Cisco vWAAS on Microsoft Hyper-V

This chapter describes how to use Cisco vWAAS on Microsoft Hyper-V, and contains the following sections:

About Cisco vWAAS on Microsoft Hyper-V

Microsoft Hyper-V, available for Cisco vWAAS in WAAS Version 6.1.x and later, is a native hypervisor for x86_64 systems to enable platform virtualization. Cisco vWAAS on Microsoft Hyper-V extends Cisco networking benefits to Microsoft Windows Server Hyper-V deployments. It improves utilization, consolidates server workloads, and reduces costs. To achieve this, Cisco vWAAS on Hyper-V uses hardware virtualization to enable multiple operating systems to run on a single host, and allows the operating systems to share the same underlying physical hardware.

Cisco vWAAS on Microsoft Hyper-V supports all the WAN-optimization functionalities that are supported by physical Cisco WAAS devices. Physical memory for Cisco vWAAS on Hyper-V is provided by a Cisco UCS server.

You can configure the VM on Microsoft Hyper-V as virtual Cisco WAAS Central Manager (vCM) or as Cisco vWAAS:

- The Microsoft Hyper-V device configured as Cisco vCM has the same functionality as Cisco WAAS Central Manager, and can manage any other device managed by the Cisco WAAS Central Manager.
- The Microsoft Hyper-V device configured as Cisco vWAAS has the same functionality as the non-Hyper-V Cisco vWAAS. Physical memory for Cisco vWAAS on Microsoft Hyper-V is provided by the Cisco UCS server.

Supported Host Platforms, Software Versions, and Disk Type

Table 5-1 shows the platforms and software versions supported for Cisco vWAAS on Microsoft Hyper-V.

Table 5-1 Platforms and Software Versions Supported for Cisco vWAAS on VMware ESXi

PID and Device Type	Earliest Supported Cisco WAAS Version	Host Platforms	Earliest Supported Host Version	Disk Type
• PID: OE-VWAAS-HYPERV • Device Type: OE-VWAAS-HYPERV	• 6.1x	• Cisco UCS • Cisco UCS-E Series	• Microsoft Windows 2008 R2	• VHD

Cisco vWAAS on Microsoft Hyper-V System Requirements

This section contains the following topics:

System Infrastructure Requirements

Your Cisco WAAS system must have the following to deploy Cisco vWAAS on Microsoft Hyper-V:

- Microsoft Hyper-V Hypervisor: The hypervisor enables multiple operating systems to run on a single host. vWAAS runs as a guest on any host running Hyper-V 2008 R2 or greater.
- Hyper-V Virtual Switch: The Hyper-V Virtual Switch is a software-based Layer 2 switch that connects VMs to both virtual networks and the physical network. It provides policy enforcement for security, isolation, and service levels, and includes features for tenant isolation, traffic shaping, simplified troubleshooting, and protection against malicious virtual machines.

  Hyper-V Virtual Switch is available in Hyper-V Manager when you install the Hyper-V server.
- Microsoft System Center Virtual Machine Manager (SCVMM): Microsoft's virtual machine support center for Windows-based systems. SCVMM upholds Microsoft's focus on efficiency with features to help administrators consolidate multiple physical servers within a central virtualized environment.
- PowerShell: A task-based command-line shell and scripting language built on .NET. PowerShell helps system administrators and power-users rapidly automate tasks that manage operating systems (Linux, macOS, and Windows) and processes. Power Shell commands let you manage computers from the command line.

Hardware Virtualization Requirements

This section describes Cisco vWAAS on Microsoft Hyper-V hardware virtualization requirements for CPU, disk, CD-ROM, and Flash.

- CPU: Cisco vWAAS on Hyper-V supports 2, 4, and 8 CPU configurations. Cisco vWAAS on Microsoft Hyper-V requires a minimum CPU limit.

Note A Cisco vWAAS VM with different CPU configurations works, but is not recommended.

