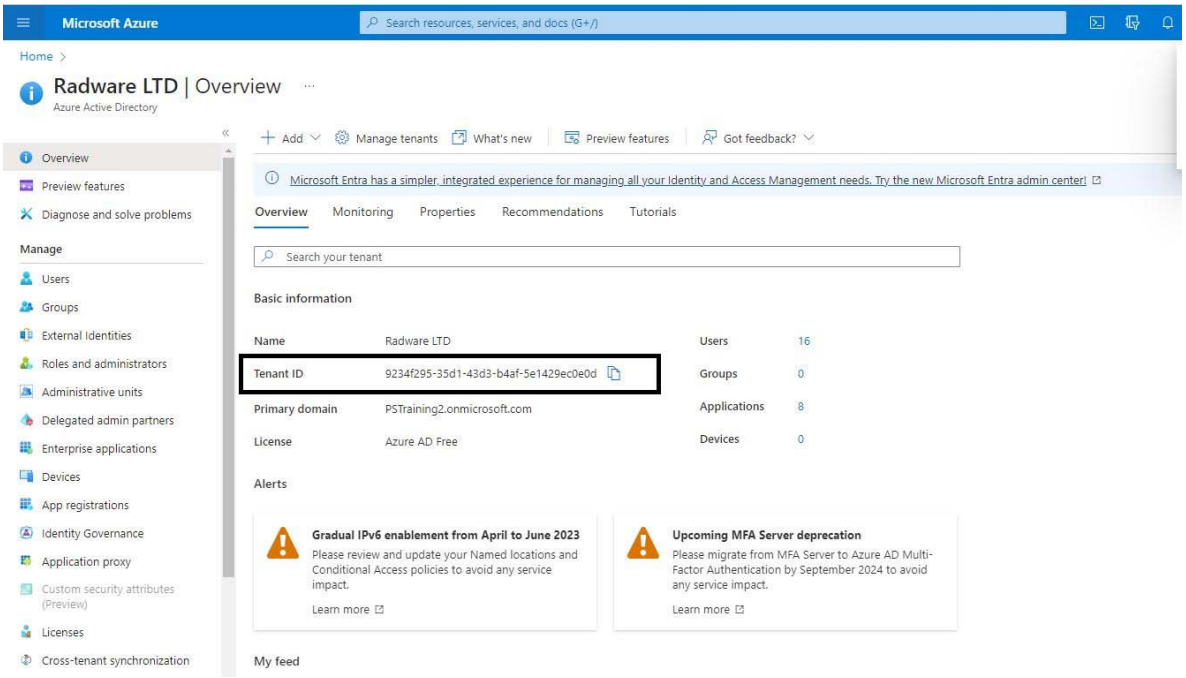
- A user name and password for the Azure portal.
- Administrator authorization in Azure account in order to add access control (owner).

Tenant ID

Tenant represents your organization ID in the Azure active directory (AD).

You can retrieve your tenant ID by navigating to the Azure Active Directory. In the Overview tab, under Basic information section, you have the Tenant ID. Copy it and paste it in Alteon as tenant ID field.

- Web UI: **Configuration > System > Azure Credentials** and **Resource> Alteon Tenant ID**
- CLI: **/cfg/sys/azure/tenant**

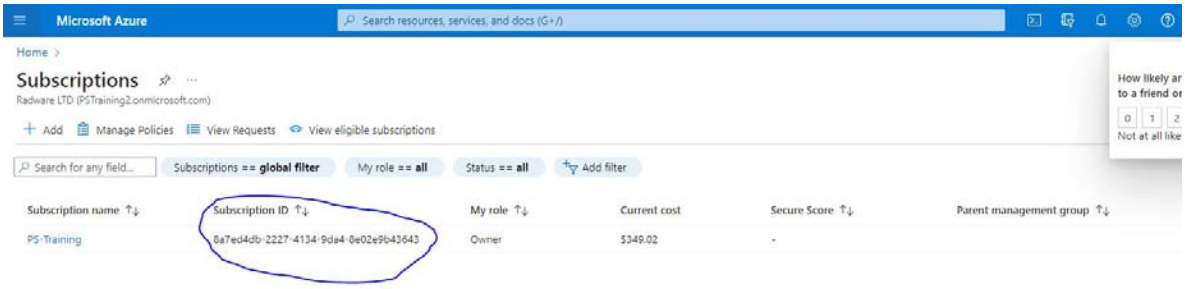


Subscription ID

In order to view your organization subscription from your Azure portal, click **Subscriptions**, and from the subscriptions list copy the **Subscription ID** which you should enter to the subscription ID field in the Alteon Web UI or using the CLI command **`/cfg/sys/azure/subscrip`**.

In order to view your organization subscriptions, from your Azure portal, click **Subscriptions**. From the subscriptions list copy the **Subscription ID** where the Alteon VA is installed and paste it in Alteon as subscription ID.

