Deploy Microsoft SQL Server 2014 on a Cisco Application Centric Infrastructure Policy Framework

August 2015
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Main Benefits</td>
<td>3</td>
</tr>
<tr>
<td>Goals of This Document</td>
<td>4</td>
</tr>
<tr>
<td>Integration Options</td>
<td>4</td>
</tr>
<tr>
<td>Scope</td>
<td>5</td>
</tr>
<tr>
<td>Technology Use Cases</td>
<td>5</td>
</tr>
<tr>
<td><strong>Solution Design</strong></td>
<td>6</td>
</tr>
<tr>
<td>Network Topology</td>
<td>6</td>
</tr>
<tr>
<td>Microsoft SQL Server 2014 Architecture</td>
<td>8</td>
</tr>
<tr>
<td>Integrating Cisco ACI Fabric with Microsoft SCVMM</td>
<td>10</td>
</tr>
<tr>
<td>Creating EPGs and Defining Contracts</td>
<td>16</td>
</tr>
<tr>
<td>Workload Details</td>
<td>19</td>
</tr>
<tr>
<td><strong>Validation</strong></td>
<td>20</td>
</tr>
<tr>
<td>Validation</td>
<td>20</td>
</tr>
<tr>
<td>Cisco APIC Network Statistics</td>
<td>20</td>
</tr>
<tr>
<td>Verification Summary</td>
<td>22</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>23</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>23</td>
</tr>
</tbody>
</table>
Introduction

Efficient management of modern Microsoft SQL Server infrastructure is becoming increasingly complicated with the rapidly changing business requirements many companies face today. Modern enterprise database applications demand high performance in addition to very high availability. These requirements must also be balanced with ongoing needs for greater efficiency, lower infrastructure costs, and increased ease of management.

Cisco® Application Centric Infrastructure (Cisco ACI™) is a next-generation data center fabric infrastructure designed to meet the needs of rapidly changing business demands. Cisco and Microsoft have partnered to enable enterprise applications to take advantage of an application-centric infrastructure framework for application optimization, efficient deployment, and optimal performance. With Cisco ACI, the data center responds dynamically to the changing needs of applications, rather than having applications conform to constraints imposed by the infrastructure. The policies automatically adapt the infrastructure to the needs of the business to shorten application deployment cycles.

Cisco ACI enables a scalable, efficient cloud infrastructure that is application centric. Cisco ACI technology combines the benefits of software-defined networking (SDN) with centralized policy control, allowing data centers to automate, virtualize, and pool infrastructure and network resources and provision them based on application requirements. As a result, data centers gain speed and flexibility when deploying applications as well as the capability to consolidate resources, secure data, and reduce costs.

Cisco extends the Cisco ACI policy framework to Microsoft Windows Server and Microsoft Hyper-V with Microsoft System Center. With Microsoft Windows Azure Pack (WAP) integration, the Cisco Unified Computing System™ (Cisco UCS®) and Cisco ACI policy framework enables enterprises to offer database as a service on a Microsoft private cloud with Microsoft SQL Server 2014 and efficiently manage the infrastructure with only a few resources.

Main Benefits

The benefits of Cisco ACI with SQL Server include:

- Reduced data center complexity because Cisco ACI uses the existing management framework of System Center for managing Hyper-V virtual workloads
- Improved deployment time and performance
- Capability to provide hybrid cloud computing with consistent policies across applications, network, security, and database management resources
- Optimized SQL Server 2014 database performance and resiliency with SQL Server 2014 AlwaysOn technology and cloud infrastructure integration capabilities
- Holistic health monitoring of both physical and Windows Hyper-V virtual implementations
- Superior scalability and high availability

SQL Server is the critical database server for many enterprise applications. Cisco supports SQL Server with an application-policy model using Cisco ACI designed to allow the entire data center to better align with today’s growing business needs. SQL Server with Cisco ACI benefits customers with ease of manageability and deployment and outstanding scalability and agility.
Goals of This Document
In this document, you will learn how easily you can deploy SQL Server 2014 on Cisco ACI and Cisco UCS servers. You will also learn why Cisco ACI with the Cisco Application Policy Infrastructure Controller (APIC) provides an optimal platform for deploying and using the new features in SQL Server 2014. Additionally, you will learn about the unique and advanced infrastructure framework that Cisco ACI provides and how it solves many of the critical business problems that challenge traditional deployment models.