- Disk sizes for Microsoft vWAAS on Microsoft Hyper-V: Disk sizes for Cisco vWAAS on Microsoft Hyper-V are the same as those for VMware ESXi, for each model. For more information on disk sizes for WAAS versions up to Version 6.x, see VMware ESXi Server Datastore Memory and Disk Space for Cisco vWAAS and Cisco vCM Models, page 4-3 in the chapter "Cisco vWAAS on VMware ESXi".
- CD-ROM: Cisco vWAAS on Microsoft Hyper-V supports standard ISO image file for its CD-ROM device.
- Flash: Unlike physical Cisco WAAS devices, Cisco vWAAS on Microsoft Hyper-V does not have access to a separate Flash device. Instead, Cisco vWAAS Flash is installed on the first hard disk, and also uses this first disk for booting. A separate larger disk hosts the caches, including DRE and CIFS. Other Flash functionalities are supported as in VMware ESXi.

Deployment Options for Cisco vWAAS on Microsoft Hyper-V

You can deploy Cisco vWAAS on Microsoft Hyper-V as an installable product or in a standalone role:

- Cisco vWAAS on Microsoft Hyper-V as installable product in the Windows server: Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2.
- Cisco vWAAS on Microsoft Hyper-V as standalone role in the Hyper-V server: Used with Microsoft Hyper-V Server 2012 R2 or Microsoft Hyper-V Server 2016.

Table 5-2 shows Microsoft Hyper-V servers and Microsoft System Center Virtual Machine Manager (SCVMM) support for Cisco vWAAS.

Table 5-2 Cisco vWAAS Support for Microsoft Hyper-V Servers and SCVMM

Microsoft Hyper-V Server	Microsoft SCVMM	Cisco vWAAS Supported
Microsoft Hyper-V Server 2008	SCVMM 2008	No
Microsoft Hyper-V Server 2008 R2	SCVMM 2008 R2	No
Microsoft Hyper-V Server 2008 R2	SCVMM 2012 or SCVMM 2012 R2	Yes
Microsoft Hyper-V Server 2012	SCVMM 2012 or SCVMM 2012 R2	Yes
Microsoft Hyper-V Server 2012 R2	SCVMM 2012 or SCVMM 2012 R2	Yes
Microsoft Hyper-V Server 2016	---	Yes

Note If you want to install SCVMM in Windows 2008 R2, you must first register it with Windows 2012 or Windows 2012 R2.

Table 5-3 shows platforms supported for Cisco vWAAS and Cisco vCM on Microsoft Hyper-V, deployed as a standalone or installable product.

Table 5-3 Platforms Supported for Cisco vWAAS in Microsoft Hyper-Server or Microsoft Windows Server

Standalone Product in Microsoft Hyper-V Server		*Installable Product in Windows Server*
Hyper-V Server 2008 R2	**Hyper-V Server 20012 or 2012 R2 or 2016**	**Windows Server 2012 or 2012 R2**
UCS E-Series and UCS servers	UCS E-Series and UCS servers	UCS E-Series and UCS servers
vCM-100	vCM-100	vCM-100
vCM-500	vCM-500	vCM-500
vCM-1000	vCM-1000	vCM-1000
vCM-2000	vCM-2000	vCM-2000
vWAAS-150 (For Cisco WAAS Version 6.2.1 and later, supported on Cisco Enhanced High-Speed WAN Interfaced Card (EHWIC) and Cisco Network Interfaced Module (NIM.))	vWAAS-150 (For Cisco WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)	vWAAS-150 (For Cisco WAAS Version 6.2.1 and later, supported on Cisco EHWIC and NIM.)
vWAAS-200	vWAAS-200	vWAAS-200
vWAAS-750	vWAAS-750	vWAAS-750
vWAAS-1300	vWAAS-1300	vWAAS-1300
vWAAS-2500	vWAAS-2500	vWAAS-2500
vWAAS-6000	vWAAS-6000	vWAAS-6000
vWAAS-12000	vWAAS-12000	vWAAS-12000
—	vWAAS-50000	vWAAS-50000

OVA Package Formats for Cisco vWAAS on Microsoft Hyper-V

This section contains the following topics:

OVA Package for Cisco vWAAS on Microsoft Hyper-v in Cisco WAAS Version 6.1.x and Later

For Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.1.x and later, Cisco provides an OVA or NPE OVA package for each Cisco vWAAS connection profile (examples shown in Table 5-4) and for each vCM connection profile (examples shown in Table 5-5).