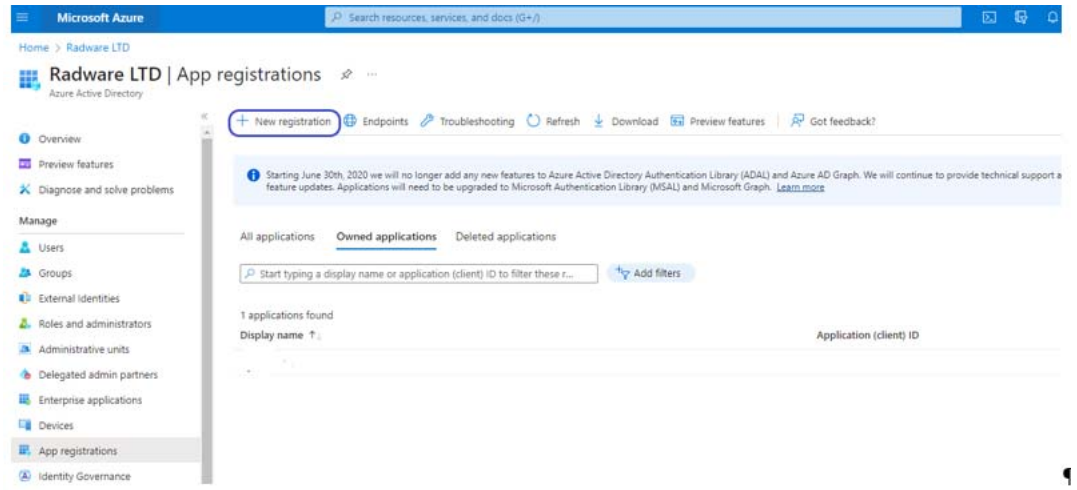
- Web UI: **Configuration > System > Azure Credentials** and **Resource> Alteon Subscription ID**
- CLI: **/cfg/sys/azure/subscrip**



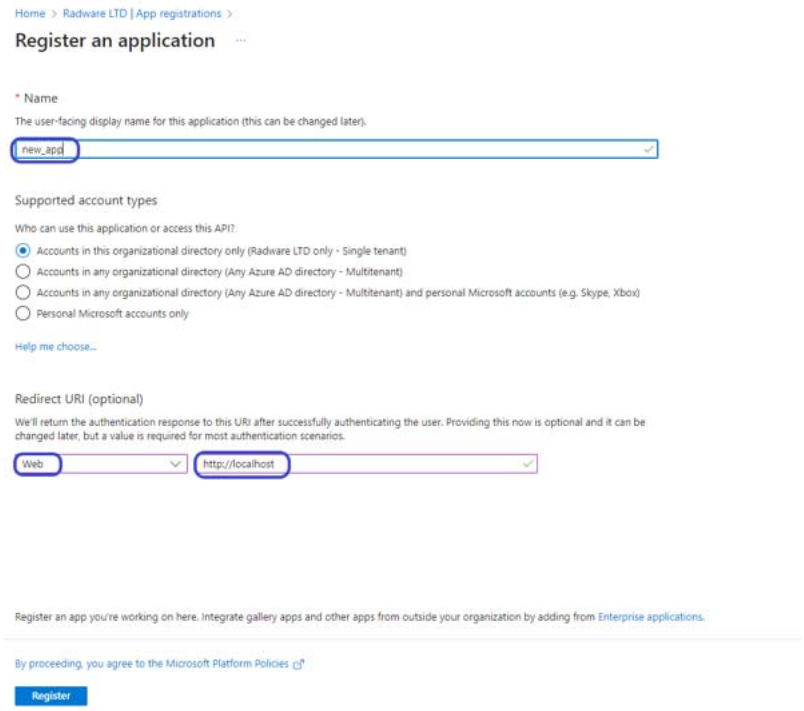
Client ID

Client ID represents the application registered in the Azure portal. It should be created in the portal, and its ID configured in Alteon. After the application is created, it should be assigned the required privileges under every subscription it uses.

From the Azure portal, navigate to the Azure Active Directory, and click **App registrations** and then **New registration**.



Assign the new application name (remember this name, as it will be used later on). Under the Redirect URI chose Web as the application type, enter **http://localhost** as the URI and click Register.



Copy the ID of the application you created and paste it as the client ID field in Alteon.