The primary goal of this document is to demonstrate the ease with which you can deploy SQL Server 2014 with Microsoft System Center Virtual Machine Manager (SCVMM) integration on a Cisco ACI policy framework. This document also presents the benefits of this deployment.

Integration Options
Cisco offers two solutions for integration with a Microsoft private cloud to enhance the network management capabilities of the Microsoft platform:

- Cisco ACI integration for deployments using SCVMM only
- Cisco ACI integration for deployments using both WAP and SCVMM

This document discusses only the first solution: deployment of SQL Server on Cisco ACI using only SCVMM integration.

Cisco ACI Integration for Deployments Using Both WAP and SCVMM
For deployments using both WAP and SCVMM, Cisco ACI integrates with WAP to provide a self-service experience for tenants. A Cisco ACI resource provider in WAP administers the APIC for network management. Networks are created in SCVMM and are available in WAP for respective tenants.

WAP for Windows Server is a collection of Azure technologies available to customers without additional installation charges. It runs on top of Windows Server 2012 R2 and System Center 2012 R2. Its use of Azure technologies enables companies to offer a robust, self-service, multitenant cloud that is consistent with the look and feel of the public Azure experience.

WAP includes the following capabilities:

- Management portal for tenants: Customizable self-service portal for provisioning, monitoring, and managing services such as networks, bridge domains, virtual machines, firewalls, load balancers, and shared services
- Management portal for administrators: Portal for administrators to configure and manage resource clouds, user accounts, tenant offers, quotas, pricing, website clouds, virtual machine clouds, and service bus clouds
- Service management API: Representational State Transfer (REST) API that helps enable a range of integration scenarios, including custom portals and billing systems

Customers who want a single management pane through self-service portals can use WAP to deploy SQL Server database servers.

Scope
This document discusses the advantages of deploying SQL Server 2014 on the Cisco ACI framework using Cisco ACI policy designs and the SQL Server 2014 AlwaysOn feature with SCVMM integration. The implementation details of SQL Server with its AlwaysOn and SCVMM integration are beyond the scope of this document.

Technology Use Cases
The document discusses the design of Cisco ACI policy for deploying SQL Server on Cisco ACI infrastructure. It discusses the fabric design for a typical enterprise-class SQL Server database application deployment.

This document also shows how the deployed system uses the AlwaysOn availability group feature in SQL Server 2014 to provide high-availability and disaster-recovery capabilities for enterprise-level databases.
Solution Design

Network Topology

The Cisco APIC integrates with a Microsoft SCVMM instance to transparently extend the Cisco ACI policy framework to Microsoft Hyper-V workloads. The APIC uses application network profiles (ANPs) to represent Cisco ACI policies. The ANPs provide logical representations of all components of the application and its interdependencies with the Cisco ACI fabric. After these ANPs are defined in the APIC, the integration between SCVMM and the APIC helps ensure that these network policies can be applied to Hyper-V workloads. The APIC integrates with SCVMM to simplify workload connectivity.

Cisco ACI uses a spine-and-leaf topology. All leaf nodes connect to all spine nodes. Spine nodes do not connect to each other, and leaf nodes do not connect to each other. Figure 1 shows a simple topology, which consists of a pair of spine switches dual-connected with 40 Gigabit Ethernet to each of the leaf switches. All physical and virtual devices can be connected through the mgmt0 port to an out-of-band management network, which can be used to access the switch’s command-line interface (CLI) or to connect to the REST API of the APIC. The use of multiple spine and leaf nodes helps ensure high availability through the network environment.