The Cisco OVA package for Cisco vWAAS on Microsoft Hyper-V contains the following:

- SCVMM template file
- WAAS image ISO file
- Virtual Hard Disk (VHD) file for Flash

- PowerShell deployment script for SCVMM
- PowerShell deployment script for standalone hosts

Note For a listing of hypervisor OVA, zip, and tar.gz files for vWAAS, see the Cisco Wide Area Application Services (WAAS) Download Software page and select the WAAS software version used with your vWAAS instance.

Table 5-4 OVA Package Format Examples for Cisco vWAAS on Microsoft Hyper-V for Cisco WAAS Version 6.1.x and Later

Package Format	File Format Example
• Cisco Hyper-V 150 package file	• Hv-Cisco-vWAAS-150-6.2.3d-b-68.zip
• Cisco Hyper-V 150 package file for NPE	• Hv-Cisco-vWAAS-150-6.2.3d-npe-b-68.zip
• Cisco Hyper-V 200 package file	• Hv-Cisco-vWAAS-200-6.2.3d-b-68.zip
• Cisco Hyper-V 200 package file for NPE	• Hv-Cisco-vWAAS-200-6.2.3d-npe-b-68.zip
• Cisco Hyper-V 750 package file	• Hv-Cisco-vWAAS-750-6.2.3d-b-68.zip
• Cisco Hyper-V 750 package file for NPE	• Hv-Cisco-vWAAS-750-6.2.3d-npe-b-68.zip
• Cisco Hyper-V 1300 package file	• Hv-Cisco-vWAAS-1300-6.2.3d-b-68.zip
• Cisco Hyper-V 1300 package file for NPE	• Hv-Cisco-vWAAS-1300-6.2.3d-npe-b-68.zip
• Cisco Hyper-V 2500 package file	• Hv-Cisco-vWAAS-2500-6.2.3d-b-68.zip
• Cisco Hyper-V 2500 package file for NPE	• Hv-Cisco-vWAAS-2500-6.2.3d-npe-b-68.zip

Table 5-5 Cisco OVA Package Formats for Cisco vCM for Cisco WAAS Version 6.1.x and Later

Package Format	File Format Example
• Cisco Hyper-V 100N package file	• Hv-Cisco-100N-6.2.3d-b-68.zip
• Cisco Hyper-V 100N package file for NPE	• Hv-Cisco-100N-6.2.3d-npe-b-68.zip

Unified OVA Package for Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and Later

For Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and later, Cisco provides a single, unified OVA for NPE and non-NPE version of the Cisco WAAS image for all the Cisco vWAAS models for that hypervisor.

Each unified OVA package is a preconfigured VM image that is ready to run on a particular hypervisor.The PowerShell deployment script for each unified ova package file provides the model and other required parameters to launch Cisco vWAAS in WAAS in the required configuration

The following are examples of the unified OVA and NPE OVA package files' filenames for Microsoft Hyper-V:

- OVA: Cisco-HyperV-vWAAS-Unified-6.4.1-b-33.zip
- NPE OVA: Cisco-HyperV-vWAAS-Unified-6.4.1-b-33-npe.zip

The unified OVA package for Microsoft Hyper-V contains the following files.

- SCVMM template file
- WAAS image ISO
- Virtual hard disk file for Flash
- PowerShell deployment script for SCVMM and a set of template .xml files
- PowerShell deployment script for standalone hosts and a set of template .xml files

Installing Cisco vWAAS on Microsoft Hyper-V

This section contains the following topics:

Installing Cisco vWAAS on Microsoft Hyper-V for Cisco vWAAS in Cisco WAAS Version 5.x to 6.2.x

Cisco vWAAS on Microsoft Hyper-V is installed using the Microsoft Virtual Machine Manager (VMM), with the Virtual Hard Disk (VHD) file. During installation, there is an option to import preconfigured and preinstalled Cisco vWAAS images to Microsoft Hyper-V. After you have completed installation, complete the activation and registration process with the procedures described in Activating and Registering Cisco vWAAS on Microsoft Hyper-V, page 5-8.