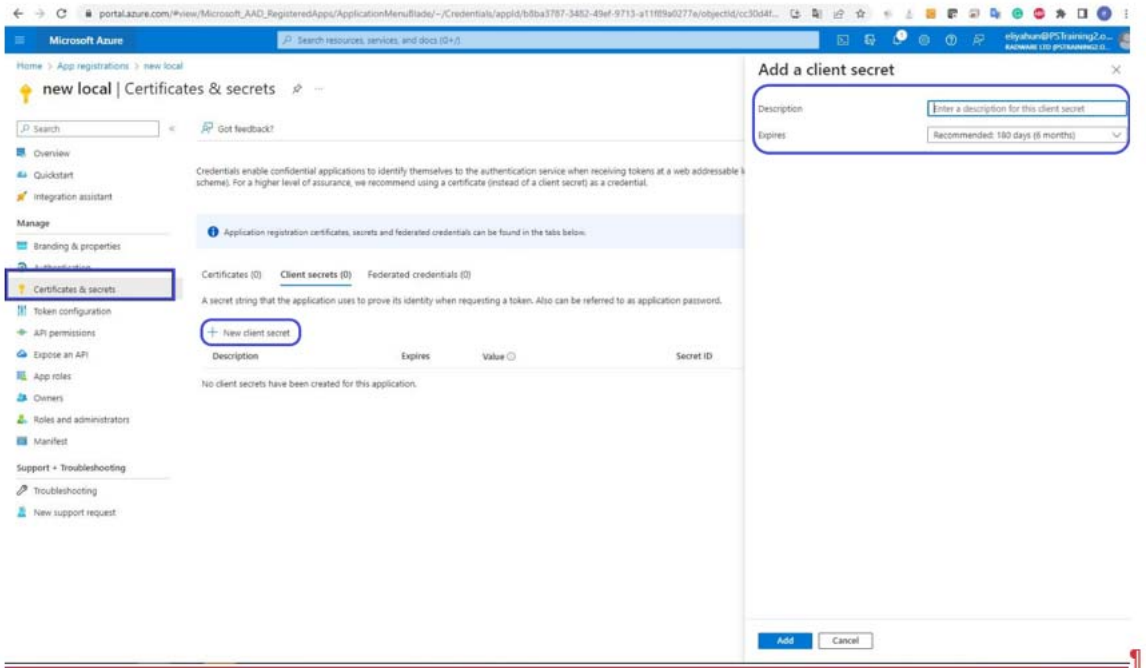
- Web UI: **Configuration > System > Azure Credentials** and **Resource> Alteon Client ID**
- CLI: **`/c/sys/azure/client`**

Under required permissions, verify you have Windows Azure Active Directory, with Sign in and read user profile delegated permissions.

Client Secret

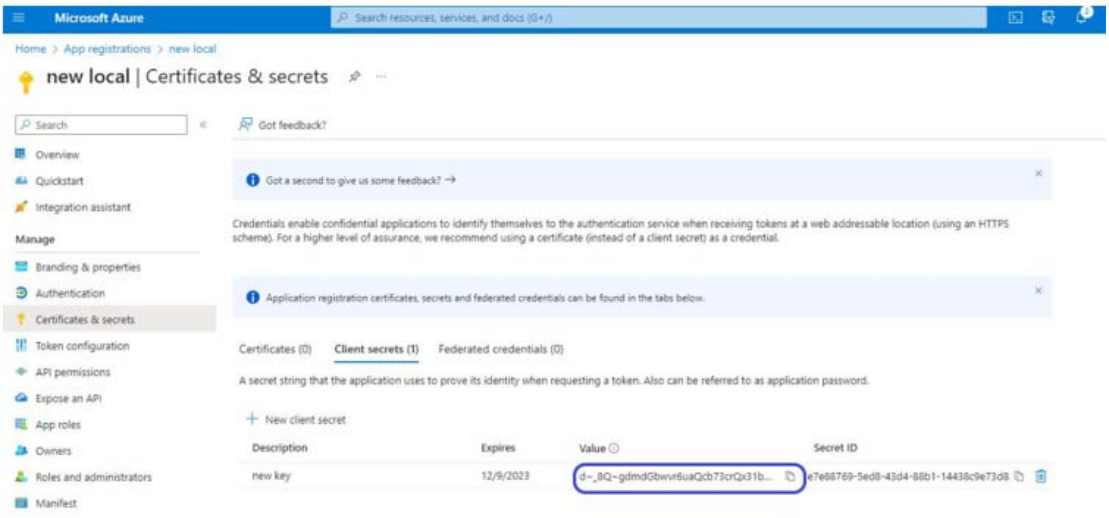
In the application you created, click **Certificates & secrets**.

Click on **New secret**, set the **Description** and **Expires** and click **Add**.



Once secret is created, copy the Value and paste it in the as the client secret in Alteon configuration.