**Figure 1. Network Topology**

The network topology in Figure 1 shows a sample Cisco ACI deployment: two Cisco Nexus® 9505 Switches configured as spine switches, two Cisco Nexus 9396 Switches configured as leaf switches, and APICs. Leaf switches, also known as border switches, provide connectivity outside the fabric. The leaf switches connect to the SCVMM cloud, and a separate client virtual machine is used to send the user requests. The SCVMM cloud contains two Cisco UCS C240 M4 Rack Servers and one Cisco UCS C220 M3 Rack Server. The Cisco UCS C240 M4 servers run Microsoft Windows Server 2012 R2 with Hyper-V to host two Microsoft SQL Server 2014 virtual machines, represented as SQL node 1 and SQL node 2 in Figure 1. These two virtual servers are configured as a Windows failover cluster and synchronously replicate each other with the Microsoft AlwaysOn availability group feature enabled. The SCVMM cloud also contains a Cisco UCS C220 M3 server, which hosts two virtual machines.
for Microsoft Windows Active Directory (AD) and SCVMM. The topology also indicates the presence of Cisco Catalyst® 3750 Switches deployed in a pair for management connectivity.

Hardware and Software Versions
Table 1 shows the hardware and software versions used in this deployment model.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Device</th>
<th>Image</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing</td>
<td>Cisco UCS C240 M4 and C220 M3</td>
<td>Version 2.0 (3e)</td>
<td>Cisco UCS server</td>
</tr>
<tr>
<td>Network adapter</td>
<td>Cisco UCS Virtual Interface Card (VIC) 1225</td>
<td>Version 2.0 (3e)</td>
<td>Cisco VIC</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco Nexus 9508</td>
<td>Version N9000-11.1 (0.202)</td>
<td>Spine switch</td>
</tr>
<tr>
<td></td>
<td>Cisco Nexus 9396</td>
<td>Version N9000-11.1 (0.202)</td>
<td>Leaf switch</td>
</tr>
<tr>
<td></td>
<td>Cisco APIC</td>
<td>Version 1.1 (0.846)</td>
<td>Cisco controller</td>
</tr>
<tr>
<td></td>
<td>Cisco NX-OS Software</td>
<td>Version N9000-11.1 (0.202)</td>
<td>Switch</td>
</tr>
<tr>
<td>Cisco Software</td>
<td>APIC agent for Hyper-V</td>
<td>—</td>
<td>Hyper-V agent</td>
</tr>
<tr>
<td></td>
<td>APIC agent for SCVMM</td>
<td>—</td>
<td>APIC SCVMM agent</td>
</tr>
<tr>
<td>Microsoft software</td>
<td>Microsoft Windows 2012 R2 with Hyper-V role enabled</td>
<td>Version 2012 R2</td>
<td>Data center operating system</td>
</tr>
<tr>
<td></td>
<td>Microsoft SCVMM</td>
<td>Version 2012 R2</td>
<td>Enterprise version</td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server 2014</td>
<td>Version 2014</td>
<td>Enterprise version</td>
</tr>
<tr>
<td>HammerDB open-source software</td>
<td>HammerDB</td>
<td>Version 2.17</td>
<td>Load-test tool</td>
</tr>
</tbody>
</table>

Configuring Cisco APIC
The APIC is designed to transparently provide complete visibility into virtualized servers. Figure 2 shows the workflow for configuring the APIC.

Figure 2. Cisco APIC Configuration Workflow

1. **Create a VLAN pool.** The VLAN pool should be dynamic to allow the Microsoft Virtual Machine Manager (VMM) and APIC to allocate VLANs and negotiate VLAN tagging.
2. **Create a VMM domain and controller.** The VMM domain consists of the VMM and the VLAN pool that the VMM uses to send traffic to the leaf switches. The VMM domain is associated with an attachable entity profile (AEP), a policy group, and the interfaces to which the domain is attached to define the locations to which the virtual machines can move.
3. **Create an AEP.** The AEP provides physical infrastructure connectivity information. It provides a span of VLAN pools on the leaf switches and ports. A VMM domain automatically derives the physical interface policies from
the interface policy groups that are associated with an AEP. You can use an override policy in the AEP to specify a different physical interface policy for a VMM domain.

4. **Create interface policy.** You can associate policy groups with interfaces and with switches by using the interface profiles and the switch profiles. To add a port into a set of physical servers, you need to add an interface to the interface profile.

5. **Create a switch profile.** You create a switch profile to add a range of ports to a leaf switch or a pair of leaf switches.

