CHAPTER 6

Cisco vWAAS in Microsoft Azure

This chapter describes how to provision, deploy, and verify Cisco vWAAS in Microsoft Azure.

This chapter contains the following sections:

- About Cisco vWAAS in Microsoft Azure
- Provisioning the vWAAS VM in Microsoft Azure
- Deploying vWAAS in Microsoft Azure
- Verifying the vWAAS in Azure Deployment

About Cisco vWAAS in Microsoft Azure

Azure is a Microsoft Cloud that provisions virtual machines (VMs) on the Microsoft Hyper-V hypervisor. vWAAS in Azure is part of WAAS support for Office 365, and is an end-to-end solution with enterprise branch offices.

- vWAAS in Azure is available for vWAAS Version 6.2.1x and later, and is supported for vWAAS-200, vWAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, and vWAAS-12000v.

This section contains the following topics:

- Platforms Supported for Cisco vWAAS in Microsoft Azure
- Operating Considerations for Cisco vWAAS in Microsoft Azure
- Operating Limitations for Cisco vWAAS in Microsoft Azure
- Upgrade/Downgrade Considerations for Cisco vWAAS in Microsoft Azure

Platforms Supported for Cisco vWAAS in Microsoft Azure

The following platforms are supported for Cisco vWAAS in Microsoft Azure:

- vWAAS in Azure is available for vWAAS Version 6.2.1x and later, and is supported for vWAAS-200, vWAAS-750, vWAAS-1300, vWAAS-2500, vWAAS-6000, and vWAAS-12000v.
- vWAAS in Azure is not currently supported for vWAAS-50000.

Table 6-1 Microsoft Azure VM Sizes for Cisco WAAS vWAAS Models

vWAAS Model	Maximum Connections	Data Disk	Minimum Azure VM Size
vWAAS-200	200	160 GB	D2_v2 (2 cores, 7GB)
vWAAS-750	750	250 GB	D2_v2 (2 cores, 7GB)
vWAAS-1300	1300	300 GB	D2_v2 (2 cores, 7GB)
vWAAS-2500	2500	400 GB	D3_v2 (4 cores, 14GB)
vWAAS-6000	6000	500 GB	D3_v2 (4 cores, 14GB)
vWAAS-12000	12000	750 GB	D3_v2 (4 cores, 14GB)

Operating Considerations for Cisco vWAAS in Microsoft Azure

Note the following operating considerations for Cisco vWAAS in Microsoft Azure:

- vWAAS in Azure is available for all vWAAS models, for WAAS Version 6.2.1 and later.
- You can display and identify an Azure vWAAS device on the WAAS Central Manager or the CLI:
  - On the WAAS Central Manager, navigate to the **Manage Devices** screen. The vWAAS in Azure device type is displayed as **OE-VWAAS-AZURE**.
  - On the CLI, use either the **show version** EXEC command or the **show hardware** EXEC command. Output for both commands will include device ID, shown as **OE-VWAAS-AZURE**.
- vWAAS in Azure communicates with the WAAS Central Manager in the same ways as physical appliances communicate with the Central Manager.

  A vWAAS in Azure device is displayed on the WAAS Central Manager as AZURE-VWAAS. To display vWAAS in Azure devices, navigate to **Home** > **Devices** > **All Devices**. The Device Type column shows all WAAS and vWAAS devices.

Note For vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.

- Registering the vWAAS in Azure to the WAAS Central Manager:
  - If you register the vWAAS with the WAAS Central Manager using a private IP address, following the usual vWAAS registration process described in Configuring vWAAS Settings of Chapter 2, “Configuring and Cisco vWAAS and Viewing vWAAS Components.
  - If you register the vWAAS with the WAAS Central Manager using a public IP address, you must specify the public address of the vWAAS in the WAAS Central Manager Device Activation screen (navigate to **Devices** > *device-name* > **Activation**).