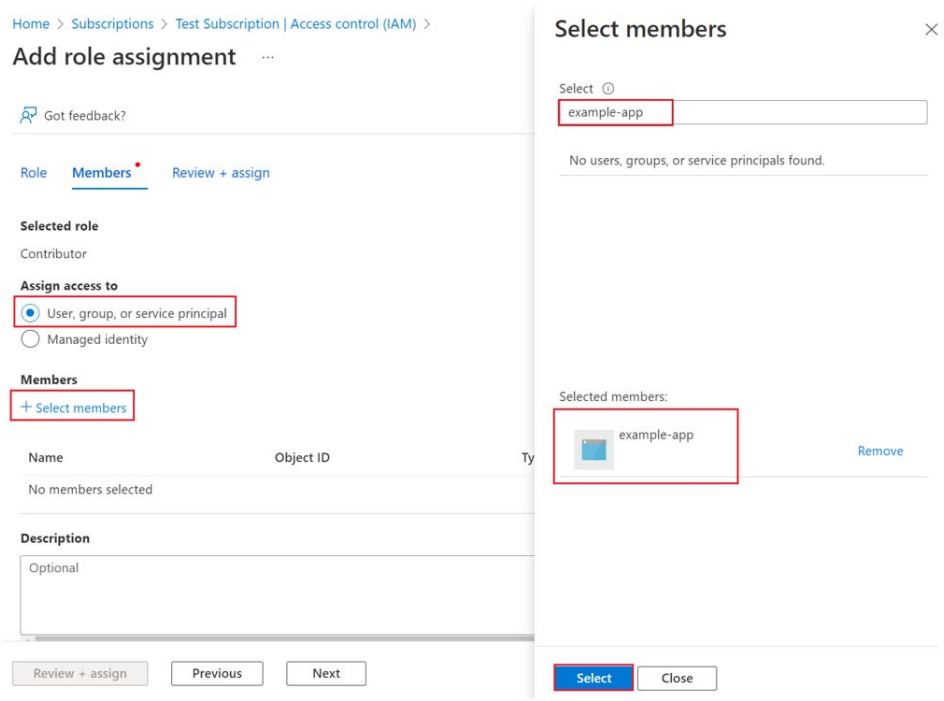
- Web UI: **Configuration > System > Azure Credentials** and **Resource> Alteon Client Secret**
- CLI: **`/c/sys/azure/secret`**



Assign a Role to the Application

To access resources in your subscription, you must assign a role to the application.

1. Select **Access control (IAM)**.
2. Select **Add**, then select **Add role assignment**.
3. In the **Role** tab, select the role you wish to assign to the application in the list.
4. Select the **Contributor** role.
5. Select **Next**.
6. On the *Members* tab, select **Assign access to**, then select **User, group, or service principal.**
7. Select **Select members**. By default, Azure AD applications aren't displayed in the available options. To find your application, Search for it by its name.
8. Click the **Select** button, then select **Review + assign**.



Verifying the Configuration

It is recommended to verify your configuration with a command line from any Linux machine with *wget* application version 1.15 or above (that supports PUT command–any Azure or AWS Ubuntu will probably will be good), and with proper DNS server configuration.

In order to do so, you will also need to have a resource group available under the subscription ID, and at least one network interface card in it.

It is recommended to navigate to https://resources.azure.com/ were you can easily explore all your resources.

The test below contains three stages: getting a token, reading NIC info, and updating NIC info.

Getting a Token

Construct the following command with your parameters, and paste it to your Linux machine

```
wget --method=POST --body-data="resource=https://
management.core.windows.net/
&client_id=<client_id>&grant_type=client_credentials&client_secret=<cli
ent_secret>" --header="Content-Type: application/x-www-form-urlencoded"
https://login.windows.net/<tenant_id>/oauth2/token
```

You should get a *200OK* response, and a token file will be created at local directory in *json* format. Print the file created.

If you get an authentication error, one of the parameters is not configured properly.

```
HTTP request sent, awaiting response... 200 OK
Length: 1351 (1.3K) [application/json]
Saving to: ?€ťoken?€™


100%[=============================================>] 1,351 -.-K/s   in
0s


2017-09-18 07:19:52 (348 MB/s) - ?€ťoken?€™ saved [1351/1351]


radware@gilc-ubuntu:~$ cat token
{"token_type":"Bearer","expires_in":"3599","ext_expires_in":"0","expire
s_on":"1505722792","not_before":"1505718892","resource":"https://
management.core.windows.net/
","access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkhIQnlLV
S0wRHFBcU1aaDZaRlBkMlZXYU90ZyIsImtpZCI6IkhIQnlLVS0wRHFBcU1aaDZaRlBkMlZX
YU90ZyJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuY29yZS53aW5kb3dzLm5ldC8iLC
Jpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC8yNThhYzRlNC0xNDZhLTQxMWUtOWRjO
C03OWE5ZTEyZmQ2ZGEvIiwiaWF0IjoxNTA1NzE4ODkyLCJuYmYiOjE1MDU3MTg4OTIsImV4
cCI6MTUwNTcyMjc5MiwiYWlvIjoiWLTc5YTllMTJmZDZkYS8iLCJvaWQiOiIxM2MyMzkyZS
1iOGM1LTQ2ODMtYmEyZi0yNjQxMjdmMjMzZmQiLCJzdWIiOiIxM2MyMzkyZS1iOGM1LTQ2O
DMtYmEyZi0yNjQxMjdmMjMzZmQiLCJ0aWQiOiIyNThhYzRlNC0xNDZhLTQxMWUtOWRjOC03
OWE5ZTEyZmQ2ZGEiLCJ1dGkiOiJTRkFZb1RDLWxFV3ZHdEhlWlVJVUFBIiwidmVyIjoiMS4
wIn0.kRaWWa3_f9-
hBhbpnPnnF1tX9RDxgbAqRewqkhyXytQWOVSowEWaA5pP36VrpvEFcRf4ypNyN7gq-
u6LuC132mxLmknGEJHkW2tuxevpUiUWb8fwp716GyDQWrCZmJ0UehIm5UQG5W5veyxpD9zP
xOlZRluFZcpLGGLM-
UGh6E3hcsQ2ile0ZSjp09yi9lG4tEwjmKKtgYoOFpKqCSVcffjdTf_yd9Muu-
GPivMhpn4bQXj4qtxVBU1aL7UiVWX36ZaC1Pe9xwfV4BnLHueDmtJrhnqn2ksUvhne4fQu_
QmVVwFuchihvmM2vij9QX5sb0mCYS1Jmg"}radware@gilc-ubuntu:~$
```