6. **Set up Domain Host Configuration Protocol (DHCP) relay.** Cisco ACI fabric wide flooding is disabled by default, but you can enable flooding within a bridge domain. However, when the DHCP server is in a different endpoint group (EPG) than the clients, a DHCP relay is required. You should set up DHCP relay even when Layer 2 flooding is disabled.

Microsoft SQL Server 2014 Architecture

This section provides an overview of the end-to-end design of the reference architecture for SQL Server 2014 with the AlwaysOn feature implemented in the Cisco ACI fabric.

Figure 3 illustrates Microsoft Windows Server Failover Clustering (WSFC) with two SQL Server 2014 virtual machines and with the AlwaysOn availability group feature enabled. This combined feature enablement provides infrastructure support for the high-availability and disaster-recovery features of the hosted database server.

**Figure 3.** Microsoft SQL Servers in a Microsoft Windows Failover Cluster with the AlwaysOn Feature Enabled
An AlwaysOn availability group is composed of replicas of one or more databases. There is one primary replica and one to eight secondary replicas. The sample configuration in this document shows a single secondary replica. A secondary replica is a copy of the database from the primary replica. When the database is modified, changes are replicated to all secondary replicas.

This sample configuration also uses an availability group listener, to direct the incoming connections to the primary replica or to a read-only secondary replica. The listener provides fast application failover after an availability group fails over. An availability group listener is a virtual network name (VNN) to which clients can connect to access a database in a primary or secondary replica of an AlwaysOn availability group.

The VNN is registered in the Domain Name System (DNS) and is always owned by the SQL Server instance on which the primary replica resides. All the IP addresses that are supplied while configuring the availability group listener are registered in DNS under the same virtual network name. In this document, the availability group listener is referred to as SQL AG.

After SQL AG is created, you should verify that the clients can connect. The only change in the application connection is that instead of pointing to a specific server in the connection string, you point to SQL AG. SQL AG can connect only using TCP, and it can be resolved by your local DNS to the list of IP addresses and TCP port (1433) that are mapped to the VNN. When failover occurs, client connections are reset, and the ownership of the availability group listener (SQL AG) moves to the SQL Server instance that takes over the primary replica role. The VNN endpoint is then bound to the new IP addresses and TCP port of the new primary replica instance. Depending on the client, automatic reconnection to the availability group will occur, or you may have to manually restart the affected application or connection.

In this document, the availability group is configured with synchronous-commit mode. In this mode, transactions are not complete until they are committed to all databases in the synchronous availability group.

The network connections for the Cisco UCS C240 M4 server integration and management options use a shared LAN on motherboard (LOM) with two separate cables: for data traffic and for management traffic. Two 10 Gigabit Ethernet Small Form-Factor Pluggable (SFP) cables are connected separately to leaf 1 and leaf 2 for data traffic. For management traffic, a 1 Gigabit Ethernet cable is connected to a pair of Catalyst 3750 Switches.

Tables 2 and 3, respectively, show the configuration details for the SQL Server AlwaysOn availability group and availability replica group features.

**Table 2.** Microsoft SQL Server AlwaysOn Availability Group

<table>
<thead>
<tr>
<th>Microsoft SQL Server Availability Group</th>
<th>Member (Instance)</th>
<th>Default Role</th>
<th>Database</th>
<th>Database Configuration</th>
<th>Database Size</th>
<th>Memory Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability group database</td>
<td>• SQL2014-NODE1:SQLNODE1 • SQL2014-NODE2:SQLNODE2</td>
<td>• Primary • Secondary</td>
<td>Online Transaction Processing (OLTP) workloads</td>
<td>Database and log are on the same drive</td>
<td>50 GB</td>
<td>• Minimum: 8 GB • Maximum: 16 GB</td>
</tr>
</tbody>
</table>
Table 3. Microsoft SQL Server AlwaysOn Availability Replica Group

<table>
<thead>
<tr>
<th>Availability group database</th>
<th>Service Instance</th>
<th>Initial Role</th>
<th>Automatic Failover</th>
<th>Synchronous Commit</th>
<th>Allow Readable Secondary</th>
<th>Replication Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL2014-NODE1\SQLNODE1</td>
<td>Primary</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>SQL services network</td>
</tr>
<tr>
<td>SQL2014-NODE2\SQLNODE2</td>
<td>Secondary</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>SQL services network</td>
</tr>
</tbody>
</table>

Integrating Cisco ACI Fabric with Microsoft SCVMM

The workflow in Figure 4 shows the steps involved in establishing communication between Cisco ACI and SCVMM for network management.