This section contains the following topic:

Installing Cisco vWAAS on Microsoft Hyper-V with a VHD Template

There are seven VHD templates available for Cisco vWAAS, and four VHD templates available for Cisco vCM.

You can import a pre-configured, model-based VHD file for your deployment. For more information on installing Microsoft Hyper-V with a VHD template, contact your Cisco account representative.

To install Cisco vWAAS on Hyper-V with a VHD template, follow these steps:

Step 1 Download the Cisco vWAAS package to the computer where the SCVMM2012 or the 2012 R2 console is installed.

Step 2 Unzip the Cisco vWAAS package.

Step 3 Log in to the SCVMM console.

Step 4 Launch the PowerShell window that is displayed in the SCVMM.

Step 5 Navigate to the PowerShell script in the uncompressed vWAAS package:
.\Cisco-vWAAS-model-name-6.0.0-ISO\Cisco-vWAAS-model-name-6.0.0-ISO

Step 6 Run the **deploy-vwaas-***model-name* PowerShell script.

Step 7 Follow the procedure that is requested by the deployment script.

Step 8 If your deployment uses a Cisco vWAAS-12000 or Cisco vWAAS-50000 model, you must enter a maximum amount of memory in Non-Uniform Memory Access (NUMA) configuration of at least RAM size or higher, in MB, otherwise the device will not be able to boot up.

Note Entering the maximum memory amounts as shown in Step 9 should be completed *only after* you have deployed Cisco vWAAS in Microsoft Hyper-V (as shown in Step 1 through Step 7).

Step 9 To enter the maximum amount of memory, follow these steps:

a. From the **SC VMM** console, choose **Hardware > Processor > NUMA**.

The **NUMA Configuration** window is displayed.

b. In the **Maximum amount of memory (MB)** field, enter an amount, in MB:

- For Cisco vWAAS-12000, enter an amount of at least 12288 MB.
- For Cisco vWAAS-50000, enter an amount of at least 49152 MB.

Installing Cisco vWAAS on Microsoft Hyper-V in Cisco WAAS Version 6.4.1 and Later

To deploy Microsoft Hyper-V in Cisco vWAAS in WAAS 6.4.1 and later, follow this step:

Step 1 From the Cisco WAAS Installer for Hyper-V, enter the number of your Cisco vWAAS or Cisco vCM model:

```
----- Cisco WAAS Installer for vWAAS -----

    1 . vWAAS-150
    2 . vWAAS-200
    3 . vWAAS-750
    4 . vWAAS-1300
    5 . vWAAS-2500
    6 . vWAAS-6000R
    7 . vWAAS-6000
    8 . vWAAS-12000
    9 . vWAAS-50000
    10 . vCM-100N
    11 . vCM-500N
    12 . vCM-1000N
    13 . vCM-2000N

    Enter vWAAS/vCM model number to install [ ]:
```

The automated Hyper-V package generation copies all the Cisco vWAAS model template XML files in the zip file. Based on your input, the corresponding XML template is registered and used for the specified Cisco vWAAS model deployment.

Activating and Registering Cisco vWAAS on Microsoft Hyper-V

You can manage Cisco vWAAS on Microsoft Hyper-V through the Cisco WAAS Central Manager. Cisco vWAAS on Microsoft Hyper-V supports all the functionalities that are supported by Cisco WAAS devices.

This section describes how to activate and register Cisco vWAAS on Microsoft Hyper-V. For installation information, see Installing Cisco vWAAS on Microsoft Hyper-V, page 5-6.

When a Hyper-V vWAAS VM is started on the Microsoft Hyper-V, it boots up and prompts you to enter basic boot configuration information, including configuring a Microsoft Hyper-V interface and Cisco WAAS Central Manager IP address.