Copy the access token value. This is your token.

Read NIC Info

You will now need the resource group name, and the NIC resource name. Construct the following command:

```
wget -S --header="Authorization: Bearer <access_token>" https://
management.azure.com/subscriptions/<subscription_id>/resourceGroups/
<resource_group_name>/providers/Microsoft.Network/networkInterfaces/
<NIC_resource_name>?api-version=2017-03-01
```

You should get an HTTP *200OK* response, with a new *json* format file.

Copy the file with a new file named **dataFile** for convenience.

If you get an error, like 404, it probably means that one of the resource names is wrong, or does not exist under the subscription ID, or the NIC is not part of the resource group.

If you get an HTTP 403 forbidden error, it probably means the application role is not set or doesn't have the correct privileges.

Updating the NIC Information

Construct a new command as follows:

```
wget -S --header="Content-Type: application/json" --
header="Authorization: Bearer <access_token>" --method=PUT --body-
file=dataFile https://management.azure.com/subscriptions/
<subscription_id>/resourceGroups/<resource_group_name>/providers/
Microsoft.Network/networkInterfaces/<NIC_resource_name>?api-
version=2017-03-01
```

Again you should get an HTTP *200OK* response. This means you are able to update NIC information.

If you get an HTTP 403 forbidden error, it probably means the application role is not set or doesn't have the correct privileges.

Note: Application privileges might enable you to read NIC information at the previous phase, but not allow you to update. In this case, as well, the application role should be set correctly.

RADWARE LTD. END USER LICENSE AGREEMENT

By accepting this End User License Agreement (this "License Agreement") you agree to be contacted by Radware Ltd.'s ("Radware") sales personnel.

If you would like to receive license rights different from the rights granted below or if you wish to acquire warranty or support services beyond the scope provided herein (if any), please contact Radware's sales team.