**Figure 4.** Workflow for Microsoft SCVMM Integration with Cisco ACI Fabric

To integrate the Cisco ACI fabric with SCVMM, two Cisco ACI components must be installed outside the fabric:

- The APIC agent, a Windows installer (ApicVMMService.msi) is configured on SCVMM. The agent is configured with the IP addresses and credentials of the APICs. The agent communicates with the APIC through REST APIs. Microsoft PowerShell is used to configure Microsoft components.
• Hyper-V Agent, a Windows installer (HypervAgent.msi), is configured on all the connected Hyper-V computing hosts that are directly connected to the leaf switches. It runs with administrative credentials. OpFlex, REST, and Windows Management Instrumentation (WMI) enable communication with the leaf switches. This Windows executable uses infrastructure channel (infrachannel) and Virtual Extensible (VXLAN) tunnel endpoint (VTEP) interface on the host.

Cisco ACI Integration with Microsoft SCVMM Topology
The APIC adds the created EPGs and associates them with the VMM domain in SCVMM. VLANs for EPGs are assigned by the APIC and are sent across through the APIC agent. The APIC agent polls the APIC for the EPGs added in the SCVMM cloud. The agent creates a virtual machine network with the VLANs specified in the EPGs. SCVMM then creates a virtual machine and attaches the newly created virtual machine to the virtual machine network. When the virtual machine is attached to the virtual machine network, the Hyper-V hosts send the message “EP Attach” to the connected leaf switch through the OpFlex protocol. The leaf switch sends a message about the new endpoint (EP) to the APIC. The APIC then downloads the created endpoint policies to the leaf switch.

Figure 5 shows the SCVMM logical connectivity with the integrated Cisco ACI fabric. SCVMM integrates with Cisco ACI using the Cisco ACI plug-in, which is installed in Microsoft Windows Services. Using REST APIs, the administrator can access the APIC and create the required policies. The figure also shows the Cisco ACI fabric and Hyper-V hosts with all the virtual machines running on each of these hosts.
When SCVMM is integrated with Cisco ACI fabric, EPGs are created in the APIC and pushed to SCVMM as virtual machine networks. Virtual machines provisioned in SCVMM can then consume these networks.
Microsoft SCVMM Support for Microsoft SQL Server

Microsoft has added application deployments that support the System Center 2012 VMM. The VMM natively deploys instances of SQL Server, as service-oriented applications, to private clouds managed by the VMM. With this private cloud implementation, Microsoft blurs the line between the virtualization platform and the application.

The high-level steps for deploying an instance of SQL Server 2014 with VMM are as follows:

1. Create a SQL Server profile in the VMM that uses the virtual hard disk (VHD) image from the system-prepared virtual machine.
2. Create a VMM service template that includes the SQL Server profile as an application.
3. Deploy an instance of the service (a new virtual machine running SQL Server 2014) in the private cloud.

Logical Connectivity of Microsoft SCVMM with Cisco ACI Fabric

Figure 6 shows the logical connectivity of the network design. In the figure, the SQL nodes, which are Hyper-V hosted virtual machines, are connected to the Hyper-V logical network in the SCVMM cloud through four unique virtual machine network interface cards (VMNICs). Out-of-band management ports of Hyper-V hosts and the Cisco ACI fabric are connected to Catalyst 3750 Switches for management connectivity.

Figure 6. Logical Connectivity of Network Components
This example uses four VMNICs—Public, Cluster, SQLServices, and CommonServices—created on SQL nodes 1 and 2, which are part of the EPGs. When an EPG is created, the APIC assigns a unique VLAN to the created EPG from the VLAN pool. These VLANs segregate the traffic among the created EPGs. The Public and CommonServices EPGs communicate through contracts. The data plane has 10 Gigabit Ethernet connectivity through the Cisco UCS VIC 1225.

