Cisco ACI with Microsoft SCVMM

This chapter contains the following sections:

About Cisco ACI with Microsoft SCVMM

The Application Policy Infrastructure Controller (APIC) integrates with Microsoft VM management systems and enhances the network management capabilities of the platform. The Cisco Application Centric Infrastructure (ACI) integrates at the following levels of the Microsoft VM Management systems:

- Cisco ACI with Microsoft System Center Virtual Machine Manager (SCVMM)—When integrated with Cisco ACI, SCVMM enables communication between ACI and SCVMM for network management.

Note Migrating from SCVMM to SCVMM HA is not supported by Microsoft.

- Cisco ACI and Microsoft Windows Azure Pack—For information about how to set up Cisco ACI and Microsoft Windows Azure Pack, see Cisco ACI with Microsoft Windows Azure Pack Solution Overview.

Cisco ACI with Microsoft SCVMM Solution Overview

At this integration point the Application Policy Infrastructure Controller (APIC) and Microsoft System Center Virtual Machine Manager (SCVMM) communicate with each other for network management. Endpoint groups

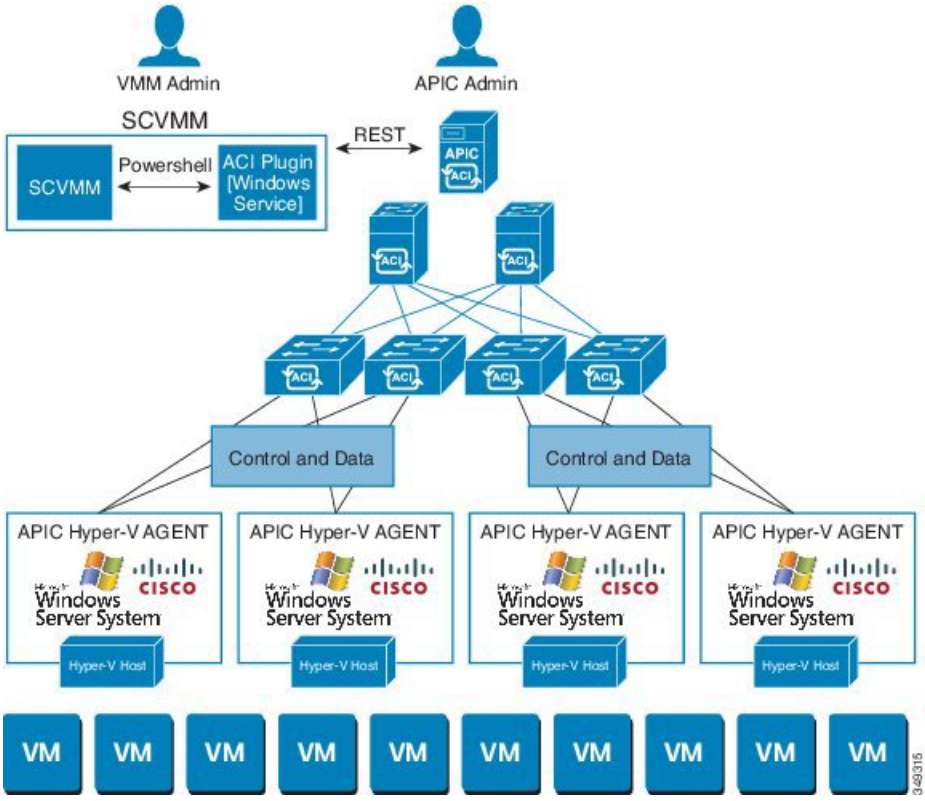
(EPGs) are created in APIC and are created as VM networks in SCVMM. Compute is provisioned in SCVMM and can consume these networks.

Physical and Logical Topology of SCVMM

This figure shows a representative topology of a typical System Center Virtual Machine Manager (SCVMM) deployment with Cisco Application Centric Infrastructure (ACI) fabric. The Microsoft SCVMM service can be deployed as a Standalone Service or as a Highly Available Service on physical hosts or virtual machines, but will logically be viewed as a single SCVMM instance which communicates to the APIC.

Connectivity between an SCVMM Service and the Application Policy Infrastructure Controller (APIC) is over the management network.

Figure 1: Topology with ACI Fabric and SCVMM



About the Mapping of ACI Constructs in SCVMM

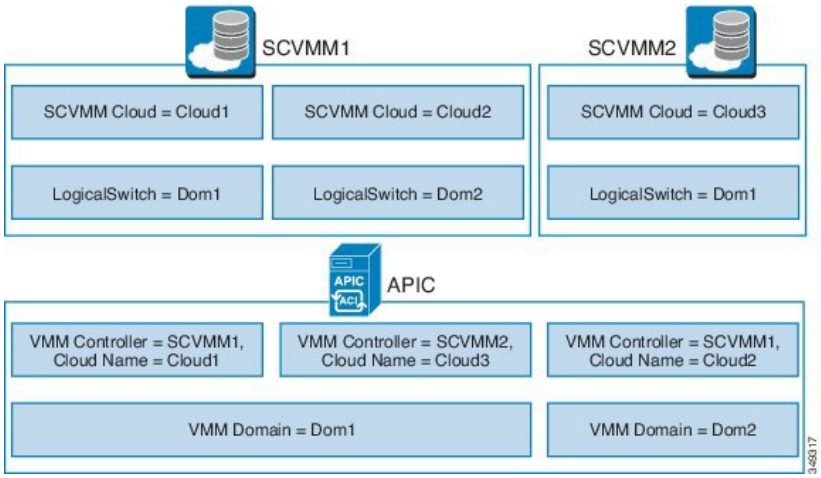
This section shows a table and figure of the mapping of Application Policy Infrastructure Controller (APIC) constructs in Microsoft System Center Virtual Machine Manager (SCVMM).

Table 1: Mapping of APIC and SCVMM constructs

APIC	System Center
VMM Domain	Logical Switch and Logical Network

APIC	System Center
VMM Controller	SCVMM
SCVMM Cloud Name	Cloud (Fabric)
EPG	VM Network
Infrastructure VLAN	One infrastructure VM network for each logical switch

Figure 2: Mapping of ACI and SCVMM constructs



The mapping is bound by the following rule:

- One VMM domain cannot map to the same SCVMM more than once.

SCVMM Fabric Cloud and Tenant Clouds

Microsoft System Center Virtual Machine Manager (SCVMM) provides an object called "Cloud", which acts as a container of logical and physical fabric resources. ACI Integration with SCVMM automatically creates the various logical networking pieces and enables the logical networks at your designated cloud. When configuring ACI Integration with SCVMM, the fabric cloud is the cloud that is specified as the root container on the Application Policy Infrastructure Controller (APIC), while the tenant cloud is an SCVMM cloud that contains a subset of the host groups specified in the fabric cloud. SCVMM contains all the host groups that will be used to deploy the logical switch. Once the fabric cloud is set up and the logical switch has been deployed to the hosts in the host groups, an SCVMM Admin can then create tenant clouds and enable the apicLogicalNetwork on that tenant cloud, enabling Windows Azure Pack tenants to create and deploy tenant networks on the fabric.

Example:

```
SCVMM Cloud Name:  Fabric_Cloud
      Host Groups:  All Hosts
            Host Group HumanResources:
                  HyperV Node:  Node-2-24
            Host Group Engineering:
                  HyperV Node:  Node-2-25

SCVMM Cloud Name:  HR_Cloud
```

```
      Host Groups: HumanResources

SCVMM Cloud Name:  Engineering_Cloud
      Host Groups:  Engineering
```

Getting Started with Cisco ACI with Microsoft SCVMM

This section describes how to get started with Cisco Application Centric Infrastructure (ACI) with Microsoft System Center Virtual Machine Manager (SCVMM).

You must download and unzip the Cisco ACI and Microsoft Integration file for the 2.2(1) release before installing Cisco ACI with Microsoft Windows Azure Pack.

1. Go to Cisco's Application Policy Infrastructure Controller (APIC) Website:

   http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

2. Choose **All Downloads for this Product**.
3. Choose the release version and the **aci-msft-pkg-2.2.1x.zip** file.
4. Click **Download**.
5. Unzip the **aci-msft-pkg-2.2.1x.zip** file.

Note Cisco ACI with Microsoft System Center Virtual Machine Manager (SCVMM) only supports ASCII characters. Non-ASCII characters are not supported.

Ensure that **English** is set in the System Locale settings for Windows, otherwise ACI with SCVMM will not install. In addition, if the System Locale is later modified to a non-English Locale after the installation, the integration components may fail when communicating with the APIC and the ACI fabric.

Prerequisites for Getting Started with Cisco ACI with Microsoft SCVMM

Before you get started, ensure that you have verified that your computing environment meets the following prerequisites:

- Ensure that one of the following Microsoft System Center Virtual Machine Manager (SCVMM) versions with the Administrator Console Builds are met:
  - SCVMM 2019 RTM (Build 10.19.1013.0) or newer
  - SCVMM 2016 RTM (Build 4.0.1662.0) or newer
  - SCVMM 2012 R2 with Update Rollup 9 (Build 3.2.8145.0) or newer
- Ensure that Windows Server 2019, or 2016, or 2012 R2 is installed on the Hyper-V server with the Hyper-V role enabled.

  See Microsoft's documentation.

- Ensure the cloud is configured in SCVMM and appropriate hosts added to that cloud.

  See Microsoft's documentation.

- If there are switches between the Cisco Application Centric Infrastructure (ACI) leaf switch and the Hyper-V host (such as a Fabric Interconnect), you must allow the infrastructure VLAN on these intermediary devices.
- Ensure "default" AEP exists with infrastructure VLAN enabled.
- Ensure you have the Cisco MSI files for APIC SCVMM and the Host Agent.

  See Getting Started with Cisco ACI with Microsoft SCVMM, on page 4.

- Ensure that you scheduled a maintenance window for the SCVMM Installation. The Cisco ACI SCVMM Installation process with automatically restart the current running SCVMM service instance.

Note If the VMs in SCVMM are configured with Dynamic MAC, then it takes time for the APIC to update the VM Inventory as the SCVMM takes time to learn or discover these MAC addresses.

- Ensure the Hyper-V Management Tools is installed on the Hyper-V hosts as well as the SCVMM server.

  To install the Hyper-V Management Tools feature:

  1. In the **Remote Server Administration Tools**, **Add Roles and Features** > **Feature** > **Remote Server Administration Tools** > **Role Administration Tools** > **Hyper-V Management Tools** and finish the wizard to install the feature.
  2. Repeat for each Hyper-V and the SCVMM server.

  This installs the Hyper-V PowerShell cmdlets needed for the APIC SCVMM and host agent.

Installing, Setting Up, and Verifying the Cisco ACI with Microsoft SCVMM Components

This section describes how to install, set up, and verify the Cisco Application Centric Infrastructure (ACI) with Microsoft System Center Virtual Machine Manager (SCVMM) components.

Component	Task
Install the APIC SCVMM Agent on SCVMM or on a Highly Available SCVMM	See Installing the APIC SCVMM Agent on SCVMM, on page 7. See Installing the APIC SCVMM Agent on a Highly Available SCVMM, on page 7 For the Windows Command Prompt method, see Installing the APIC Agent on SCVMM Using the Windows Command Prompt, on page 35.
Generate the OpflexAgent certificate	See Generating APIC OpFlex Certificate, on page 8.