Note After you have registered the vWAAS in Azure device to the WAAS Central Manager, you must configure the public IP address of the Central Manager. The vWAAS in Azure device can contact the Central Manager only by using the public IP address of the registration. To set the public IP address of the WAAS Central Manager:

1. In the WAAS Central Manager, navigate to **Home** > **Devices** > *Primary-CM-Device* > **Configure** > **Network** > **NatSettings**.

2. In the NAT IP field, enter the public IP address of the Central Manager.

Operating Limitations for Cisco vWAAS in Microsoft Azure

Note the following operating limitations for Cisco vWAAS in Microsoft Azure:

- vWAAS auto-registration is not supported, because Microsoft Azure uses DHCP to configure VMs with IP address and Azure fabric server IP address. There will be operational issues if you deploy a separate DHCP server for auto-registration.

  Functionality similar to auto-registration is available by providing the WAAS CM IP address during VM provisioning. The vWAAS VM will try to register with this WAAS CM during provisioning.
- Microsoft Azure does not support GRE, IPv6, or Jumbo Frames, therefore vWAAS in Azure does not support these features.

Note For vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.

- WAAS/vWAAS with Akamai Connect is not supported for vWAAS in Azure.

Upgrade/Downgrade Considerations for Cisco vWAAS in Microsoft Azure

Note the following upgrade/downgrade considerations for Cisco vWAAS in Microsoft Azure:

- The procedure for upgrading or downgrading vWAAS in Azure, for all vWAAS models except vWAAS-50000, is the same as for any other WAAS device.
- Downgrading a device or device group for vWAAS in Azure to a WAAS Version earlier than Version 6.2.1 is not supported.

Deployment Options for Cisco vWAAS in Miscrosoft Azure

There are two major deployment options for Cisco vWAAS in Microsoft Azure:

- A SaaS application, such as an enterprise application where you control hosting of the application

  In this type of deployment, both the application server and Cisco vWAAS can be put in the Azure cloud just as in a private cloud. The vWAAS is very close to the server, and tied to the server movement. In this case, the traffic flow is very similar to that in a normal enterprise data center deployment.
- A SaaS application such as Office 365, where you do not control hosting of the application

In this type of deployment, you do not have control over the application in the cloud; you control only the vWAAS. In this case, traffic from the CSR in the branch is tunneled to the CSR in Azure, which is then redirected to the vWAAS. A Destination Network Address Translation (DNAT) is performed to get the traffic back to the CSR in the Azure cloud from the SaaS application. For more information on Office 365 and WAAS, see *Accelerate Microsoft Office 365 Shared Deployments with Cisco WAAS WAN Optimization*.

Provisioning the vWAAS VM in Microsoft Azure

Note To deploy vWAAS in Azure, you need a Microsoft Azure Pay-As-You-Go subscription. Subscription procedure and billing information are available on the Microsoft Azure website.

To provision the vWAAS VM in Microsoft Azure, follow these steps:

Step 1 Login to the Microsoft Azure portal.

Step 2 Navigate to **New** > **Compute** > **Virtual Machine** > **From Gallery**.

The **Create a Virtual Machine/Choose an Image** screen is displayed.

Step 3 At the **Create a Virtual Machine/Choose an Image** > **My Images** screen, select the vWAAS Azure image for your system.

The **Create a Virtual Machine/Virtual Machine Configuration** screen is displayed.

Step 4 In the Virtual Machine Name field, enter the name of the VM you want to create. Use only letters and numbers, up to a maximum of 15 characters.

Step 5 In the Tier field, select **Standard**.

Step 6 At the Size dropdown list, select the Azure VM size for your system. Table 6-2 shows the minimum Azure VM size for each vWAAS model available for provisioning in the Tier field.

Table 6-2 Microsoft Azure VM Sizes for Cisco WAAS vWAAS Models

vWAAS Model	Maximum Connections	Data Disk	Minimum Azure VM Size
vWAAS-200	200	160 GB	D2_v2 (2 cores, 7GB)
vWAAS-750	750	250 GB	D2_v2 (2 cores, 7GB)
vWAAS-1300	1300	300 GB	D2_v2 (2 cores, 7GB)
vWAAS-2500	2500	400 GB	D3_v2 (4 cores, 14GB)

Note Use the Microsoft Azure Tier field to select an Azure VM for the vWAAS models shown in Table 6-2. For vWAAS-6000 and vWAAS-12000, you must use the template to specify the Azure VM. For more information, see Deploying vWAAS in Microsoft Azure. For Azure VM sizes for vWAAS-6000 and vWAAS-12000, see Table 6-1.