Like any other computing stack, this solution also depends on an out-of-band management network to configure and manage network and computing nodes through a 1 Gigabit Ethernet modular LOM (mLOM). The management interfaces from the physical servers are physically connected to the out-of-band management switches. Management network access is also required to access Hyper-V hosts and management virtual machines. To support reliance on the out-of-band management connectivity, Cisco UCS rack servers are directly connected to the out-of-band management switches, and in this design the management network path is separated from the data network path. The following section provides more information about how to create EPGs and contracts.

As shown in Figure 7, Cisco UCS rack servers, Hyper-V, SCVMM cloud, client virtual machine, and Cisco ACI leaf and spine switches are connected to the Catalyst 3570 Switches deployed in a pair to provide out-of-band management.

Some of the design principles used in this deployment model include the following:

- Both leaf switches are connected to the spine switches with dual-connected 40 Gigabit Ethernet.
- A unique private network and associated bridge domain are defined for the tenant, forming a private Virtual Routing and Forwarding (VRF) network. The VRF instance provides connectivity to the external infrastructure.
- Unique VLANs are configured for the tenant to provide per-tenant connectivity in the Cisco ACI fabric.

In this design, an application tenant is configured with (at least) two separate domains: an SCVMM domain and a physical machine domain, for internal application communication and external application connectivity, respectively.

![Figure 7. Configured Domains in the Tenant](image)
Application tiers communicate internally using contracts between various EPGs. The external communication for the application is provided by defining the external-facing contracts in the private network. The external-facing host and virtual machines such as the SQL nodes are statically bound to connect to the internal networks using contracts (Figure 8).

Figure 8. Static Binding of SQL Node

The tenant SQLDBServices contains an application network profile: SQL-Application. The application network profile contains EPG-Public, EPG-SQLServices, EPG-CommonServices, and EPG-Cluster. The EPGs can talk to each other using contracts.

As discussed earlier, the created EPGs are attached to the VMM domain in the Microsoft SCVMM cloud as part of the Infrastructure configuration. The virtual machine network, which is pushed to the SCVMM by the APIC, will have a VLAN assigned from the created VLAN pool. By default, the APIC dynamically manages the allocation of a VLAN for an EPG. After an EPG is configured and attached to the SCVMM domain, the configured virtual machine networks will be displayed as shown in Figure 9.

Figure 9. Configured Virtual Machine Networks in the Tenant SQLDBServices
Creating EPGs and Defining Contracts

Figure 10 shows the steps involved in creating EPGs and defining contracts for the created EPGs to establish communication.

**Figure 10.** Workflow for Creating EPGs and Contracts

Figure 11 shows the relationship between the EPGs with the created application profiles. The tenant SQLDBServices contains SQL-Application profiles. An application profile contains four EPGs: EPG Public, EPG SQLServices, EPG CommonServices, and EPG Cluster. The EPGs can talk to each other using the CommonServices and Public contracts.

**Figure 11.** EPGs Attached to Application Profile
Figure 12 shows the mapping of the SCVMM network to EPGs.

**Figure 12.** Consumer and Provider Contracts Between EPGs

- **EPG CommonServices:** In almost all the application deployments, application servers need to access common services. Some examples of common services are Active Directory, DNS, and management and monitoring software. In this solution, EPG CommonServices was created to host services shared among the EPGs. The policies defined in the CommonServices EPG can be used by any EPG or tenant.

- **EPG Cluster:** Communication between server clusters is critical for smooth cluster operations. This example uses the dedicated EPG Cluster for secure communication, allowing WSFC network communication.

- **EPG SQLServices:** EPG SQLServices is a dedicated EPG that allows communication between SQL Server 2014 services and the availability group.

- **EPG Public:** EPG Public allows external client network communication with SQL services.

Figure 13 summarizes the details.
**CommonServices contract:** This is a service contract created between EPGs SQLServices, CommonServices, and Cluster. The CommonServices EPG provides the contract, and the SQLServices and Cluster EPGs are the consumers for CommonServices (provider contract). With these two contracts, the CommonServices EPG shares services such as Lightweight Directory Access Protocol (LDAP), DNS, DHCP, and Remote Display Protocol (RDP) among the EPGs. Contracts use CommonServices filters to limit the traffic between the applications to certain ports and protocols. CommonServices uses filters that allow only ports 53, 67, 389, and 3389 for secure communication between EPGs in this example.