Component	Task
Add the OpFlex certificate policy to APIC	See Adding the OpFlex Certificate Policy to APIC, on page 9.
Install the OpflexAgent certificate	See Installing the OpflexAgent Certificate, on page 10.
Configure APIC IP Settings with APIC credentials on the SCVMM Agent or on the SCVMM Agent on a Highly Available SCVMM	See Configuring APIC IP Settings with OpflexAgent Certificate on the SCVMM Agent, on page 13. or See Configuring APIC IP Settings with OpflexAgent Certificate on the SCVMM Agent on a Highly Available SCVMM, on page 15.
Install the APIC Hyper-V Agent on the Hyper-V server	See Installing the APIC Hyper-V Agent on the Hyper-V Server, on page 16. For the Windows Command Prompt method, see Installing the APIC Hyper-V Agent on the Hyper-V Server Using the Windows Command Prompt , on page 36.
Verify the APIC SCVMM Agent installation on SCVMM or on a Highly Available SCVMM	See Verifying the APIC SCVMM Agent Installation on SCVMM, on page 19. or See Verifying the APIC SCVMM Agent Installation on a Highly Available SCVMM, on page 19.
Verify the APIC Hyper-V Agent installation on the Hyper-V server	See Verifying the APIC Hyper-V Agent Installation on the Hyper-V Server, on page 20.
Create SCVMM Domain Profiles	See Creating SCVMM Domain Profiles, on page 21 and Creating a SCVMM Domain Profile Using the GUI, on page 21. For the NX-OS Style CLI method, see Creating a SCVMM Domain Profile Using the NX-OS Style CLI. For the REST API method, see Creating a SCVMM Domain Profile Using the REST API.
Verify the SCVMM VMM Domain and SCVMM VMM	See Verifying the SCVMM VMM Domain and SCVMM VMM, on page 24.
Deploy the logical switch to the host on SCVMM	See Deploying the Logical Switch to the Host on SCVMM, on page 24.
Enable the Logical Network on Tenant Clouds	See Enabling the Logical Network on Tenant Clouds, on page 25.

Installing the APIC SCVMM Agent on SCVMM

This section describes how to install the Application Policy Infrastructure Controller (APIC) SCVMM agent on System Center Virtual Machine Manager (SCVMM).

Procedure

Step 1 Log in to the SCVMM server with SCVMM administrator credentials.

Step 2 On the SCVMM server in Explorer, locate the **APIC SCVMM Agent.msi** file.

Step 3 Right-click **APIC SCVMM Agent.msi** file and select **Install**.

Step 4 In the **Cisco APIC SCVMM Agent Setup** dialog box, perform the following actions:

a) Click **Next**.

b) Check the **I accept the terms in the License Agreement** check box and click **Next**.

c) Enter your account name and password credentials.

Provide the same credentials that you used for the SCVMM console. The Cisco APIC SCVMM agent requires these credentials for the SCVMM operations to be able to function.

The installation process verifies the entered account name and password credentials. If the installation fails, the SCVMM shows an error message and you must re-enter valid credentials.

d) After successful validation of the account name and password credentials, click **Install**.

e) Click **Finish**.

Note You can configure only one APIC cluster per SCVMM, as one SCVMM can interact with only one APIC cluster.

Installing the APIC SCVMM Agent on a Highly Available SCVMM

This section describes how to install the Application Policy Infrastructure Controller (APIC) SCVMM agent on a Highly Available System Center Virtual Machine Manager (SCVMM).

Procedure

Step 1 Log in to the Current Owner Node of the Highly Available SCVMM installation.

Step 2 On the SCVMM server in File Explorer, locate the **APIC SCVMM Agent.msi** file.

Step 3 Right-click **APIC SCVMM Agent.msi** file and select **Install**.

Step 4 In the **Cisco APIC SCVMM Agent Setup** dialog box, perform the following actions:

a) Click **Next**.

b) Check the **I accept the terms in the License Agreement** check box and click **Next**.

c) Enter your account name and password credentials.

Provide the same credentials that you used for the SCVMM console. The Cisco APIC SCVMM agent requires these credentials for the SCVMM operations to be able to function.

The installation process verifies the entered account name and password credentials. If the installation fails, the SCVMM shows an error message and you must re-enter valid credentials.

d) After successful validation of the account name and password credentials, click **Install**.
e) Click **Finish**.

Step 5 Repeat steps 1-4 for each Standby Node in the Windows Failover Cluster.

Generating APIC OpFlex Certificate

This section describes how to generate APIC OpFlex certificate to secure communication between the Application Policy Infrastructure Controller (APIC) and SCVMM agents.

Note This should only be done once per installation.

Procedure

Step 1 Log in to the SCVMM server, choose **Start** > **Run** > **Windows Powershell**, and then, in the app bar, click **Run as administrator**.

Step 2 Load **ACISCVMMPsCmdlets** and create a new OpflexAgent.pfx certificate file, by entering the following commands:

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.INSCISCO> cd \
PS C:\> cd '.\Program Files (x86)\ApicVMMService'
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets

CommandType     Name                       ModuleName
-----------     ----                       ----------
Cmdlet          Get-ACIScvmmOpflexInfo     ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials        ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert         ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert        ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials        ACIScvmmPsCmdlets
```

Step 3 Generate a new OpFlex Certificate, by entering the following commands. The "New-ApicOpflexCert" PowerShell command will both generate the PFX certificate package file for use on other machines and install the certificate to the local machine's Certificate Store.

```
PS C:\Program Files (x86)\ApicVMMService> $pfxpassword = ConvertTo-SecureString "MyPassword"
 -AsPlainText -Force
PS C:\Program Files (x86)\ApicVMMService> New-ApicOpflexCert -ValidNotBefore 1/1/2015
-ValidNotAfter 1/1/2020
-Email t0@domain.com -Country USA -State CA -Locality "San Jose" -Organization MyOrg
-PfxPassword $pfxpassword
Successfully created:
C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx

PS C:\Program Files (x86)\ApicVMMService>
```

Step 4 Display the certificate information to be used on APIC using the REST API.

See Displaying the Certificate Information to be Used on APIC Using the REST API, on page 9.

Displaying the Certificate Information to be Used on APIC Using the REST API

This section describes how to display the certificate information to be used on APIC using the REST API.

Procedure

To display the certificate information to be used on the APIC.

```
PS C:\Program Files (x86)\ApicVMMService> $pfxpassword = ConvertTo-SecureString "MyPassword"
-AsPlainText -Force
PS C:\Program Files (x86)\ApicVMMService> Read-ApicOpflexCert -PfxFile
"C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx" -PfxPassword $pfxpassword
-----BEGIN CERTIFICATE-----
MIIDojCCAoqgAwIBAgIQHz+F2luuOpFKK0p3jxWRfjANBgkqhkiG9w0BAQ0FADBfMRwwGgYJKoZI
hvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkGA1UECAwCQ0ExDDAKBgNV
BAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwHhcNMTUwMTAxMDAwMDAwWhcNMjAwMTAxMDAw
MDAwWjBfMRwwGgYJKoZIhvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkG
A1UECAwCQ0ExDDAKBgNVBAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCzQS3rvrIdxiHfeAUqtX68CdjIL1+nDtqBH8LzDk0RBVb0KU6V
9cYjCAMwW24FJo0PMt4XblvFJDbZUfjWgEY1JmDxqHIAhKIujGsyDoSZdXaKUUv3ig0bzcswEGvx
khGpAJB8BCnODhD3B7Tj0OD8Gl8asd1u24xOy/8MtMDuan/2b32QRmn1uiZhSX3cwjnPI2JQVIif
n68L12yMcp1kJvi6H7RxVOiES33uz00qjxcPbFhsuoFF1eMT1Ng41sTzMTM+xcE6z72zgAYN6wFq
T1pTCLCC+0u/q1yghYu0LBnARCYwDbe2xoa8ClVcL3XYQlEFlp1+HFfd//p1ro+bAgMBAAGjWjBY
MBIGA1UdEwEB/wQIMAYBAf8CAQAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFGuzLCG5
4DEcP+bPiFbiDjMDQ3tMMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQ0FAAOCAQEANc5kKvN4
Q62tIYa1S2HSyiwjaMq7bXoqIH/ICPRqEXu1XE6+VnLnYqpo3TitLmU4G99uz+aS8dySNWaEYghk
8jgLpu39HH6yWxdPiZlcCQ17J5B5vRu3Xjnc/2/ZPqlQDEElobrAOdTko4uAHG4lFBHLwAZA/f72
5fciyb/pjNPhPgpCP0r7svElQ/bjAP1wK8PhCfd7k2rJx5jHr+YX8SCoM2jKyzaQx1BAdufspX3U
7AWH0aF7ExdWy/hW6CduO9NJf+98XNQe0cNH/2oSKYCl9qEK6FesdOBFvCjlRYR9ENqiY4q7xpyB
tqDkBm80V0JslU2xXn+G0yCWGO3VRQ==
-----END CERTIFICATE-----
PS C:\Program Files (x86)\ApicVMMService>
```

Adding the OpFlex Certificate Policy to APIC

This section describes how to add the OpFlex certificate policy to theApplication Policy Infrastructure Controller (APIC) .

Procedure

Add the AAA policy to allow authenticate this certificate on the APIC server. The Hyper-V agent certificate policy can be added in APIC through the GUI or REST Post:

- GUI method:
  1. **a.** Log in to the APIC GUI, on the menu bar, choose **ADMIN** > **AAA**.
  2. **b.** In the **Navigation** pane, choose **Security Management** > **Local Users** and click on **admin**.

c. In the **PROPERTIES** pane, choose **Actions** > **Create X509 Certificate**, in the drop-down list, enter the name and data.

d. In the **Create X509 Certificate** dialog box, in the **Name** field, you must enter "**OpflexAgent**".

e. On the SCVMM server, enter the output of the PowerShell Read-ApicOpflexCert cmdlet.

f. When you run the Read-ApicOpflexCert cmdlet, provide the full link when prompted for the name of the pfx file: **C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx**, then enter the password.

g. Copy from the beginning of "-----BEGIN CERTIFICATE-----" to the end of "-----END CERTIFICATE-----"and paste it in the **DATA** field.

h. Click **SUBMIT**.

i. In the **PROPERTIES** pane, under the **User Certificates** field, you will see the user certificate displayed.

- REST Post method:

```
POST
http://<apic-ip>/api/policymgr/mo/uni/userext/user-admin.json?rsp-subtree=full
{"aaaUserCert":{"attributes":
{"name":"OpflexAgent", "data":"
-----BEGIN CERTIFICATE-----
MIIDojCCAoqgAwIBAgIQHz+F2luuOpFKK0p3jxWRfjANBgkqhkiG9w0BAQ0FADBfMRwwGgYJKoZI
hvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkGA1UECAwCQ0ExDDAKBgNV
BAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwHhcNMTUwMTAxMDAwMDAwWhcNMjAwMTAxMDAw
MDAwWjBfMRwwGgYJKoZIhvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkG
A1UECAwCQ0ExDDAKBgNVBAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCzQS3rvrIdxiHfeAUqtX68CdjIL1+nDtqBH8LzDk0RBVb0KU6V
9cYjCAMwW24FJo0PMt4XblvFJDbZUfjWgEY1JmDxqHIAhKIujGsyDoSZdXaKUUv3ig0bzcswEGvx
khGpAJB8BCnODhD3B7Tj0OD8Gl8asd1u24xOy/8MtMDuan/2b32QRmn1uiZhSX3cwjnPI2JQVIif
n68L12yMcp1kJvi6H7RxVOiES33uz00qjxcPbFhsuoFF1eMT1Ng41sTzMTM+xcE6z72zgAYN6wFq
T1pTCLCC+0u/q1yghYu0LBnARCYwDbe2xoa8ClVcL3XYQlEFlp1+HFfd//p1ro+bAgMBAAGjWjBY
MBIGA1UdEwEB/wQIMAYBAf8CAQAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFGuzLCG5
4DEcP+bPiFbiDjMDQ3tMMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQ0FAAOCAQEANc5kKvN4
Q62tIYa1S2HSyiwjaMq7bXoqIH/ICPRqEXu1XE6+VnLnYqpo3TitLmU4G99uz+aS8dySNWaEYghk
8jgLpu39HH6yWxdPiZlcCQ17J5B5vRu3Xjnc/2/ZPqlQDEElobrAOdTko4uAHG4lFBHLwAZA/f72
5fciyb/pjNPhPgpCP0r7svElQ/bjAP1wK8PhCfd7k2rJx5jHr+YX8SCoM2jKyzaQx1BAdufspX3U
7AWH0aF7ExdWy/hW6CduO9NJf+98XNQe0cNH/2oSKYCl9qEK6FesdOBFvCjlRYR9ENqiY4q7xpyB
tqDkBm80V0JslU2xXn+G0yCWGO3VRQ==
-----END CERTIFICATE-----
```

Installing the OpflexAgent Certificate

This section describes how to install the OpflexAgent Certificate.

Procedure

Step 1 Log in to the SCVMM server with administrator credentials.

Step 2 Use one of the following methods:

- For large-scale deployments, see Microsoft's documentation for Deploy Certificates by Using Group Policy:

https://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx.

- For small-scale deployments follow these steps:

  You must add OpFlex security certificate to the local machine. The Microsoft SCVMM agent has a security certificate file named **OpflexAgent.pfx** located in the **C:\Program Files (x86)\ApicVMMService** folder on the SCVMM server. If the following steps are not performed on your SCVMM servers, the APIC SCVMM Agent cannot communicate with the Application Policy Infrastructure Controller (APIC) .

  Install the OpFlex security certificate on the SCVMM Windows Server 2012 local machine's certificate repository. On each SCVMM server, install this certificate by performing the following steps:

  a. Choose **Start** > **Run**.

  b. Enter **mmc** and click **OK**.

  c. In the **Console Root** window, on the menu bar, choose **Add/Remove Snap-in**.

  d. In the **Available Snap-ins** field, choose **Certificates** and click **Add**.

  e. In the **Certificates snap-in** dialog box, choose the **Computer Account** radio button, and click **Next**.

  f. In the **Select Computer** dialog box, choose the **Local Computer** radio button, and click **Finish**.

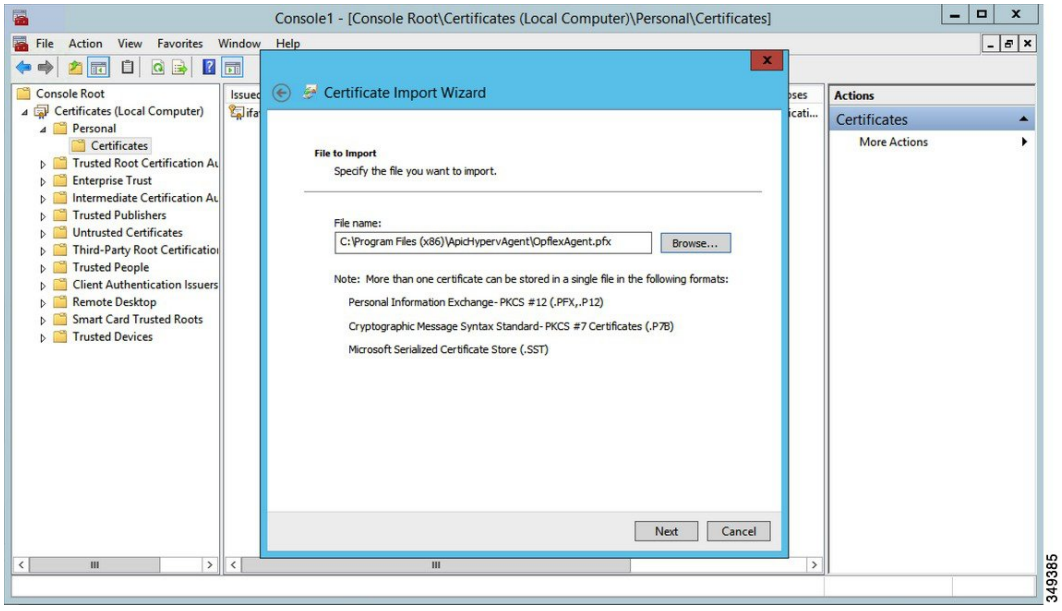
  g. Click **OK** to go back to the main **MMC Console** window.

  h. In the **MMC Console** window, double-click **Certificates (local computer)** to expand its view.

  i. Right-click **Certificates** under **Personal** and choose **All Tasks** > **Import**.

  j. In the **Certificates Import Wizard** dialog box, perform the following actions:

    1. Click **Next**.
    2. Browse to the **Opflex Agent** file and click **Next**.



  k. Enter the password for the certificate that was provided when you installed MSI.

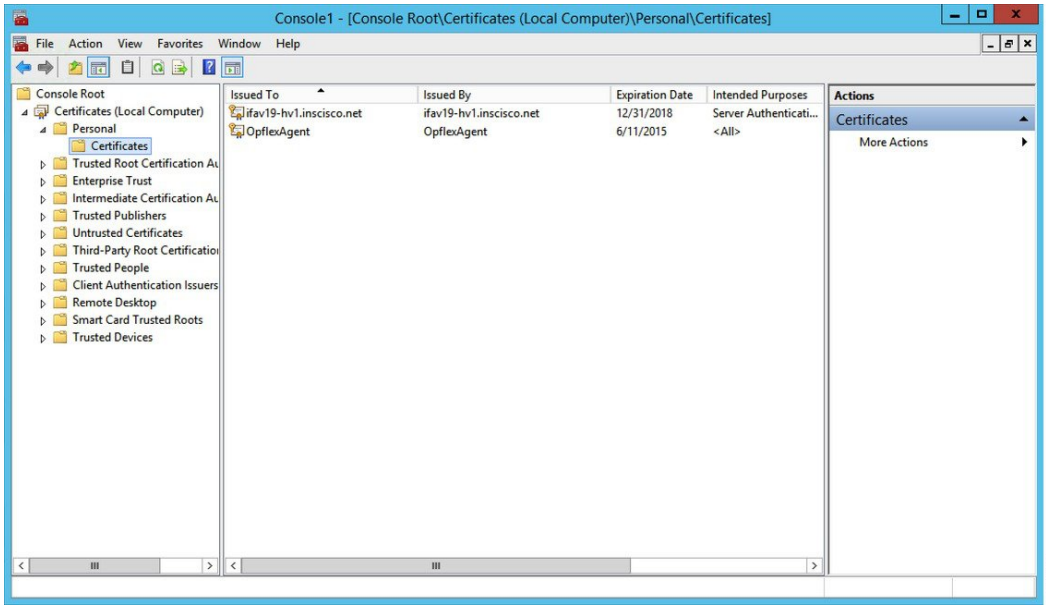
l. You must choose the **Mark this key as exportable. This will allow you to back up or transport your keys at a later time** radio button.

m. Choose the **Include all extended properties** radio button.

n. Choose the **Place all certificates in the following store** radio button, browse to locate **Personal**, and click **Next**.

o. Click **Finish**.

p. Click **OK**.



Step 3 Repeat steps 1 through 5 for each SCVMM server.

Replacing the OpFlex Certificate

Use this procedure to replace the OpFlex certificate.

Note Run this procedure only during a maintenance window.

Procedure

Step 1 Move all EPGs associated SCVMM domains to Pre-Provision mode. Follow these steps:

a) Log in to Cisco APIC.

b) Navigate to **Tenants** > *Tenant_Name* > **Application Profile** > *Application Profile_Name* > **Application EPGs** > *EPG_Name* > **Domains**.

c) Select the SCVMM Domain, and select **Pre-provision** for the **Resolution Immediacy** field.

Step 2 Verify to confirm if zero-MAC IDEps are deployed to the leafs of all the targeted EPGs/VLANs.

Traffic will continue to flow regardless of what occurs on the ACI Agents on SCVMM and Hyper-V hosts.

Step 3 Disable the ACI SCVMM agent.

SCVMM controller goes offline.

Step 4 Delete the old OpflexAgent certificates from the SCVMM HA cluster.

Step 5 Delete the old OpflexAgent user certificate from the APIC admin user.

Navigate to **Administration** > **Users** > **Admin** > **User Certificates**.

OpFlex status faults on Hyper-V nodes are displayed.

Step 6 Regenerate a new OpFlexAgent Certificate. For the detailed procedure, see Generating APIC OpFlex Certificate, on page 8.

As part of the (re)generation, the certificate is automatically installed on the SCVMM which generated the certificate.

a) Install the OpflexAgent Certificate on the other SCVMM HA node. For the detailed procedure, see Installing the APIC SCVMM Agent on SCVMM, on page 7.

b) Create the user certificate policy under APIC > **Administration** > **Users** > **Admin** > **User Certificates**. Add the OpFlex agent certificate here based on the newly created certificate.

Step 7 Start the ACI SCVMM Agent.

a) Verify the SCVMM controller moves to the *Online* state on APIC.

Note Do not proceed until the SCVMM Controller on APIC moves to the *Online* state.

Step 8 Disable the Hyper-V agent.

Step 9 Delete the old OpFlexAgent Certificate from your Hyper-V Nodes(s).

Step 10 Install the new OpFlexAgent on all the Hyper-V Node(s). For the detailed procedure, see Installing the APIC Hyper-V Agent on the Hyper-V Server, on page 16.

Step 11 Start the ACI Hyper-V Agent on all the Hyper-V Node(s).

Step 12 Verify the Opflex status moves to the *Online* status for all the Hyper-V Nodes. For the detailed procedure, see Verifying the APIC Hyper-V Agent Installation on the Hyper-V Server, on page 20.

Note Ensure and wait until the OpFlex status is displayed as *Online* for all the target Hyper-V Nodes.

Step 13 Move the EPGs from Pre-Provision to its previous configuration.

Configuring APIC IP Settings with OpflexAgent Certificate on the SCVMM Agent

This section describes how to configure the Cisco Application Policy Infrastructure Controller (APIC) IP settings with OpflexAgent Certificate on the System Center Virtual Machine Manager (SCVMM) agent.

Procedure

Step 1 Log in to the SCVMM server and choose **Start** > **Run** > **Windows PowerShell**.

Step 2 Load **ACISCVMMPsCmdlets** by entering the following commands:

Example:

Note Get-ApicCredentials and Set-ApicCredentials are now deprecated, use Get-ApicConnInfo and Set-ApicConnInfo.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.INSCISCO> cd \
PS C:\> cd '.\Program Files (x86)\ApicVMMService'
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Get-ACIScvmmOpflexInfo                             ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials                                ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert                                 ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert                                ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials                                ACIScvmmPsCmdlets


PS C:\Program Files (x86)\ApicVMMService>
```

Step 3 Set up Cisco APIC connection parameters for the SCVMM agent by entering the following commands, adding at least one Cisco APIC:

```
PS C:\Users\administrator.APIC> Set-ApicConnInfo -ApicNameOrIPAddress APIC_1_IP
-CertificateSubjectName OpflexAgent

Apic Credential is successfully set to APIC SCVMM service agent.
```

If you enter more than one -ApicNameOrIPAddress, use the following format:
"*APIC_1_IP*;*APIC_2_IP*;*APIC_3_IP*;*APIC_N_IP*"

If you enter the wrong information in **Set-ApicCredentials**, the information fails to apply and validate on the Cisco APIC. This information is not preserved.

```
PS C:\Program Files (x86)\ApicVMMService> Set-ApicConnInfo -ApicNameOrIPAddress APIC_1_IP
-CertificateSubjectName O
pflexAgentWrong
Failed cmdlet with Error: Invalid APIC Connection Settings.
Set-ApicConnInfo : The remote server returned an error: (400) Bad Request.
At line:1 char:1
+ Set-ApicConnInfo -ApicNameOrIPAddress APIC_1_IP -CertificateSubjectName Opf ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-ApicConnInfo], WebException
    + FullyQualifiedErrorId : Failed cmdlet with Error: Invalid APIC Connection
Settings.,Cisco.ACI.SCVMM.
    PowerShell.SetApicConnInfo
```

Step 4 Verify that the Cisco APIC connection parameters are set properly on Cisco APIC SCVMM Agent by entering the following command:

```
PS C:\Program Files (x86)\ApicVMMService> Get-ApicConnInfo


EndpointAddress        :
Username               :
```

```
Password               :
ApicAddresses          : 172.23.139.224
ConnectionStatus       : Connected
adminSettingsFlags     : 0
certificateSubjectName : OpflexAgent
ExtensionData          :


PS C:\Program Files (x86)\ApicVMMService>
```

Configuring APIC IP Settings with OpflexAgent Certificate on the SCVMM Agent on a Highly Available SCVMM

This section describes how to configure the Application Policy Infrastructure Controller (APIC) IP settings with OpflexAgent Certificate on the System Center Virtual Machine Manager (SCVMM) agent.