To activate and register Cisco vWAAS on Microsoft Hyper-V, following these steps:

Step 1 Configure the IP address or gateway on the Cisco vWAAS interface. Also configure *name-server*, *domain-name*, and any other static routes, as required.

Step 2 (Optional) If necessary, configure WCCP interception. For more information on configuring WCCP interception, see WCCP Interception. No configuration is necessary for appnav-controller interception.

Step 3 Configure the Cisco WAAS Central Manager IP address so that Cisco vWAAS can be registered with the Cisco WAAS Central Manager.

Step 4 Hyper-V vWAAS connects with the Cisco WAAS Central Manager and registers itself. Hyper-V vWAAS is considered in service after it is registered successfully and it optimizes the connections.

Step 5 The following are scenarios where a Cisco vWAAS cannot not successfully register with the Cisco WAAS Central Manager:

- If Hyper-V vWAAS cannot register with the Cisco WAAS Central Manager, it generates an alarm and does not optimize connections. Contact Cisco Technical Support (TAC) if you need assistance to resolve this situation.
- Hyper-V vWAAS may register successfully with the Cisco WAAS Central Manager, but lose connectivity due to a shutdown or power off. If it remains functional, Cisco vWAAS will continue to optimize the connections in the offline state.
- If you deregister the Hyper-V vWAAS (with the **cms deregister** EXEC command), the Hyper-V vWAAS is removed from service.

Step 6 After Cisco vWAAS on Microsoft Hyper-V is operational on a device, the Cisco WAAS Central Manager displays the following information for the device:

- The Hyper-V device is displayed under the **Devices** > **All Devices** listing under **Device Type** as **OE-VWAAS**.
- The Hyper-V device is displayed in the **Devices** > *device-name* > **Dashboard** as **OE-VWAAS-HYPER-V**.

Traffic Interception Methods for Cisco vWAAS on Microsoft Hyper-V

This section has the following topics:

About Traffic Interception for Cisco vWAAS on Microsoft Hyper-V

When Cisco vWAAS is deployed in Microsoft Hyper-V hosts, the Cisco WAE device is replaced by the Microsoft Hyper-V host. No change is required in the Cisco WAAS traffic interception mechanism in the switches or routers. The WCCP protocol also works like the vWAAS ESXi deployment in the vWAAS Hyper-V deployment.

Cisco vWAAS on Microsoft Hyper-V provides the same WAN acceleration functionality provided by the physical WAN acceleration Cisco WAE device. You can also deploy multiple Cisco vWAAS in one or more Microsoft Hyper-V hosts to form a Cisco WAAS farm in either the edge or the core of the network.

WCCP Interception

WCCP interception, WCCP GRE, and WCCP L2 are supported for all Cisco vWAAS on Microsoft Hyper-V deployments.

To select WCCP as the interception method for a Cisco WAE, follow these overview steps. For a full description of each step, see the *Cisco Wide Area Application Services Configuration Guide*.

Before You Begin

Before you do the following procedure, you should have already configured your router for basic WCCP, as described in the *Cisco Wide Area Application Services Configuration Guide*.

Step 1 From the Cisco WAAS Central Manager menu, choose Devices > *device-name*.

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

The **Interception Configuration** window appears.

Step 3 In the **Interception Method Settings** area, from the **Interception Method** drop-down list, choose **WCCP** to enable the WCCP interception on the vWAAS device.

Step 4 To enable WCCP on the device, in the **WCCP Settings** area, check the **Enable WCCP Service** check box.

Step 5 With WCCP selected, the **Service Type** field displays **TCP Promiscuous**.

Step 6 In the **Service ID1** field, specify the first service ID of the WCCP service pair, with an ID number of 1 to 99.

After you click **Submit**, the **Service ID2** field is filled in with the second service ID of the pair, which is one greater than Service ID1, with an ID number of 2 to 100.

Step 7 To use the default gateway of the WAE as the router to associate with the WCCP TCP promiscuous service, check the **Use Default Gateway as WCCP Router** check box.

If you leave this box unchecked, you can use the **WCCP Routers** field to specify a list of one or more routers by their IP addresses, separated by spaces.