THIS LICENSE AGREEMENT GOVERNS YOUR USE OF ANY SOFTWARE DEVELOPED AND/OR DISTRIBUTED BY RADWARE AND ANY UPGRADES, MODIFIED VERSIONS, UPDATES, ADDITIONS, AND COPIES OF THE SOFTWARE FURNISHED TO YOU DURING THE TERM OF THE LICENSE GRANTED HEREIN (THE "SOFTWARE"). THIS LICENSE AGREEMENT APPLIES REGARDLESS OF WHETHER THE SOFTWARE IS DELIVERED TO YOU AS AN EMBEDDED COMPONENT OF A RADWARE PRODUCT ("PRODUCT"), OR WHETHER IT IS DELIVERED AS A STANDALONE SOFTWARE PRODUCT. FOR THE AVOIDANCE OF DOUBT IT IS HEREBY CLARIFIED THAT THIS LICENSE AGREEMENT APPLIES TO PLUG-INS, CONNECTORS, EXTENSIONS AND SIMILAR SOFTWARE COMPONENTS DEVELOPED BY RADWARE THAT CONNECT OR INTEGRATE A RADWARE PRODUCT WITH THE PRODUCT OF A THIRD PARTY (COLLECTIVELY, "CONNECTORS") FOR PROVISIONING, DECOMMISSIONING, MANAGING, CONFIGURING OR MONITORING RADWARE PRODUCTS. THE APPLICABILITY OF THIS LICENSE AGREEMENT TO CONNECTORS IS REGARDLESS OF WHETHER SUCH CONNECTORS ARE DISTRIBUTED TO YOU BY RADWARE OR BY A THIRD PARTY PRODUCT VENDOR. IN CASE A CONNECTOR IS DISTRIBUTED TO YOU BY A THIRD PARTY PRODUCT VENDOR PURSUANT TO THE TERMS OF AN AGREEMENT BETWEEN YOU AND THE THIRD PARTY PRODUCT VENDOR, THEN, AS BETWEEN RADWARE AND YOURSELF, TO THE EXTENT THERE IS ANY DISCREPANCY OR INCONSISTENCY BETWEEN THE TERMS OF THIS LICENSE AGREEMENT AND THE TERMS OF THE AGREEMENT BETWEEN YOU AND THE THIRD PARTY PRODUCT VENDOR, THE TERMS OF THIS LICENSE AGREEMENT WILL GOVERN AND PREVAIL. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE CONTAINING RADWARE'S PRODUCT, OR BEFORE DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING RADWARE'S STANDALONE SOFTWARE (AS APPLICABLE). THE SOFTWARE IS LICENSED (NOT SOLD). BY OPENING THE PACKAGE CONTAINING RADWARE'S PRODUCT, OR BY DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE (AS APPLICABLE), YOU CONFIRM THAT YOU HAVE READ AND UNDERSTAND THIS LICENSE AGREEMENT AND YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT. FURTHERMORE, YOU HEREBY WAIVE ANY CLAIM OR RIGHT THAT YOU MAY HAVE TO ASSERT THAT YOUR ACCEPTANCE AS STATED HEREINABOVE IS NOT THE EQUIVALENT OF, OR DEEMED AS, A VALID SIGNATURE TO THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE UNOPENED PRODUCT PACKAGE OR YOU SHOULD NOT DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE (AS APPLICABLE). THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND RADWARE, AND SUPERSEDES ANY AND ALL PRIOR PROPOSALS, REPRESENTATIONS, OR UNDERSTANDINGS BETWEEN THE PARTIES. "YOU" MEANS THE NATURAL PERSON OR THE ENTITY THAT IS AGREEING TO BE BOUND BY THIS LICENSE AGREEMENT, THEIR EMPLOYEES AND THIRD PARTY CONTRACTORS. YOU SHALL BE LIABLE FOR ANY FAILURE BY SUCH EMPLOYEES AND THIRD PARTY CONTRACTORS TO COMPLY WITH THE TERMS OF THIS LICENSE AGREEMENT.

1. **License Grant**. Subject to the terms of this Agreement, Radware hereby grants to you, and you accept, a limited, nonexclusive, nontransferable license to install and use the Software in machine-readable, object code form only and solely for your internal business purposes ("Commercial License"). If the Software is distributed to you with a software development kit (the "SDK"), then, solely with regard to the SDK, the Commercial License above also includes a limited, nonexclusive, nontransferable license to install and use the SDK solely on computers within your organization, and solely for your internal development of an integration or interoperation of the Software and/or other Radware Products with software or hardware products owned, licensed and/or controlled by you (the "SDK Purpose"). To the extent an SDK is

distributed to you together with code samples in source code format (the "Code Samples") that are meant to illustrate and teach you how to configure, monitor and/or control the Software and/or any other Radware Products, the Commercial License above further includes a limited, nonexclusive, nontransferable license to copy and modify the Code Samples and create derivative works based thereon solely for the SDK Purpose and solely on computers within your organization. The SDK shall be considered part of the term "Software" for all purposes of this License Agreement. You agree that you will not sell, assign, license, sublicense, transfer, pledge, lease, rent or share your rights under this License Agreement nor will you distribute copies of the Software or any parts thereof. Rights not specifically granted herein, are specifically prohibited.