Procedure

Step 1 Log in to the Owner Node SCVMM server and choose **Start** > **Run** > **Windows PowerShell**.

Step 2 Load **ACISCVMMPsCmdlets** by entering the following commands:

Example:

Note Get-ApicCredentials and Set-ApicCredentials are now deprecated, use Get-ApicConnInfo and Set-ApicConnInfo.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.INSCISCO> cd \
PS C:\> cd '.\Program Files (x86)\ApicVMMService'
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Get-ACIScvmmOpflexInfo                             ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials                                ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert                                 ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert                                ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials                                ACIScvmmPsCmdlets


PS C:\Program Files (x86)\ApicVMMService>
```

Step 3 Set up Cisco APIC connection parameters for the SCVMM agent by entering the following commands, adding one or more Cisco APIC:

```
PS C:\Users\administrator.APIC> Set-ApicConnInfo -ApicNameOrIPAddress APIC_1_IP
-CertificateSubjectName OpflexAgent

Apic Credential is successfully set to APIC SCVMM service agent. 10:25 AM
```

If you enter more than one -ApicNameOrIPAddress, use the following format:

```
"APIC_1_IP;APIC_2_IP;APIC_3_IP;APIC_N_IP"
```

If you enter the wrong information in **Set-ApicCredentials**, the information fails to apply and validate on the Cisco APIC. This information is not preserved.

```
PS C:\Program Files (x86)\ApicVMMService> Set-ApicConnInfo -ApicNameOrIPAddress APIC_1_IP
-CertificateSubjectName O
pflexAgentWrong
Failed cmdlet with Error: Invalid APIC Connection Settings.
Set-ApicConnInfo : The remote server returned an error: (400) Bad Request.
At line:1 char:1
+ Set-ApicConnInfo -ApicNameOrIPAddress APIC_1_IP -CertificateSubjectName Opf ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-ApicConnInfo], WebException
    + FullyQualifiedErrorId : Failed cmdlet with Error: Invalid APIC Connection
Settings.,Cisco.ACI.SCVMM.
    PowerShell.SetApicConnInfo
```

Step 4 Verify that the Cisco APIC connection parameters are set properly on the Cisco APIC SCVMM Agent by entering the following command:

```
PS C:\Program Files (x86)\ApicVMMService> Get-ApicConnInfo


EndpointAddress        :
Username               :
Password               :
ApicAddresses          : 172.23.139.224
ConnectionStatus       : Connected
adminSettingsFlags     : 0
certificateSubjectName : OpflexAgent
ExtensionData
```

Installing the APIC Hyper-V Agent on the Hyper-V Server

This section describes how to install the APIC Hyper-V agent on the Hyper-V server.

Before you begin

Scheduled downtime for the Hyper-V node. For more information regarding Hyper-V Maintenance Mode behavior, see: https://technet.microsoft.com/en-us/library/hh882398.aspx

Procedure

Step 1 Log on to the SCVMM server and bring the Hyper-V node into Maintenance Mode.

Step 2 Log in to the Hyper-V server with administrator credentials.

Step 3 On the Hyper-V server in File Explorer, locate the **APIC Hyper-V Agent.msi** file.

Step 4 Right-click the **APIC Hyper-V Agent.msi** file and choose **Install**.

Step 5 In the **ApicHypervAgent Setup** dialog box, perform the following actions:

a) Check the **I accept the terms in the License Agreement** check box.
b) Click **Install**.
c) Click **Finish**.

Step 6 Follow the steps in Microsoft's documentation to view and bring the apicVSwitch Logical Switch into compliance. Also referred to in this guide as Host Remediate or Logical Switch Instance Remediation: https://technet.microsoft.com/en-us/library/dn249415.aspx

Step 7 Use one of the following methods:

- For large-scale deployments, see Microsoft's documentation for Deploy Certificates by Using Group Policy:

  https://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx

- For small-scale deployments follow these steps:

  You must add OpFlex security certificate in the local system. The Microsoft Hyper-V agent has a security certificate file named **OpflexAgent.pfx** located in the **C:\Program Files (x86)\ApicVMMService** folder on the SCVMM server. If the following steps are not performed on your Hyper-V servers, the APIC Hyper-V Agent cannot communicate with the Cisco Application Centric Infrastructure (ACI) fabric leaf switches.

  Install the OpFlex security certificate on the Hyper-V Windows Server 2012 local machine's certificate repository. On each Hyper-V server, install this certificate by performing the following steps:

  a. Choose **Start** > **Run**.

  b. Enter **mmc** and click **OK**.

  c. In the **Console Root** window, on the menu bar, choose **Add/Remove Snap-in**.

  d. In the **Available Snap-ins** field, choose **Certificates** and click **Add**.

  e. In the **Certificates snap-in** dialog box, choose the **Computer Account** radio button, and click **Next**.

  f. In the **Select Computer** dialog box, choose the **Local Computer** radio button, and click **Finish**.

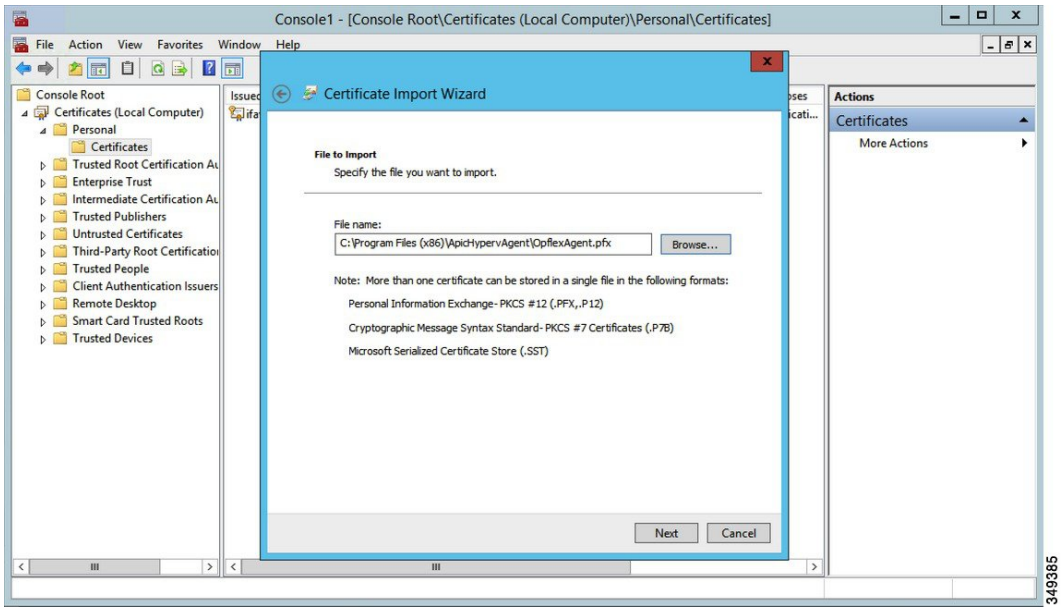
  g. Click **OK** to go back to the main **MMC Console** window.

  h. In the **MMC Console** window, double-click **Certificates (local computer)** to expand its view.

  i. Right-click **Certificates** under **Personal** and choose **All Tasks** > **Import**.

  j. In the **Certificates Import Wizard** dialog box, perform the following actions:

  1. Click **Next**.
  2. Browse to the **Opflex Agent** file and click **Next**.



k. Enter the password for the certificate that was provided when you installed MSI.

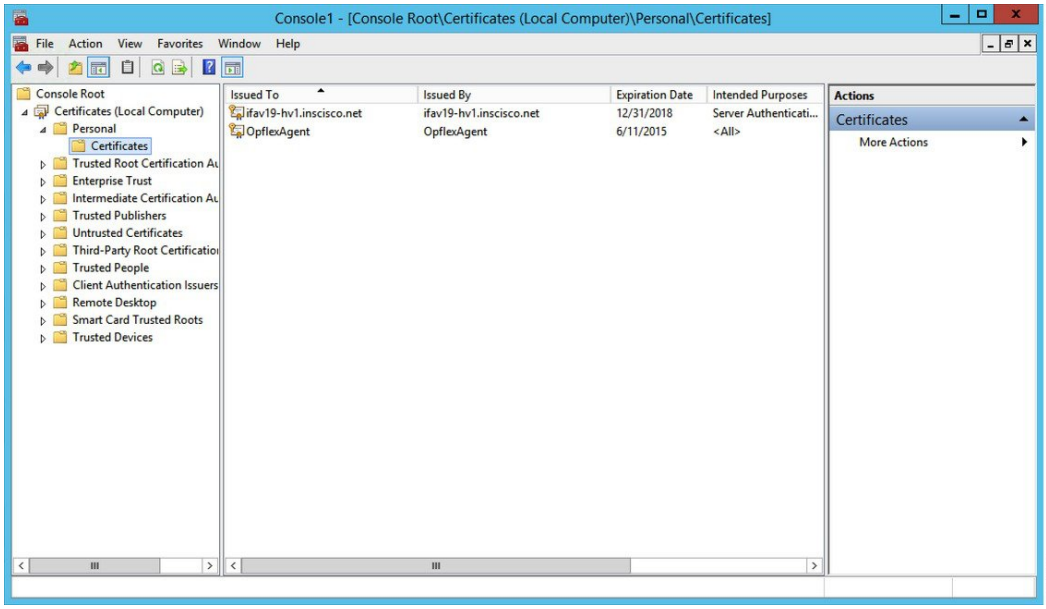
l. You must choose the **Mark this key as exportable. This will allow you to back up or transport your keys at a later time** radio button.

m. Choose the **Include all extended properties** radio button.

n. Choose the **Place all certificates in the following store** radio button, browse to locate **Personal**, and click **Next**.

o. Click **Finish**.

p. Click **OK**.



Step 8 Log on to the SCVMM Sserver and bring the Hyper-V node out of Maintenance Mode.

Step 9 Repeat steps 1 through 8 for each Hyper-V server.

Verifying the Installation of Cisco ACI with Microsoft SCVMM

Verifying the APIC SCVMM Agent Installation on SCVMM

This section describes how to verify the APIC SCVMM agent installation on System Center Virtual Machine Manager (SCVMM).

Procedure

Step 1 Choose **Start** > **Control Panel**.

Step 2 In the **Control Panel** window, enter **Control Panel\Programs\Programs and Features** in the address bar.

Step 3 Locate **Cisco APIC SCVMM Agent**. If **Cisco APIC SCVMM Agent** is present, then the product is installed.

If **Cisco APIC SCVMM Agent** is not present, then the product is not installed. See the Installing the APIC SCVMM Agent on SCVMM, on page 7 or Installing the APIC Agent on SCVMM Using the Windows Command Prompt, on page 35 section.

Step 4 Verify the **ApicVMMService** is in RUNNING state through the GUI or CLI:

- GUI method: Choose **Start** > **Run** and enter **services.msc**. In the **Service** pane, locate the **ApicVMMService** and verify the state is RUNNING.
- CLI method: From the command prompt, enter the **sc.exe query ApicHypervAgent** command and verify the state is RUNNING:

```
sc.exe query ApicVMMService

SERVICE_NAME: ApicVMMService
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
```

Verifying the APIC SCVMM Agent Installation on a Highly Available SCVMM

This section describes how to verify the APIC SCVMM agent installation on a Highly Available System Center Virtual Machine Manager (SCVMM).

Procedure

Step 1 Choose **Start** > **Control Panel**.

Step 2 In the **Control Panel** window, enter **Control Panel\Programs\Programs and Features** in the address bar.

Step 3 Locate **Cisco APIC SCVMM Agent**. If **Cisco APIC SCVMM Agent** is present, then the product is installed.

If **Cisco APIC SCVMM Agent** is not present, then the product is not installed. See the Installing the APIC SCVMM Agent on SCVMM, on page 7 or Installing the APIC Agent on SCVMM Using the Windows Command Prompt, on page 35 section.

Step 4 Verify the **ApicVMMService** is in RUNNING state through the GUI or CLI:

- GUI method: Choose **Start** > **Run** and enter **services.msc**. In the **Service** pane, locate the **ApicVMMService** and verify the state is RUNNING.
- CLI method: From the command prompt, enter the **sc.exe query ApicHypervAgent** command and verify the state is RUNNING:

```
sc.exe query ApicVMMService

SERVICE_NAME: ApicVMMService
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
```

Step 5 Choose **Start** > **PowerShell** and enter the following commands:

```
PS C:\Users\administrator.APIC\Downloads> Get-ClusterResource -Name ApicVMMService

Name            State         OwnerGroup          ResourceType
----            -----         ----------          ------------
ApicVMMService  Online        clustervmm07-ha     Generic Service

PS C:\Users\administrator.APIC\Downloads> Get-ClusterCheckpoint -ResourceName ApicVMMService

Resource        Name
--------        ----
ApicVMMService  SOFTWARE\Wow6432Node\Cisco\Apic

PS C:\Users\administrator.APIC\Downloads> Get-ClusterResourceDependency -Resource
ApicVMMService

Resource        DependencyExpression
--------        --------------------
ApicVMMService  ([VMM Service clustervmm07-ha])
```

Verifying the APIC Hyper-V Agent Installation on the Hyper-V Server

This section describes how to verify the APIC Hyper-V agent installation on the Hyper-V server.

Procedure

Step 1 Choose **Start** > **Control Panel**.

Step 2 In the **Control Panel** window, enter **Control Panel\Programs\Programs and Features** in the address bar.

Step 3 Locate **Cisco APIC Hyperv Agent**. If **Cisco APIC Hyperv Agent** is present, then the product is installed.

If **Cisco APIC Hyperv Agent** is not present, then the product is not installed. See the Installing the APIC Hyper-V Agent on the Hyper-V Server, on page 16 or Installing the APIC Hyper-V Agent on the Hyper-V Server Using the Windows Command Prompt , on page 36 section.

Step 4 Verify the **ApicHypervAgent** is in RUNNING state through the GUI or CLI:

- GUI method: Choose **Start** > **Run** and enter **services.msc**. In the **Service** pane, locate the **ApicHypervAgent** and verify the state is RUNNING.
- CLI method: From the command prompt, enter the **sc.exe query ApicHypervAgent** command and verify the state is RUNNING:

```
sc.exe query ApicHypervAgent

SERVICE_NAME: ApicHypervAgent
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
```

Setting Up ACI Policies

Creating SCVMM Domain Profiles

In this section, the examples of a VMM domain are System Center Virtual Machine Manager (SCVMM) domains. The example tasks are as follows:

- Configuring the VMM domain name and SCVMM controller.
- Creating an attach entity profile and associating it to the VMM domain.
- Configuring a pool.
- Verifying all configured controllers and their operational states.

Creating a SCVMM Domain Profile Using the GUI

Before you begin

Before you create a VMM domain profile, you must establish connectivity to an external network using in-band or out-of-band management network on the Application Policy Infrastructure Controller (APIC).

Procedure

Step 1 Log in to the APIC GUI, and then choose **Virtual Networking** > **Inventory**.

Step 2 In the **Navigation** pane, expand **VMM Domains**, right-click the VM Provider **Microsoft** and choose **Create SCVMM Domain**.

Step 3 In the **Create SCVMM domain** dialog box, in the **Name** field, enter the domain's name (productionDC).

Step 4 Optional: In the **Delimiter** field, enter one of the following: |, ~, **!**, **@**, ^, +, or =. If you do not enter a symbol, the system default | delimiter will appear in the policy.

Step 5 In the **Associated Attachable Entity Profile** field, from the drop-down list, choose **Create Attachable Entity Profile**, and perform the following actions to configure the list of switch interfaces across the span of the VMM domain:

a) In the **Create Attachable Access Entity Profile** dialog box, in the **Profile** area, in the **Name** field, enter the name (profile1), and click **Next**.
b) In the **Association to Interfaces** area, expand **Interface Policy Group**.
c) In the **Configured Interface, PC, and VPC** dialog box, in the **Configured Interfaces, PC, and VPC** area, expand **Switch Profile**.
d) In the **Switches** field, from the drop-down list, check the check boxes next to the desired switch IDs (101 and 102).
e) In the **Switch Profile Name** field, enter the name (swprofile1).
f) Expand the + icon to configure interfaces.
g) Choose the appropriate interface ports individually in the switch image (interfaces 1/1, 1/2, and 1/3). The **Interfaces** field gets populated with the corresponding interfaces.
h) In the **Interface Selector Name** field, enter the name (selector1).
i) In the **Interface Policy Group** field, from the drop-down list, choose **Create Interface Policy Group**.
j) In the **Create Access Port Policy Group** dialog box, in the **Name** field, enter the name (group1).
k) Click **Submit**.
l) Click **Save**, and click **Save** again.
m) Click **Submit**.
n) In the **Select the interfaces** area, under **Select Interfaces**, click the **All** radio button.
o) Verify that in the **vSwitch Policies** field, the **Inherit** radio button is selected.
p) Click **Finish**.

The **Attach Entity Profile** is selected and is displayed in the **Associated Attachable Entity Profile** field.

Step 6 In the **VLAN Pool** field, from the drop-down list, choose **Create VLAN Pool**. In the **Create VLAN Pool** dialog box, perform the following actions:

a) In the **Name** field, enter the VLAN pool name (VlanRange).
b) In the **Allocation Mode** field, verify that the **Dynamic Allocation** radio button is selected.
c) Expand **Encap Blocks** to add a VLAN block. In the **Create Ranges** dialog box, enter a VLAN range.

Note We recommend a range of at least 200 VLAN numbers. Do not define a range that includes the reserved VLAN ID for infrastructure network because that VLAN is for internal use.

d) Click **OK**, and click **Submit**.

In the **VLAN Pool** field, "VlanRange-dynamic" is displayed.

Step 7 Expand **SCVMM**. In the **Create SCVMM Controller** dialog box, verify that the **Type** is **SCVMM**, and then perform the following actions:

a) In the **Name** field, enter the name (SCVMM1).
b) To connect to a SCVMM HA Cluster, specify the SCVMM HA Cluster IP address or the SCVMM Cluster Resource DNS name, which was specified during the SCVMM HA installation. See How to Connect to a Highly Available VMM Management Server by Using the VMM Console: https://technet.microsoft.com/en-us/library/gg610673.aspx
c) In the **Host Name (or IP Address)** field, enter the Fully Qualified Domain Name (FQDN) or IP address of your SCVMM.
d) In the **SCVMM Cloud Name** field, enter the SCVMM cloud name (ACI-Cloud).

e) Click **OK**.
f) In the **Create SCVMM Domain** dialog box, click **Submit**.

Step 8 Verify the new domain and profiles, by performing the following actions:

a) On the menu bar, choose **Virtual Networking** > **Inventory**.
b) In the navigation pane, choose **VMM Domains** > **Microsoft** > **productionDC** > **SCVMM1**.
c) In the **Work** pane, view the VMM domain name to verify that the controller is online.
d) In the **Work** pane, the SCVMM1 properties are displayed including the operational status. The displayed information confirms that connection from the APIC controller to the SCVMM server is established, and the inventory is available.

Configuring the Port Channel Policy

This section describes how to configure the port channel policy.

Modifying the Interface Port Channel Policy

The Cisco ACI SCVMM Agent synchronizes the SCVMM uplink port profile with the aggregated interface port channel policies and performs an automated update when there are changes to the policy.

To update the policy for Hyper-V servers, perform the following steps.

Procedure

Step 1 Log in to the Cisco APIC GUI, and on the menu bar, choose **Fabric** > **Access Policies**.
Step 2 In the navigation pane, expand **Interfaces** > **Leaf Interfaces** > **Policy Groups**.
Step 3 Choose the policy group and check the name of the policy group.
Step 4 Navigate to the policy group and update it based on your requirements (for example, LACP or MAC pinning).

Overriding the VMM Domain VSwitch Policies for Blade Servers

When Blade servers are connected to ACI fabric interface port channel policy will be used between interface and fabric interconnect. When fabric interconnect is configured for LACP you will need to configure the Hyper-V server for MAC pinning mode.

To configure the Hyper-V server for MAC pinning mode perform the following steps.

Procedure

Step 1 Log in to the APIC GUI, on the menu bar, choose **Virtual Networking**.
Step 2 In the navigation pane, expand **VMM Domains** > **Microsoft** > ***Domain_Name***.
Step 3 In the **Work** pane, click **ACTIONS** and choose **Create VSwitch Policies**.
Step 4 On the port channel policy, select the existing policy for mac pinning or create a new policy.

Note If the hosts are already connected to logical switch, then the SCVMM admin should perform host remediate for all the hosts for uplink policy to take effect.

Verifying the SCVMM VMM Domain and SCVMM VMM

Procedure

In the System Center Virtual Machine Manager Console GUI, the following object has been created by the SCVMM agent for the newly created SCVMM VMM domain and VMM Controller's rootContName (SCVMM Cloud Name):

a) Click **Fabric** at the bottom left side pane and under fabric verify the following objects:

Note Do not manually change this setting through the SCVMM GUI. It is managed via the ACI Agent installed on the SCVMM Server. The SCVMM Port Profile configuration is set based on APIC configuration, see Configuring the Port Channel Policy section.

.

Example:

1. Choose **Networking** > **Logical Switches** and in the right side pane, the logical switch name is **apicVSwitch_*VMMdomainName*** > **Properties**.

   ACI/SCVMM Integration only supports **Logical Switch** > **Uplink Mode as Team**.

2. Choose **Networking** > **Logical Networks** and in the right side pane, the logical network name is **apicLogicalNetwork_*VMMdomainName***.

3. Choose **Networking** > **Port Profiles** and in the right side pane, the port profile name is **apicUplinkPortProfile_*VMMdomainName*** > **Properties**.

   LACP uplink configuration: Load Balancing Algorithm: Address Hash, Teaming Mode: LACP.

   All other uplink configurations (ex: mac-pinning): Load Balancing Algorithm: Hyper-V Port, Teaming Mode: Switch Independent.

b) Click **VMs and Services** in the bottom left side pane.

Example:

1. Choose **VM Networks**.

2. In the right side pane, the VM network name is **apicInfra|10.0.0.30|*SCVMM Controller HostNameORIPAddress filed value*|*VMMdomainName***.

   You must use infra VM Network to create VTEP on the Hyper-V server.

Deploying the Logical Switch to the Host on SCVMM

This section describes how to deploy the logical switch to the host on System Center Virtual Machine Manager (SCVMM).

Note If SCVMM upgrade is performed and hosts are already connected to logical switch then SCVMM admin should perform host remediation for all the hosts for hosts to establish connection to leaf.

Procedure

Step 1 Log in to the SCVMM server, in the **Navigation** pane, choose **Fabric** on the bottom left.

Step 2 In the **Navigation** pane, expand **Networking** > **Logical Switches** to ensure the logical switch is created (apicVswitch_cloud1).

Step 3 In the **Navigation** pane, choose **VMs and Services** on the bottom left.

Step 4 In the **Navigation** pane, expand **All Hosts**.

Step 5 Choose the Hyper-V host folder (Dev8).

Step 6 Right-click the Hyper-V host (Dev8-HV1) and choose **Properties**.

Step 7 In the **Dev8-HV1.inscisco.net Properties** dialog box, choose **Virtual Switches** and perform the following actions:

a) Choose **+ New Virtual Switch**.
b) Choose **New Logical Switch**.
c) In the **Logical switch** field, from the drop-down list, choose a logical switch (apicVswitch_cloud1).
d) In the **Adapter** field, from the drop-down list, choose an adapter (Leaf1-1-1 - Intel(R) Ethernet Server Adapter X520-2 #2).
e) In the **Uplink Port Profile** field, from the drop-down list, choose an Uplink Port Profile (apicUplinkPortProfile_Cloud01).
f) Click **New Virtual Network Adapter**, choose the unnamed virtual network adapter, and enter the name (dev8-hv1-infra-vtep).
g) Click **Browse**.
h) In the **Dev8-HV1.inscisco.net Properties** dialog box, choose the VM network (apicInfra|10.0.0.30|dev8-scvmm.apic.net|Cloud01) and click **OK**.
i) In the **Virtual Machine Manager** dialog box, click **OK**.

Step 8 Click **Jobs** on the bottom left.

Step 9 In the **History** pane, you can check the status of the **Change properties of virtual machine host** job to ensure that the job has completed.

Step 10 You must refresh the host under SCVMM for the Hyper-V server to reflect proper Hyper-V Host IP address in SCVMM. Once it has been refreshed, the APIC GUI reflects the updated Hyper-V Host IP information.

Enabling the Logical Network on Tenant Clouds

This section describes how to enable the Cisco ACI Integration with SCVMM Tenant Clouds. For more information, see the SCVMM Fabric Cloud and Tenant Clouds, on page 3.

Procedure

Step 1 Log in to the SCVMM server with SCVMM administrator credentials, and open up the SCVMM Admin Console.

Step 2 On the SCVMM Admin Console, navigate to VMs and Services.

Step 3 In the **Navigation** pane, expand **Clouds**, right-click on your target Tenant Cloud (HR_Cloud) and choose **Properties**.

Step 4 In the Pop-Up Window, in the **Navigation** pane, choose **Logical Networks**

a) Locate the logical network which was automatically created as part of associating the VMM Domain to this SCVMM.
b) Click the logical network check box (apicLogicalNetwork_MyVmmDomain).
c) Click **OK**.

The tenant cloud is now ready to be used within ACI Integration at the Windows Azure Pack Plan configuration page.

Upgrading the Cisco ACI with Microsoft SCVMM Components

If you are trying to upgrade to SCVMM 2016, you must follow the Microsoft procedure and then install the Cisco ACI with Microsoft SCVMM components as a fresh install.

Prerequisites:

If upgrading to SCVMM 2012 R2, Microsoft servers that you integrate into ACI must be updated with the KB2919355 and KB3000850 update rollups prior to upgrading ACI to the 2.2(1) release. The KB2919355 update rollup includes the 2929781 patch, which adds new TLS cipher suites and changes the cipher suite priorities in Windows 8.1 and Windows Server 2012 R2.

You must patch the following Microsoft servers:

- Microsoft Windows Azure Pack Resource Provider Servers
- Microsoft Windows Azure Pack Tenant Site Servers
- Microsoft Windows Azure Pack Admin Site Servers
- Microsoft System Center Service Provider Foundation/Orchestration Servers
- Microsoft System Center 2012 R2 Servers
- Microsoft HyperV 2012 R2 Servers

Upgrading the ACI Microsoft SCVMM Components Workflow

This sections describes upgrading the ACI Microsoft SCVMM components workflow.

Procedure

Step 1 Upgrade the APIC Controller and the Switch Software.

For more information, see the *Cisco APIC Firmware Management Guide*.

Step 2 Upgrade the APIC SCVMM Agent on SCVMM or Upgrade the APIC SCVMM Agent on a Highly Available SCVMM.

For more information, see Upgrading the APIC SCVMM Agent on SCVMM, on page 27.

For more information, see Upgrading the APIC SCVMM Agent on a High Available SCVMM, on page 28.

Step 3 Upgrade the APIC Hyper-V Agent.

For more information, see Upgrading the APIC Hyper-V Agent, on page 28.

Upgrading the APIC SCVMM Agent on SCVMM

This section describes how to upgrade the APIC SCVMM agent on System Center Virtual Machine Manager (SCVMM).

Before you begin

Scheduled downtime for the Microsoft SCVMM Server. The upgrade process will automatically restart the Microsoft System Center Virtual Machine Manager Service, resulting in the SCVMM Service to be temporarily unable to handle any change or query requests.

Procedure

Upgrade the APIC SCVMM agent on SCVMM.

If upgrading from release 1.1(2x) or later:

a) Follow the steps outlined in the Installing the APIC SCVMM Agent on SCVMM, on page 7.

The MSI packages handles uninstalling the previous version and installing the new version as part of the upgrade.

If upgrading from a prior release of 1.1(2x):

a) Follow the steps outlined in the Installing the APIC SCVMM Agent on SCVMM, on page 7.

The MSI packages handles uninstalling the previous version and installing the new version as part of the upgrade.

b) Follow the steps outline in the Exporting APIC OpFlex Certificate, on page 42.
c) Follow the steps outline in the Installing the OpflexAgent Certificate, on page 10.

d) Follow the steps outline in the Configuring APIC IP Settings with OpflexAgent Certificate on the SCVMM Agent, on page 13 or Configuring APIC IP Settings with OpflexAgent Certificate on the SCVMM Agent on a Highly Available SCVMM, on page 15.

Upgrading the APIC SCVMM Agent on a High Available SCVMM

This section describes how to upgrade the APIC SCVMM agent on a high available System Center Virtual Machine Manager (SCVMM).

Procedure

Step 1 Log in to a Standby node of the Highly Available SCVMM installation.

Step 2 On the SCVMM server in File Explorer, locate the **APIC SCVMM Agent.msi** file.

Step 3 Right-click **APIC SCVMM Agent.msi** file and select **Install**.

The MSI packages handles uninstalling the previous version and installing the new version as part of the upgrade.

Step 4 In the **Cisco APIC SCVMM Agent Setup** dialog box, perform the following actions:

a) Click **Next**.

b) Check the **I accept the terms in the License Agreement** check box and click **Next**.

c) Enter your account name and password credentials.

Provide the same credentials as used for the SCVMM console. The Cisco APIC SCVMM agent requires these credentials for the SCVMM operations to be able to function.

The installation process verifies the entered account name and password credentials. If the installation fails, the SCVMM shows an error message and you must re-enter valid credentials.

d) After successful validation of the account name and password credentials, click **Install**.

e) Click **Finish**.

Step 5 Repeat steps 1-4 for each Standby Node in the Windows Failover Cluster.

Step 6 Failover from the Current Owner Node of the Highly Available SCVMM installation to one of the newly upgrade Standby Nodes.

Step 7 Follow steps 2-4 on the final Standby Node of the Windows Failover Cluster.

Upgrading the APIC Hyper-V Agent

This section describes how to upgrade the APIC Hyper-V agent.

Before you begin

Scheduled downtime for the Hyper-V node. For more information regarding Hyper-V Maintenance Mode behavior, see: https://technet.microsoft.com/en-us/library/hh882398.aspx

Procedure

Upgrade the APIC Hyper-V agent.

If upgrading from release 1.1(2x) or later:

a) Follow steps 1-8 in the Installing the APIC Hyper-V Agent on the Hyper-V Server, on page 16. Skip step 7. Step 7 is not required for upgrades as the OpflexAgent certificate is already installed on the Hyper-V node.

   The MSI packages handles uninstalling the previous version and installing the new version as part of the upgrade.

If upgrading from a prior release of 1.1(2x):

a) Follow the steps outlined in the Uninstalling the APIC Hyper-V Agent.
b) Follow steps 1-8 in the Installing the APIC Hyper-V Agent on the Hyper-V Server, on page 16. Skip step 7. Step 7 is not required for upgrades as the OpflexAgent certificate is already installed on the Hyper-V node.

   The MSI packages handles uninstalling the previous version and installing the new version as part of the upgrade.

Deploying Tenant Policies

Deployment Tenant Policies Prerequisites

Ensure that your computing environment meets the following prerequisites:

- Ensure you have installed the APIC SCVMM Agent.

  For details, see Installing the APIC SCVMM Agent on SCVMM, on page 7.

- Ensure you have installed the APIC Hyper-V Agent.

  For details, see Installing the APIC Hyper-V Agent on the Hyper-V Server, on page 16.

- Ensure you have created a logical switch.

  See Microsoft's documentation.

- Ensure you have created a virtual switch.

  See Microsoft's documentation.

Creating a Tenant

Procedure

Step 1 On the menu bar, choose **TENANTS**, and perform the following actions:

a) Click **Add Tenant**.
The **Create Tenant** dialog box opens.

b) In the **Name** field, add the tenant name (ExampleCorp).

Step 2 Click **Finish**.

See the *Cisco APIC Basic Configuration Guide* for more information.

Creating an EPG

This section describes how to create an endpoint group (EPG).

Procedure

Step 1 Log in to the APIC GUI, on the menu bar, choose **TENANTS** > **Tenant Name**.

Step 2 In the **Navigation** pane, expand **Tenant Name** > **Application Profiles** > **Application Profile Name**, right-click **Application EPGs**, and choose **Create Application EPG**.

Step 3 In the **Create Application EPG** dialog box, perform the following actions:

a) In the **Name** field, enter the name (EPG1).

b) In the **Bridge Domain** field, from the drop-down list, choose one to associate with the bridge domain.

c) In the **Associate to VM Domain Profiles** field, click the appropriate radio button and click **Next**.

d) In the **Associated VM Domain Profiles** field, click the + icon, and choose a cloud to add (Cloud10).

You have now created an EPG.

Associating the Microsoft VMM Domain with an EPG

This section describes how to create a VM Network by associating the Microsoft VMM domain with an endpoint group (EPG).

Note Content in the **Hypervisors**, **Virtual Machines,** and **Virtualization Ratio** areas of the Cisco APIC capacity dashboard appears as 0 when SCVMM endpoints are learned in Pre-Provision mode.

Before you begin

Ensure you have created an EPG.

Procedure

Step 1 Log in to the Cisco APIC GUI and on the menu bar, choose **Tenants** > **Tenant Name**.

Step 2 In the **Navigation** pane, expand **Tenant Name** > **Application Profiles** > **Application Profile Name** > **Application EPGs** and select an existing EPG.

Step 3 In the **Navigation** pane, choose **Domains (VMs and Bare-Metals)**.

Step 4 In the **Domains (VM and Bare-Metals)** pane, click on the **ACTIONS** and choose **Add VMM Domain Association**.

Step 5 In the **Add VMM Domain Association** dialog box, click the **Deploy Immediacy** field radio button for either **Immediate** or **On Demand**.

See EPG Policy Resolution and Deployment Immediacy for more information.

Step 6 In the **Add VMM Domain Association** dialog box, click the **Resolution Immediacy** field radio button for either **Immediate**, **On Demand**, or **Pre-Provision**.

See EPG Policy Resolution and Deployment Immediacy for more information.

You have now created a VM Network.

Step 7 Optional: In the **Delimiter** field, use a single character as the VM Network Name delimiter, enter one of the following: |, ~, **!**, **@**, ^, +, or = . If you do not enter a symbol, the system default of | will be used.

Verifying the EPG is Associated with the VMM Domain on APIC

This section describes how to verify the endpoint group association with the VMM domain on Application Policy Infrastructure Controller (APIC).

Procedure

Step 1 Log in to the APIC GUI, on the menu bar, choose **Virtual Networking** > **Inventory**.

Step 2 In the navigation pane, expand **VMM Domains** > **Microsoft** > **Cloud10** > **Controller** > **Controller1** > **Distributed Virtual Switch** > **SCVMM|Tenant|SCVMM|EPG1|Cloud1**.

The name of the new VM Network is in the following format: ***Tenant Name|Application Profile Name|Application EPG Name|Microsoft VMM Domain***.

Step 3 In the **PROPERTIES** pane, verify the EPG associated with the VMM domain, the VM Network, and the details such as NIC NAME, VM NAME, IP, MAC, and STATE.

Verifying the EPG is Associated with the VMM Domain on SCVMM

This section describes how to verify the endpoint group (EPG) associated with the VMM domain on System Center Virtual Machine Manager (SCVMM).

Procedure

Step 1 Open the **Virual Machine Manager Console** icon on your desktop.

Step 2 In the bottom left pane, click on **VMs and Services** or press **Ctrl+M**.

Step 3 In the **VMs and Services** pane, click on **VM Networks** and verify the EPG associated with the VMM domain.

The EPG associated with the VMM domain is in the following format: ***Tenant Name|Application Profile Name|Application EPG Name|Microsoft VMM Domain***.

Creating a Static IP Address Pool

Static IP Address Pools enable an Microsoft SCVMM Server to statically assign IP Address to virtual machines during the VM Template Deployment phase. This feature removes the need to request a DHCP address from a DHCP Server. This feature is most often used to deploy server VMs which require statically assigned IP Addresses in the network such as: Windows Active Directory Domain Controllers, DNS Servers, DHCP Servers, Network Gateways, etc.

For more information regarding Static IP address pools, see the Microsoft Documentation: https://technet.microsoft.com/en-us/library/jj721568.aspx#BKMK_StaticIPAddressPools

With Cisco ACI SCVMM Integration - the Cisco APIC can automate the deployment of a Static IP Address Pool to a VM Network, bypassing the need to perform these operations on the Microsoft SCVMM Server itself.

Before you begin

Ensure an EPG is associated to a Microsoft SCVMM VMM Domain.

Procedure

Step 1 Log in to the APIC GUI, on the menu bar, choose **TENANTS** > **Tenant Name**.

Step 2 In the **Navigation** pane, expand **Tenant Name** > **Application Profiles** > **Application Profile Name** > **Application EPGs** > ***Your Target EPG***, right-click **Subnets**, and choose **Create EPG Subnet**.

Step 3 In the **Create EPG Subnet** dialog box, perform the following actions:

a) Enter a default Gateway IP in address/mask format.

b) Click **Submit**.

Step 4 Right-click on the newly created subnet and choose **Create Static IP Pool Policy**.

Step 5 In the **Create Static IP Pool Policy** dialog box, perform the following actions:

a) Enter a Name (IP).

b) Enter a Start IP and End IP.

c) Enter optional Static IP Pool policies.

The DNS Servers, DNS Search Suffix, Wins Servers fields Allow a list of entries, simply use semicolon to separate the entries. For example within the DNS Servers Field:

192.168.1.1;192.168.1.2

Note When configuring the Start IP and End IP, ensure they are within the same Subnet as the Gateway defined in Step 3. If not deployment of the Static IP Address Pool to SCVMM fails.

Only 1 Static IP Address Pool will be used for a given EPG. Do not create multiple Static IP Pool Policies under a Subnet as the others will not take effect.

The Static IP Address Pool Policy follows the VMM Domain association. If this EPG is deployed to multiple SCVMM Controllers in the same VMM Domain, then the same Static IP Addresses will be deployed, causing duplicate IP Addresses. For this scenario, deploy an addition EPG with a non-overlapping Address pool and create the necessary policies and contracts for the endpoints to communicate.

Connecting and Powering on the Virtual Machine

This section describes how to connect and power on the virtual machine.

Procedure

Step 1 Log in to the SCVMM server, choose **VMs and Services** > **All Hosts**, and choose one of the hosts.

Step 2 In the **VMs** pane, right-click on the VM host that you want to associate to the VM Network and choose **Properties**.

Step 3 In the **Properties** dialog box, choose **Hardware Configuration**, and choose a network adapter (Network Adapter 1).

Step 4 In the **Network Adapter 1** pane, perform the following actions to connect to a VM network:

a) Click the **Connect to a VM network** radio button.
b) Click the **Browse** button.
c) Verify the list of VM networks, which lists all of the VM networks to which the hypervisor is associated.

Step 5 Power on the virtual machine.

Verifying the Association on APIC

This section describes how to verify the association on Application Policy Infrastructure Controller (APIC).

Procedure

Step 1 Log in to the APIC GUI, on the menu bar, choose **Virtual Networking** > **Inventory**.

Step 2 In the navigation pane, expand **VMM Domains** > **Microsoft** > **Cloud10** > **Controller** > **Controller1** > **Hypervisors** > **Hypervisor1** > **Virtual Machines** to verify the association.

Viewing EPGs on APIC

This section describes how to view endpoint groups (EPGs) on the Application Policy Infrastructure Controller (APIC).

Procedure

Step 1 Log in to the APIC GUI, on the menu bar, choose **TENANTS** > **Tenant Name**.

Step 2 In the **Navigation** pane, expand **Tenant Name** > **Application Profiles** > **VMM** > **Application EPGs** > **EPG1**.

Step 3 In the **Application EPG - EPG1** pane, click the **OPERATIONAL** button, and verify if the endpoint group is present.

Troubleshooting the Cisco ACI with Microsoft SCVMM

Troubleshooting APIC to SCVMM Connectivity

Use the ApicVMMService logs to debug the System Center Virtual Machine Manager (SCVMM) server.

Procedure

Step 1 Log in to the SCVMM server, go to the **ApicVMMService** logs. Located at **C:\Program Files (X86)\ApicVMMService\Logs**.

Step 2 Check the **ApicVMMService** logs to debug.

If you are unable to debug, on the SCVMM server copy all the **ApicVMMService** logs from **C:\Program Files (X86)\ApicVMMService\Logs** and send them to Cisco Tech Support.

Troubleshooting Leaf to Hyper-V Host Connectivity

Use the ApicHypervAgent logs to debug the Hyper-V servers.

Procedure

Step 1 Log in to the Hyper-V servers, go to the **ApicHypervAgent** logs. Located at **C:\Program Files (x86)\ApicHypervAgent\Logs**.

Step 2 Check the **ApicHypervAgent** logs to debug.

If you are unable to debug, on the Hyper-V servers copy all the **ApicHypervAgent** logs from **C:\Program Files (x86)\ApicHypervAgent\Logs** and send them to Cisco Tech Support.

Troubleshooting the EPG Configuration Issue

If during the lifetime of the endpoint group (EPG), the VLAN ID of the EPG changes on the APIC, then SCVMM needs to update the VLAN configuration on all virtual machines for the new setting to take effect.

Procedure

To perform this operation run the following PowerShell commands on the SCVMM server:

Example:

```
$VMs = Get-SCVirtualMachine
$VMs | Read-SCVirtualMachine
$NonCompliantAdapters=Get-SCVirtualNetworkAdapter -All | Where-Object
{$_.VirtualNetworkAdapterComplianceStatus -eq "NonCompliant"}
$NonCompliantAdapters | Repair-SCVirtualNetworkAdapter
```

Reference Information

Installing the APIC Agent on SCVMM Using the Windows Command Prompt

This section describes how to install the APIC Agent on System Center Virtual Machine Manager (SCVMM) using the Windows Command Prompt.

Procedure

Step 1 Log in to the SCVMM server with SCVMM administrator credential.

Step 2 Launch the command prompt, change to the folder where you copied the **APIC SCVMM Agent.msi** file, and execute following commands:

Example:

```
C:\>cd MSIPackage

C:\MSIPackage>dir
Volume in drive C has no label.
Volume Serial Number is 726F-5AE6

Directory of C:\MSIPackage

02/24/2015  01:11 PM    <DIR>          .
02/24/2015  01:11 PM    <DIR>          ..
02/24/2015  05:47 AM         3,428,352 APIC SCVMM Agent.msi
               1 File(s)      3,428,352 bytes
```

```
               2 Dir(s)  37,857,198,080 bytes free

C:\MSIPackage>msiexec.exe /I "APIC SCVMM Agent.msi" /Qn ACCOUNT="inscisco\Administrator"
PASSWORD="MyPassword" /log "C:\InstallLog.txt"
C:\MSIPackage>sc.exe query ApicVMMService

     SERVICE_NAME: ApicVMMService
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Step 3 If the **msiexec.exe** installer package succeeds, it finishes without any warning or error messages. If it fails, it displays the appropriate warning or error message.

Installing the APIC Hyper-V Agent on the Hyper-V Server Using the Windows Command Prompt

This section describes how to install the APIC Hyper-V Agent on the Hyper-V server using the windows Command Prompt.

Procedure

Step 1 Log in to the Hyper-V server with administrator credentials.

Step 2 Launch the command prompt, change to the folder where you copied the **APIC Hyper-V Agent.msi** file, and execute the following commands:

Example:

```
C:\>cd MSIPackage

C:\MSIPackage>dir
Volume in drive C has no label.
Volume Serial Number is C065-FB79

Directory of C:\MSIPackage

02/24/2015  01:11 PM    <DIR>          .
02/24/2015  01:11 PM    <DIR>          ..
02/24/2015  05:44 AM           958,464 APIC Hyper-V Agent.msi
               1 File(s)        958,464 bytes
               2 Dir(s)  749,486,202,880 bytes free

C:\MSIPackage>msiexec.exe /I "APIC Hyper-V Agent.msi" /log "C:\InstallLog.txt"

C:\MSIPackage>msiexec.exe /I "APIC Hyper-V Agent.msi" /Qn /log "C:\InstallLog.txt"

C:\MSIPackage>sc.exe query ApicHyperVAgent

SERVICE_NAME: ApicHyperVAgent
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
```

```
WIN32_EXIT_CODE    : 0  (0x0)
SERVICE_EXIT_CODE  : 0  (0x0)
CHECKPOINT         : 0x0
WAIT_HINT          : 0x0
```

Step 3 Repeat steps 1 through 2 for each Hyper-V server.

If the **msiexec.exe** installer package succeeds, it finishes without any warning or error messages. If it fails, it displays the appropriate warning or error message.

Programmability References

ACI SCVMM PowerShell Cmdlets

This section describes how to list the Cisco Application Centric Infrastructure (ACI) System Center Virtual Machine Manager (SCVMM) PowerShell cmdlets, help, and examples.