Step 8 (Optional) In the **WCCP Assignment Settings for Load Balancing** area, from the **Assignment Method** drop-down list, choose the type of WAE load-balancing assignment method to use (**Mask** or **Hash**).

- **Mask assignment method selected:** To use a custom mask, enter a value for the source ID mask in the **Source IP Mask** field. The range, in hexadecimal, is 00000000–FE000000. The default is F00. Enter a value for the destination IP mask in the **Destination IP Mask** field. The range, in hexadecimal, is 0000000–FE000000. The default is 0.
- **Hash assignment method selected:** To specify the hash assignment method for the source IP address, check **Hash on Source IP:** and select either **Service ID1** or **Service ID2**.

  After you check a source IP, the complementary destination IP address is automatically selected.

Step 9 In the **WCCP Redirect and Egress Settings** area, from the **Redirect Method** drop-down list, choose **WCCP GRE** or **WCCP L2**.

Step 10 From the **Egress Method** drop-down list, choose **L2** or **IP Forwarding**.

Step 11 In the **Advanced WCCP Settings** area, check the **Enable Flow Protection** check box to keep the TCP flow intact and to avoid overwhelming the device when it comes up or is reassigned new traffic. For more information on flow redirection, see the Information about WCCP Flow Redirection on WAEs" section of the *Cisco Wide Area Application Services Configuration Guide*.

Step 12 In the **Flow Protection Timeout** field, specify the amount of time (in seconds) for which flow protection should be enabled. The default is **0**, which means flow protection stays enabled with no timeout.

Step 13 In the **Shutdown Delay** field, enter a maximum amount of time (in seconds) the chosen device waits to perform a clean shutdown of WCCP. The range is **0** to **86400** seconds. The default is **120** seconds.

Step 14 From the **Failure Detection Timeout** drop-down list, choose a failure detection timeout value: **30**, **15**, or **9** seconds. The default is **30** seconds. The failure detection timeout determines the length of time the router takes to detect a WAE failure.

Step 15 In the **Weight** field, specify the weight to be used for load balancing. The weight value range is **0** to **10000**.

- If the total of all the weight values of the WAEs in a service group is less than or equal to **100**, the weight value represents a literal percentage of the total load redirected to the device for load-balancing purposes.
- If the total of all the weight values of the WAEs in a service group is between **101** and **10000**, the weight value is treated as a fraction of the total weight of all the active WAEs in the service group.

Step 16 In the **Password** field, specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all other WAEs and routers within the cluster with the same password. Passwords must not exceed eight characters in length. Do not use the following characters: space, backwards single quote (‘), double quote (“”), pipe (|), or question mark (?)

Step 17 Re-enter the password in the **Confirm Password** field.

Step 18 Click **Submit** to save the settings.

AppNav Controller Interception

AppNav interception is supported for all Cisco vWAAS on Microsoft Hyper-V deployments, and works the same way as it does in the current ESXi vWAAS models.

AppNav interception enables a vWAAS node to receive traffic optimization from an AppNav controller in an AppNav deployment. If vWAAS VMs are part of an AppNav deployment and are configured as WAAS nodes in an AppNav cluster, you must configure the AppNav-controller interception method. These WAAS nodes receive traffic only from the AppNav controllers; they do not receive traffic directly from routers.

To select AppNav as the interception method, follow these steps:

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

The **Interception Configuration** window appears.

Step 3 From the **Interception Method** drop-down list, choose **appnav-controller** to enable appnav-controller interception on the vWAAS device.

Step 4 Click **Submit**.

Operating Guidelines for Cisco vWAAS on Microsoft Hyper-V

This section has the following topics:

Cisco vWAAS Deployments, Cisco UCS-E Upgrades, and Microsoft Windows Server Updates

Caution Multiple deployments of Cisco vWAAS on the same Hyper-V host *in parallel* may cause unexpected results, due to availability of free space when creating Virtual Hard Disks (VHDs). We recommend that you do *not* deploy multiple Cisco vWAAS on Microsoft Hyper-V in parallel, unless you have verified that you have enough free disk space required for the respective Cisco vWAAS models.