2. **Evaluation Use**. Notwithstanding anything to the contrary in this License Agreement, if the Software is provided to you for evaluation purposes, as indicated in your purchase order or sales receipt, on the website from which you download the Software, as inferred from any time-limited evaluation license keys that you are provided with to activate the Software, or otherwise, then You may use the Software only for internal evaluation purposes ("Evaluation Use") for a maximum of 30 days or such other duration as may specified by Radware in writing at its sole discretion (the "Evaluation Period"). The evaluation copy of the Software contains a feature that will automatically disable it after expiration of the Evaluation Period. You agree not to disable, destroy, or remove this feature of the Software, and any attempt to do so will be a material breach of this License Agreement. During or at the end of the evaluation period, you may contact Radware sales team to purchase a Commercial License to continue using the Software pursuant to the terms of this License Agreement. If you elect not to purchase a Commercial License, you agree to stop using the Software and to delete the evaluation copy received hereunder from all computers under your possession or control at the end of the Evaluation Period. In any event, your continued use of the Software beyond the Evaluation Period (if possible) shall be deemed your acceptance of a Commercial License to the Software pursuant to the terms of this License Agreement, and you agree to pay Radware any amounts due for any applicable license fees at Radware's then-current list prices.
3. **Lab License**. Notwithstanding anything to the contrary in this License Agreement, if the Software is provided to you for use in your lab or for development purposes, as indicated in your purchase order, sales receipt, the part number description for the Software, the webpage from which you download the Software, or otherwise, then You may use the Software only for internal testing and development purposes in your lab but not for any production use purposes.
4. **Subscription Software**. If you licensed the Software on a subscription basis, your rights to use the Software are limited to the subscription period. You have the option to extend your subscription. If you extend your subscription, you may continue using the Software until the end of your extended subscription period. If you do not extend your subscription, after the expiration of your subscription, you are legally obligated to discontinue your use of the Software and completely remove the Software from your system.
5. **Feedback**. Any feedback concerning the Software including, without limitation, identifying potential errors and improvements, recommended changes or suggestions ("Feedback"), provided by you to Radware will be owned exclusively by Radware and considered Radware's confidential information. By providing Feedback to Radware, you hereby assign to Radware all of your right, title and interest in any such Feedback, including all intellectual property rights therein. With regard to any rights in such Feedback that cannot, under applicable law, be assigned to Radware, you hereby irrevocably waives such rights in favor of Radware and grants Radware under such rights in the Feedback, a worldwide, perpetual royalty-free, irrevocable, sub-licensable and non-exclusive license, to use, reproduce, disclose, sublicense, modify, make, have made, distribute, sell, offer for sale, display, perform, create derivative works of and otherwise exploit the Feedback without restriction. The provisions of this Section 5 will survive the termination or expiration of this Agreement.
6. **Limitations on Use**. You agree that you will not: (a) copy, modify, translate, adapt or create any derivative works based on the Software; or (b) sublicense or transfer the Software, or include the Software or any portion thereof in any product; or (b) reverse assemble, disassemble, decompile, reverse engineer or otherwise attempt to derive source code (or the underlying ideas, algorithms, structure or organization) from the Software, in whole or in part, except and only to the extent: (i) applicable law expressly permits any such action, despite this

limitation, in which case you agree to provide Radware at least ninety (90) days advance written notice of your belief that such action is warranted and permitted and to provide Radware with an opportunity to evaluate if the law's requirements necessitate such action, or (ii) required to debug changes to any third party LGPL-libraries linked to by the Software; or (c) create, develop, license, install, use, or deploy any software or services to circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Software; (d) in the event the Software is provided as an embedded or bundled component of another Radware Product, you shall not use the Software other than as part of the combined Product and for the purposes for which the combined Product is intended; (e) remove any copyright notices, identification or any other proprietary notices from the Software (including any notices of Third Party Software (as defined below); or (f) copy the Software onto any public or distributed network or use the Software to operate in or as a time-sharing, outsourcing, service bureau, application service provider, or managed service provider environment. Notwithstanding Section 5(d), if you provide hosting or cloud computing services to your customers, you are entitled to use and include the Software in your IT infrastructure on which you provide your services. It is hereby clarified that the prohibitions on modifying, or creating derivative works based on, any Software provided by Radware, apply whether the Software is provided in a machine or in a human readable form. Human readable Software to which this prohibition applies includes (without limitation) to "Radware AppShape++ Script Files" that contain "Special License Terms". It is acknowledged that examples provided in a human readable form may be modified by a user.

7. **Intellectual Property Rights**. You acknowledge and agree that this License Agreement does not convey to you any interest in the Software except for the limited right to use the Software, and that all right, title, and interest in and to the Software, including any and all associated intellectual property rights, are and shall remain with Radware or its third party licensors. You further acknowledge and agree that the Software is a proprietary product of Radware and/or its licensors and is protected under applicable copyright law.

8. **No Warranty**. The Software, and any and all accompanying software, files, libraries, data and materials, are distributed and provided "AS IS" by Radware or by its third party licensors (as applicable) and with no warranty of any kind, whether express or implied, including, without limitation, any non-infringement warranty or warranty of merchantability or fitness for a particular purpose. Neither Radware nor any of its affiliates or licensors warrants, guarantees, or makes any representation regarding the title in the Software, the use of, or the results of the use of the Software. Neither Radware nor any of its affiliates or licensors warrants that the operation of the Software will be uninterrupted or error-free, or that the use of any passwords, license keys and/or encryption features will be effective in preventing the unintentional disclosure of information contained in any file. You acknowledge that good data processing procedure dictates that any program, including the Software, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of the Software covered by this License. Radware does not make any representation or warranty, nor does Radware assume any responsibility or liability or provide any license or technical maintenance and support for any operating systems, databases, migration tools or any other software component provided by a third party supplier and with which the Software is meant to interoperate.

   This disclaimer of warranty constitutes an essential and material part of this License.

   In the event that, notwithstanding the disclaimer of warranty above, Radware is held liable under any warranty provision, Radware shall be released from all such obligations in the event that the Software shall have been subject to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than by Radware's authorized service personnel.