Step 7 In the New User Name field, enter your user name.

Step 8 In the New Password field, enter your password.

Step 9 In the Confirm field, re-enter your password.

Step 10 (Optional) If your system uses SSH key-based authentication:

a. Check the **Upload compatible SSH key for authentication** checkbox.

b. At the Certificate field, browse for the certificate file for your system.

Step 11 (Optional) If your system requires a password, check the **Provide a password checkbox**.

Step 12 Click the right arrow at the lower right of the screen to proceed to the next screen.

The next **Create a Virtual Machine/Virtual Machine Configuration** screen is displayed.

Step 13 At the Cloud Service dropdown list, select **Create a Cloud Service**.

Step 14 In the Cloud Service DNS Name field, enter the name of the VM that you created in Step 4.

In the naming style of Azure VMs, the DNS name has **cloudapp.net** automatically appended to it.

Step 15 At the Region/Affinity Group/Virtual Network dropdown list, choose a location that is in close proximity to the resources you want to optimize, such as East US or North Europe.

The Region/Affinity Group/Virtual Network setting determines the location of the VM within the Azure cloud data centers.

Step 16 At the Storage Account dropdown list, select **Use an automatically generated storage account**.

Step 17 At the Availability Set dropdown list, choose **(None)**.

Step 18 Click the right arrow at the lower right corner of the screen to proceed to the next screen.

The **Virtual Machines/Virtual Machine Instances** screen is displayed

Step 19 By default, the **Install the VM Agent** check box is checked.

Step 20 In the Endpoints section:

a. Add an endpoint for **SSH (port 22**)

b. Add an endpoint for **HTTPS** (**port 443**)

Step 21 Click the checkmark at the lower right corner of the screen to proceed for provisioning vWAAS.

The **Virtual Machines/Virtual Machine Instances** screen is displayed, showing the newly-created VM with an initial status of *Starting (Provisioning)*.

Step 22 The process takes a few minutes before the VM status is displayed as running.

Step 23 Select the vWAAS VM.

Step 24 Attach the data disks. See Table 6-2 for data disk sizes for Azure VMs.

Step 25 Stop and then start the VM, so that it picks up the attached disks.

Your VM is ready to be deployed, with end-to-end setup.

Deploying vWAAS in Microsoft Azure

This section has the following topics:

- Deploying vWAAS VM and Data Disk with the VHD Template
- Deploying vWAAS VM with Template and Custom VHD from the Microsoft ARM Portal
- Deploying vWAAS VM Using Windows Powershell

Deploying vWAAS VM and Data Disk with the VHD Template

To deploy the vWAAS VM and data disk with the VHD template, follow these steps:

Step 1 Copy **vwaas.vhd** to the storage account using AzCopy.

The AzCopy command parameters are:

- **Source:** The local folder address on the Windows device where the VHD file is stored.
- **Dest:** The location of the container on the Azure cloud storage account.
- **Destkey:** The Azure cloud storage account key.

Step 2 Use the template to deploy the vWAAS VM.

The vWAAS VM is deployed with the data disk.

Step 3 Log in with your username and password.

Step 4 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Deploying vWAAS VM with Template and Custom VHD from the Microsoft ARM Portal

To deploy the vWAAS VM with a template and custom VHD from the Microsoft Azure Resource Manager (ARM) portal, follow these steps:

Step 1 *Prerequisite:* Verify that the vWAAS VM is provisioned in Azure, including the creation of a storage account and a VM location in Azure specified. For more information, see Provisioning the vWAAS VM in Microsoft Azure.

Step 2 Copy **vwaas.vhd** to the storage account using Azcopy.