To ensure reliable throughput with the following configuration: **vWAAS on Windows Server 2012 R2 Hyper-V in Cisco UCS-E Series 160S-M3:** we recommend that you do the following:

- Upgrade to the latest Cisco UCS-E firmware (Version 3.1.2) that is available on the Cisco Download Software Page for UCS E-Series Software, UCS E160S M3 Software.
- Verify that you have installed the critical Microsoft Windows Server updates that is available on the Microsoft Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update Rollup page. You can also obtain the standalone update package through the Microsoft Download Center by searching for **KB2887595**.

Configuring NTP Settings for Cisco vWAAS on Microsoft Hyper-V

The Network Time Protocol (NTP) allows synchronization of time and date settings for the different geographical locations of the devices in your Cisco WAAS network, which is important for proper system operation and monitoring. When you configure NTP on Cisco vWAAS on Microsoft Hyper-V, the time gets updated from the NTP server.

Note To ensure that the Cisco vWAAS on Microsoft Hyper-V system clock remains in synchronization with the system clocks of other WAAS devices, especially after a reload of Cisco vWAAS on Microsoft Hyper-V, you must *uncheck* the **Time synchronization** option. This option must be unchecked in the system that you are using for Cisco vWAAS on Microsoft Hyper-V: System Center Virtual Machine Manager (SC VMM) or the Microsoft Hyper-V Manager.

To uncheck the Time Synchronization option for NTP configuration, follow these steps:

Step 1 Uncheck the Time Synchronization option in either the SC VMM or the Hyper-V Manager:

From the Microsoft SC VMM:

a. Select **vWAAS VM**.
b. Choose **Settings** > **Management** > **Integration Services**.
c. Verify that the **Time synchronization** option is unchecked.
d. Click **OK**.

From the Microsoft Hyper-V Manager:

a. Select **vWAAS VM**.
b. Choose **Properties** > **Hardware Configuration** > **Advanced > Integration Services**.
c. Verify that the **Time synchronization** option is unchecked.
d. Click **OK**.

Microsoft Hyper-V High Availability Features

Cisco vWAAS on Microsoft Hyper-V provides multiple high availability solutions, including:

- Live Migration, page 5-12
- Network Interface Card Teaming, page 5-13

Live Migration

Microsoft Hyper-V live migration moves the running VMs with no impact on VM availability to the user. It does this by precopying the memory of the migrating VMs to the destination physical host. The administrator, or the script, that initiates the live migration decides which computer is the destination for the live migration. There is no need for special configuration for the guest operating system, as that is not affected by the live migration.

There are three methods that you can use to initiate a live migration:

- Failover Cluster console
- Virtual Machine Manager Administration console (if Virtual Machine Manager is managing physical hosts that are configured to support live migration)
- A PowerShell or WMI script

The following is a workflow for initiating and completing a live migration:

- **Create a connection between hosts:** The source physical host creates a TCP connection with the destination physical host, which is used to transfer the VM configuration data to the destination physical host. A skeleton VM is set up on the destination physical host, and memory is allocated to the destination VM.
- **Copy the working set to the destination host:** The memory assigned to the migrating VM, called the working set, is copied to the destination physical host. This memory is referred to as the working set of the migrating VM. A page of memory is 4 kB in size.
- **Mark modified memory pages:** The utilized pages within the working set are copied to the destination Microsoft Hyper-V physical host. In addition to copying the working set to the destination physical host, Microsoft Hyper-V on the source physical host monitors the pages in the working set. As the migrating VM modified the memory pages during live migration, Microsoft Hyper-V tracks and marks them as modified.
- **Copy modified memory pages:** During live migration, Microsoft Hyper-V iterates the memory copy process several times. Each time, a smaller number of modified pages need to be copies to the destination physical host. A final memory copy process copies the remaining modified memory pages to the destination physical host.