9. **Limitation of Liability**. Except to the extent expressly prohibited by applicable statutes, in no event shall Radware, or its principals, shareholders, officers, employees, affiliates, licensors, contractors, subsidiaries, or parent organizations (together, the "Radware Parties"), be liable for any direct, indirect, incidental, consequential, special, or punitive damages whatsoever relating to the use of, or the inability to use, the Software, or to your relationship with, Radware or any of the Radware Parties (including, without limitation, loss or disclosure of data or information, and/or loss of profit, revenue, business opportunity or business advantage, and/or business

interruption), whether based upon a claim or action of contract, warranty, negligence, strict liability, contribution, indemnity, or any other legal theory or cause of action, even if advised of the possibility of such damages. If any Radware Party is found to be liable to You or to any third-party under any applicable law despite the explicit disclaimers and limitations under these terms, then any liability of such Radware Party, will be limited exclusively to refund of any license or registration or subscription fees paid by you to Radware.

10. **Third Party Software**. The Software includes software portions developed and owned by third parties (the "Third Party Software"). Third Party Software shall be deemed part of the Software for all intents and purposes of this License Agreement; provided, however, that in the event that a Third Party Software is a software for which the source code is made available under an open source software license agreement, then, to the extent there is any discrepancy or inconsistency between the terms of this License Agreement and the terms of any such open source license agreement (including, for example, license rights in the open source license agreement that are broader than the license rights set forth in Section 1 above and/or no limitation in the open source license agreement on the actions set forth in Section 6 above), the terms of any such open source license agreement will govern and prevail. The terms of open source license agreements and copyright notices under which Third Party Software is being licensed to Radware or a link thereto, are included with the Software documentation or in the header or readme files of the Software. Third Party licensors and suppliers retain all right, title and interest in and to the Third Party Software and all copies thereof, including all copyright and other intellectual property associated therewith. In addition to the use limitations applicable to Third Party Software pursuant to Section 6 above, you agree and undertake not to use the Third Party Software as a general SQL server, as a stand-alone application or with applications other than the Software under this License Agreement.
11. **Term and Termination**. This License Agreement is effective upon the first to occur of your opening the package of the Product, purchasing, downloading, installing, copying or using the Software or any portion thereof, and shall continue until terminated. However, sections 5-15 shall survive any termination of this License Agreement. The Licenses granted under this License Agreement are not transferable and will terminate upon: (i) termination of this License Agreement, or (ii) transfer of the Software, or (iii) in the event the Software is provided as an embedded or bundled component of another Radware Product, when the Software is un-bundled from such Product or otherwise used other than as part of such Product. If the Software is licensed on subscription basis, this Agreement will automatically terminate upon the termination of your subscription period if it is not extended.
12. **Export**. The Software or any part thereof may be subject to export or import controls under applicable export/import control laws and regulations including such laws and regulations of the United States and/or Israel. You agree to comply with such laws and regulations, and, agree not to knowingly export, re-export, import or re-import, or transfer products without first obtaining all required Government authorizations or licenses therefor. Furthermore, You hereby covenant and agree to ensure that your use of the Software is in compliance with all other foreign, federal, state, and local laws and regulations, including without limitation all laws and regulations relating to privacy rights, and data protection. You shall have in place a privacy policy and obtain all of the permissions, authorizations and consents required by applicable law for use of cookies and processing of users' data (including without limitation pursuant to Directives 95/46/EC, 2002/58/EC and 2009/136/EC of the EU if applicable) for the purpose of provision of any services.
13. **US Government**. To the extent you are the U.S. government or any agency or instrumentality thereof, you acknowledge and agree that the Software is a "commercial computer software" and "commercial computer software documentation" pursuant to applicable regulations and your use of the is subject to the terms of this License Agreement.
14. **Governing Law**. This License Agreement shall be construed and governed in accordance with the laws of the State of Israel.
15. **Miscellaneous**. If a judicial determination is made that any of the provisions contained in this License Agreement is unreasonable, illegal or otherwise unenforceable, such provision or provisions shall be rendered void or invalid only to the extent that such judicial determination finds such provisions to be unreasonable, illegal or otherwise unenforceable, and the remainder of this License Agreement shall remain operative and in full force and effect. In any event a

party breaches or threatens to commit a breach of this License Agreement, the other party will, in addition to any other remedies available to, be entitled to injunction relief. This License Agreement constitutes the entire agreement between the parties hereto and supersedes all prior agreements between the parties hereto with respect to the subject matter hereof. The failure of any party hereto to require the performance of any provisions of this License Agreement shall in no manner affect the right to enforce the same. No waiver by any party hereto of any provisions or of any breach of any provisions of this License Agreement shall be deemed or construed either as a further or continuing waiver of any such provisions or breach waiver or as a waiver of any other provision or breach of any other provision of this License Agreement.

IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE YOU MUST REMOVE THE SOFTWARE FROM ANY DEVICE OWNED BY YOU AND IMMIDIATELY CEASE USING THE SOFTWARE.