Procedure

Step 1 Log in to the SCVMM server, choose **Start** > **Run** > **Windows PowerShell**.

Step 2 Enter the following commands:

Example:

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\ApicVMMService> cd C:\Program Files (x86)\ApicVMMService>
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Add-Type -Path .\Newtonsoft.Json.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets

CommandType     Name                       ModuleName
-----------     ----                       ----------
Cmdlet          Get-ACIScvmmOpflexInfo     ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials        ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert         ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert        ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials        ACIScvmmPsCmdlets
```

Step 3 Generating help:

Example:

```
commandname -?
```

Step 4 Generating examples:

Example:

```
get-help commandname -examples
```

Configuration References

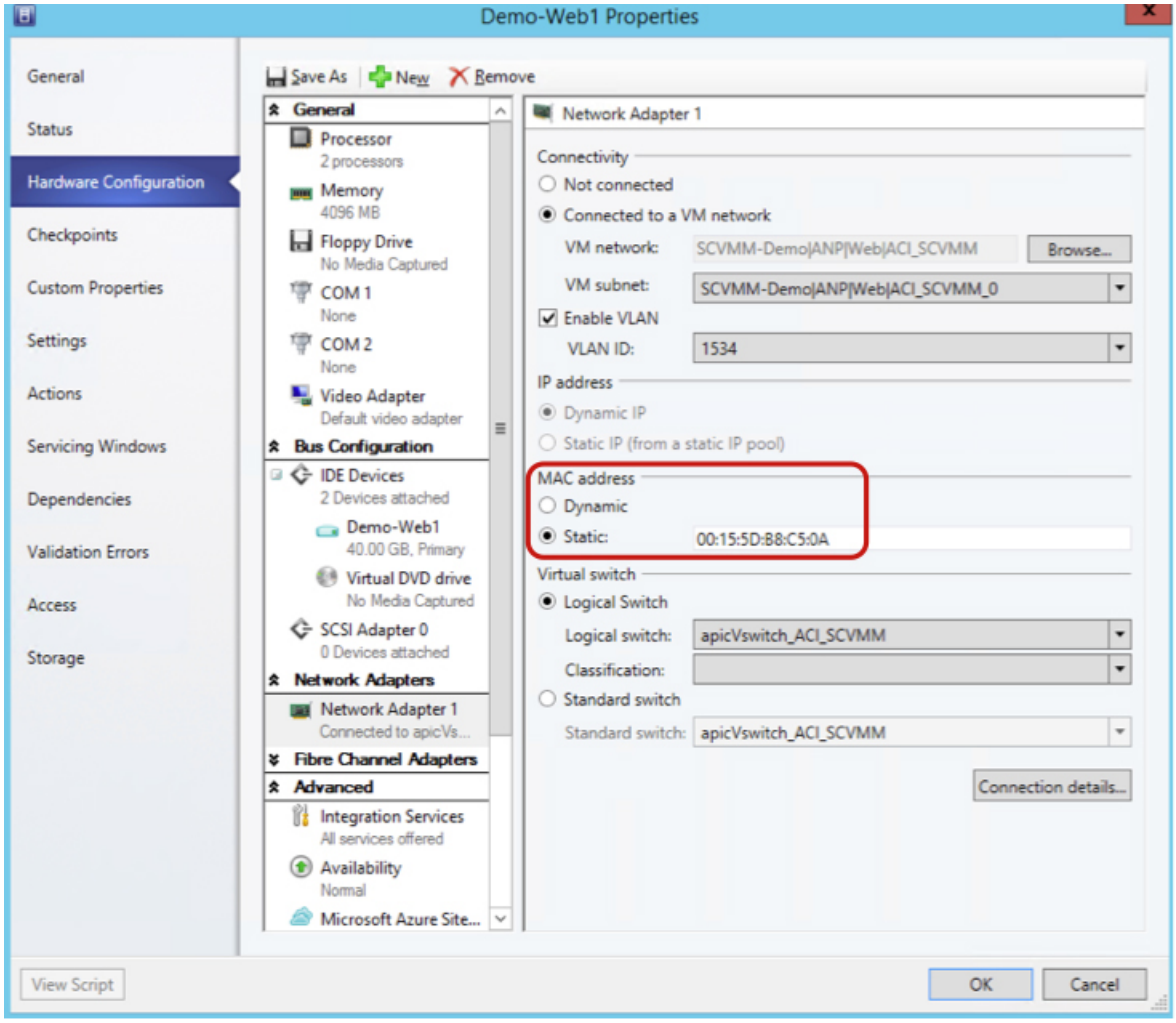
MAC Address Configuration Recommendations

This section describes the MAC address configuration recommendations.

- Both Dynamic and Static MAC are supported.
- **Static** MAC for the VM Network adapter is recommended if you want the VM inventory to show up quickly on APIC.
- If you choose **Dynamic** MAC there is a delay for the VM inventory to show up on APIC. The delay is because Dynamic MACs are not learned by SCVMM right away.

Note The Data plane works fine even though the VM inventory does not show up.

Figure 3: Shows the MAC address section in the Properties pane.



Uninstalling the Cisco ACI with Microsoft SCVMM Components

This section describes how to uninstall the Cisco Application Centric Infrastructure (ACI) with Microsoft System Center Virtual Machine Manager (SCVMM) components.

Procedure

Step 1 Detach all virtual machines from the VM networks.

See Microsoft's documentation.

Step 2 Delete the Infra VLAN tunnel endpoint (VTEP) and APIC logical switches on all Hyper-Vs.

See Microsoft's documentation.

Step 3 Verify the APIC GUI to make sure all the VMs and hosts are disconnected.

Step 4 Delete the VMM Domain from the Application Policy Infrastructure Controller (APIC).

See Guidelines for Deleting VMM Domains.

Step 5 Verify the logical switch and logical networks are removed from SCVMM.

Step 6 Uninstall the APIC SCVMM Agent on SCVMM or on a Highly Available SCVMM.

See Uninstalling the APIC SCVMM Agent, on page 40.

See Uninstalling the APIC SCVMM Agent on a Highly Available SCVMM, on page 40

Uninstalling the APIC SCVMM Agent

This section describes how to uninstall the APIC SCVMM Agent.

Procedure

Step 1 Log in to the SCVMM server.

Step 2 Choose **Start** > **Control Panel** > **Uninstall a Program**.

Step 3 In the **Programs and Features** window, right-click **ApicVMMService** and choose **Uninstall**.
This uninstalls the APIC SCVMM Agent.

Step 4 To verify if the APIC SCVMM Agent is uninstalled, in the **Programs and Features** window, verify that **ApicVMMService** is not present.

Uninstalling the APIC SCVMM Agent on a Highly Available SCVMM

This section describes how to install the Application Policy Infrastructure Controller (APIC) SCVMM agent on a Highly Available System Center Virtual Machine Manager (SCVMM).

Procedure

Step 1 Log in to any node within the Highly Available SCVMM Failover Cluster.

Step 2 Open the **Failover Cluster Manager Application**.

Step 3 In the **Windows Failover Cluster Manager** window, select **ApicVMMService** in the Highly Available SCVMM Roles/Resources tab.

Step 4 Right-click on the **ApicVMMService Role** and choose **Take Offline**.

Step 5 Once the Role is offline, right-click on the **ApicVMMService Role** and choose **Remove**.

Step 6 On each node within the Highly Available SCVMM Failover Cluster, perform the following actions to uninstall the APIC SCVMM Agent:

a) Log in to the SCVMM server.
b) Choose **Start** > **Control Panel** > **Uninstall a Program**.
c) In the **Programs and Features** window, right-click **ApicVMMService** and choose **Uninstall**.

This uninstalls the APIC SCVMM Agent.

d) To verify if the APIC SCVMM Agent is uninstalled, in the **Programs and Features** window, verify that **ApicVMMService** is not present.

Downgrading the Cisco APIC Controller and the Switch Software with Cisco ACI and Microsoft SCVMM Components

This section describes how to downgrade the Cisco APIC and the switch software with Cisco ACI and Microsoft System Center Virtual Machine Manager (SCVMM) components.

Procedure

Step 1 Uninstall the Cisco APIC SCVMM Agent on SCVMM or on a highly available SCVMM.

See Uninstalling the APIC SCVMM Agent, on page 40.

See Uninstalling the APIC SCVMM Agent on a Highly Available SCVMM, on page 40.

Step 2 Downgrade the Cisco APIC Hyper-V Agent by Completing the following steps:

a) Log in to the SCVMM server and bring the Hyper-V node into maintenance mode.
b) Log in to the Hyper-V server with administrator credentials.
c) Uninstall the Cisco APIC Hyper-V agent.
d) Install Cisco APIC Hyper-V agent to the version that the Cisco ACI fabric is being downgraded to.

Step 3 Downgrade the switch software.

Step 4 Downgrade the Cisco APIC.

See the *Cisco APIC Firmware Management Guide* for details.

Step 5 On the SCVMM server, install the SCVMM agent for the version that the Cisco ACI fabric is being downgraded to.

See Installing the APIC SCVMM Agent on SCVMM, on page 7

See Installing the APIC SCVMM Agent on a Highly Available SCVMM, on page 7

Step 6 Follow the steps in Microsoft's documentation to view and bring the Cisco APIC vSwitch logical switch into compliance.

See *How to View Host Network Adapter Settings and Increase Compliance with Logical Switch Settings in VMM*.

Exporting APIC OpFlex Certificate

This section describes how to back up APIC OpFlex certificate to a file which can be used to deploy new Hyper-V nodes, System Center Virtual Machine Manager (SCVMM) and Windows Azure Pack Resource Provider servers to the ACI Fabric when the original OpFlex certificate cannot be located.

Procedure

Step 1 Log in to a Hyper-V node which is currently a member of the ACI Fabric.

Step 2 Export the certificate from the Hyper-V node by performing the following actions:

a) Choose **Start** > **Run** and type **certlm.msc** to launch the Certificate Manager.

b) In the **navigation** pane, right-click on **Certificates - Local Computer** and choose **Find Certificates.**

c) In the **Find Certificate** dialog box, perform the following actions:

- In the **Find in** field, from the drop-down list, choose **All certificate stores**.
- In the **Contains** field, enter **OpflexAgent**.
- In the **Look in Field** field, from the drop-down list, choose **Issued By**.
- Click **Find Now**.

  Your result list should have a single Certificate in the list.

d) Right-click on the newly found **OpflexAgent** certificate and choose **Export**.

The Certificate Export Wizard will appear.

Step 3 In the **Certificate Export Wizard** dialog box, perform the following actions:

a) In the **Welcome to the Certificate Export Wizard** dialog box, click **Next**

b) In the **Export Private Key** dialog box, choose the **Yes, export the private key** radio button, and click **Next**.

c) In the **Export File Format** dialog box, choose the **Personal Information Exchange - PKCS #12 (.PFX)** radio button, check the **Include all certificates in the certificate path if possible** and **Export all extended properties** check box. Click **Next**.

d) In the **Security** dialog box, check the **Password** check box, enter your PFX password and enter your PFX password again to confirm. Click **Next**.

Your PFX password will be used later to import the PFX file on the target machine.

e) In the **File to Export** dialog box, enter the filename you wish to save the exported file (C:\OpflexAgent.pfx) and click **Next**.

f) In the **Completing the Certificate Export Wizard** dialog box, review all your specified settings are correct and click **Finish**.

g) The **Certificate Export Wizard** dialog box will appear with **The export was successful.** and click **Ok**.

Step 4 Copy the PFX file to a known location.

You can deploy the certificate through an Active Directory Group Policy or copy the file to your various Microsoft Servers which host your SCVMM, Windows Azure Pack Resource Provider, and Hyper-V services for integration into the ACI Fabric.