  The source physical host transfers the register and device state of the VM to the destination physical host. During this stage of live migration, the network bandwidth available between the source and physical host is critical to the speed of the migration. Therefore, 1 Gigabit Ethernet is recommended for this stage of live migration.

  Note The number of pages to be transferred in this stage is dictated by how actively the VM is accessing and modifying memory pages. More modified pages means a longer VM migration time in order to allow all the memory pages to be transferred to the destination physical host.

- **Complete the live migration:** After the modified memory pages have been completely copied to the destination physical host, the destination physical host has an up-to-date working set of the migrated VM. The working set for the migrated VM is present on the destination physical host in the exact state it was in when the migrated VM began the live migration process.

  Note You can cancel the live migration process at any point before this phase of the process.

- **Transfer control of the migrated VM memory and storage:** Control of storage associated with the migrated VM, such as VHD files or passthrough disks, and control of memory (working set) are transferred to the destination physical host.
- **Bring migrated VM online:** The migrated VM is brought online on the destination physical host.

Network Interface Card Teaming

The failure of an individual Microsoft Hyper-V port or virtual network adapter can cause a loss of connectivity for a VM. To prevent this, multiple virtual network adapter are used in a Network Interface Card (NIC) teaming configuration, which provides both high availability and load balancing across multiple physical network interfaces. NIC teaming is also known as network adapter teaming technology and Load Balancing Failover (LBFO).

For vWAAS on Hyper-V, NIC teaming, in Windows Server 2012, enables a virtual machine to have virtual network adapters that are connected to more than one virtual switch, and will still have connectivity even if the network adapter under that virtual switch is disconnected. NIC teaming on Windows Server 2012 supports up to 32 network adapters in a team.

With NIC teaming, you can set up two virtual switches, each connected to its own SR-IOV-capable network adapter. For more information about Cisco vWAAS with SR-IOV, see Cisco vWAAS with Single-Root I/O Virtualization, page 2-7.

NIC teaming then works in one of two ways:

- Each VM can install a virtual function from one or both SR-IOV network adapters. If a adapter disconnection occurs, the traffic can fail over from the primary virtual function to the backup virtual function without losing connectivity.
- Each VM can have a virtual function from one network adapter and a nonvirtual functional interface to the other switch. If the network adapter associated with the virtual function becomes disconnected, the traffic can fail over to the other switch without losing connectivity.

Configuring GPT Disk Format for Cisco vWAAS-50000 on Microsoft Hyper-V with Akamai Connect

The following list shows the disk requirements for Cisco vWAAS on Microsoft Hyper-V for Cisco vWAAS-50000 with Akamai Connect:

- 4-GB Flash
- 48-GB Kdump
- 1500 GB
- 850 GB for disk (for Akamai Connect)

The Microsoft Windows server does not detect disk size more than 2 TB in partition **C:** because it is in Master Boot Record (MBR) format. Therefore, in order to have a disk size more than 2 TB, you need to create partition **D:** in GUID Partition Table (GPT) format.

To convert the Hard Disk Drive (HDD) from MBR format to GPT format, follow these steps:

Step 1 Install windows in one partition of the HDD.

Step 2 After installation is complete, create a new volume to create a new disk partition:

a. Right-click the **Windows** command prompt and then select **Run as Administrator**.

b. Enter the **diskpart** command to enter **DiskPart** command mode.

The DISKPART prompt is displayed.

Step 3 At the **DISKPART** prompt:

a. Run the **create volume** command to create a new volume on the disk.

b. Run the **list disk** command to display a list of disks and associated information, including size, available free space, whether the disk is basic or dynamic.

Note the disk number of the disk for which you want to convert formats.

c. Run the **select disk** *disk-number* command.

d. Run the **clean** command to specify that all sectors on the disk are set to zero.

Note The **clean** command deletes all the data on the disk.

e. Run the **convert gpt** command to convert the disk format to GPT format.

With the GPT format, you can configure RAID capabilities for the HDD, including logical disk handling with RAID-5, logical disk handling with RAID-1, and disk hot-swap support. For more information on RAID support for Cisco WAAS, see the *Cisco Wide Area Application Services Configuration Guide*.