Step 3 Use the template to deploy the vWAAS VM.

Step 4 At the Microsoft ARM portal, navigate to **New** > **Template Deployment** > **Edit Template**.

Step 5 Paste the template here.

Step 6 For the parameters, enter the values for your system, such as resource group and resource group location, and whether or not to deploy the vWAAS VM in a new or existing virtual network.

Step 7 Accept the Terms and Conditions.

Step 8 Click Create.

Step 9 The vWAAS VM is deployed.

Step 10 Log in with your username and password.

Step 11 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Deploying vWAAS VM Using Windows Powershell

To deploy the vWAAS VM using Windows Powershell, follow these steps:

Step 1 *Prerequisite:* Verify that the vWAAS VM is provisioned in Azure, including the creation of a storage account and a VM location in Azure specified. For more information, see Provisioning the vWAAS VM in Microsoft Azure.

Step 2 Deploy vWAAS on Microsoft Hyper-V. For information on this deployment procedure, see Chapter 5, "Cisco vWAAS on Microsoft Hyper-V"

Step 3 Run the **azure_predeploy.sh** script in Hyper-V, to set the necessary Azure parameters.

Step 4 Export the flash VHD from the Hyper-V disk location to the storage account in Azure, using AzCopy.

Step 5 Use Windows Powershell commands to specify the following parameters:

- Use the **deployName** command to specify the deployment name.
- Use the **RGName** command to specify the resource group.
- Use the **locName** command to specify the location.
- Use the **templateURI** command to specify the template file.

Step 6 Use the **New-AzureRmResourceGroup -Name $RGName -Location $locName** Powershell command to create the resource group.

Step 7 Use the **New-AzureRmResourceGroupDeployment** Powershell cmdlet to deploy vWAAS in Azure. To complete the deployment, specify values for the following parameters:

- userImageStorageAccountName
- userImageStoragContainerName
- userImageVhdName
- osType
- vmName
- adminUserName
- adminPassword

Step 8 After you enter these parameters, vWAAS in Azure is deployed. The system displays provisioning information, including deployment name, provisioning state, date/time, and mode.

Step 9 Log in with your username and password.

Step 10 (Optional) To verify deployment details such as CMS registration and WAAS Central Manager address, see Verifying the vWAAS in Azure Deployment.

Verifying the vWAAS in Azure Deployment

Table 6-3 provides a checklist for verifying the vWAAS VM deployment in Microsoft Azure.

Table 6-3 Checklist for Verifying the vWAAS in Azure Deployment

Task	Description
Viewing vWAAS in Azure vWAAS devices	• On the WAAS Central Manager, navigate to the **Manage Devices** screen. The vWAAS in Azure device type is displayed as **OE-VWAAS-AZURE**. • On the WAAS CLI, use either the **show version** EXEC command or the **show hardware** EXEC command. Output for both commands will include device ID, shown as **OE-VWAAS-AZURE**.
Viewing Boot Information and Diagnostics	On the Azure portal, navigate to **Virtual Machines** > **VM** > **Settings** > **Boot Diagnostics** on the Azure portal.
Verifying CMS Registration	If the Centralized Management System (CMS) is enabled, use the **show cms device status** *name* command to display status for the specified device or device group. **Note** After you have registered the vWAAS in Azure device to the WAAS Central Manager, you must configure the public IP address of the Central Manager. The vWAAS in Azure device can contact the Central Manager only by using the public IP address of the registration. To set the public IP address of the WAAS Central Manager: 1. In the WAAS Central Manager, navigate to **Home** > **Devices** > *Primary-CM-Device* > **Configure** > **Network** > **NatSettings**. 2. In the NAT IP field, enter the public IP address of the Central Manager.
Verifying WAAS Central Manager Address	Use the **show running-config** command to display information about all WAAS device.

Note Whenever ARP cache(s) are cleared or the vWAAS is rebooted, packets may not be forwarded to the next hop in Azure cloud. To ensure that packets are successfully forwarded, use the **ping** EXEC command to update the ARP cache table.