**Public Contract:** This contract enables external access. In this example, a service contract is created between two EPGs, Public and SQLServices, with SQLServices providing contract to the Public EPG to allow the external client to connect and access SQL database services. The Public contract uses filters to limit the traffic between the application’s designated SQL Server listener port. In this example, a filter is created for secure access, allowing the EPG SQLServices to communicate only on port 1433.

The EPGs associated with the virtual machine network are displayed in the VM Networks window. You can directly use the virtual machine network to connect any existing or new virtual machines.

When you attach a virtual machine to the virtual machine network on SCVMM, power on the virtual machine and do the following (Figure 14):

- Verify the endpoint policy on the APIC.
- Verify the association on the APIC.
- Verify EPGs on the APIC.
Figure 14. Verify the Hardware Configurations in Microsoft SQL Server 2014

Workload Details
A standard TPC-C workload with an OLTP database of 50 GB was run on the primary and secondary SQL Servers (SQL node 1 and SQL node 2). HammerDB, load-test tool, ran up to 50 user workloads.
Validation

Performance validation for a pair of Microsoft SQL Server 2014 platforms with synchronized replication was performed using the Availability Group Test tool. This tool captured the true end-to-end statistics for the client-observed failover time (Figure 15).

Figure 15. Availability Group Test Showing Complete Failover Time

Validation

To emulate a complete node failure, the test ran HammerDB SQL TPC-C workload on the SQL AG instance (listener instance) from the external public network, and the node 1 host (primary server) was powered off. HammerDB showed a SQL execution failure. When the HammerDB SQL TPC-C test running on the client was restarted, the system again was able to connect to the SQL AG instance.

Cisco APIC Network Statistics

Cisco ACI is designed to offer a combination of software and hardware that can provide real-time hop-by-hop visibility and telemetry. Cisco APIC can present detailed information about the performance of individual EPGs and tenants in the network. This information includes details about latency, packet drops, and traffic paths and can be sliced at the EPG or tenant level. Telemetry information can be useful for a wide range of troubleshooting and debugging tasks, enabling an operator to quickly identify the source of a tenant problem across the physical and virtual infrastructure.

The APIC is the point of configuration for policies and the place where statistics are archived and processed to provide visibility, telemetry, application health information, and overall management of the fabric. You can see the real-time metrics in the APIC. You can choose to monitor traffic at any level, from tenant to the EPG, on the STATS tab in the right pane of the APIC GUI.
Figures 16 and 17 show the statistics for the network bandwidth used while running the workload on SQL Server 2014. The figure shows the bandwidth utilization metrics sliced at the Public and SQLServices EPGs.

Public or external clients, which are not in the Cisco ACI and SCVMM domain, can access SQL databases from an assigned port within the Cisco ACI and SCVMM domain. The complete transaction between the external clients and Cisco ACI and SCVMM domain happens on this assigned port, which provides complete isolation and security to the traffic within the Cisco ACI fabric. Figure 16 shows network bandwidth utilization of 1240 MB by external clients while accessing the SQL databases.

**Figure 16.** APIC Statistics for EPG Public

Between the SQL nodes, aggregated traffic is generated by the replication of the primary and secondary nodes along with the external client's workload while accessing the SQL databases. Figure 17 shows that the network bandwidth utilization is slightly higher (1400 MB) than that generated at the Public EPG, because of the additional replication traffic aggregation at the SQLServices EPG.
Verification Summary

Testing verified that the failover was completed successfully. Additional checks were performed to verify that the schema and application structures for the primary replica on the primary node and the secondary readable replica on the secondary node were consistent after failover.
Conclusion
As businesses quickly move to make the data center more agile, application-centric automation and virtualization of both hardware and software infrastructure become increasingly important. Cisco ACI builds the critical link between business-based requirements for applications and the infrastructure that supports them. Microsoft SCVMM integration with Cisco ACI fabric has proven to be an easy-to-manage, easy-to-deploy, self-contained infrastructure for an enterprise-class Microsoft SQL database server. This framework has proven to yield optimal performance, high-availability, efficiency, and lower infrastructure cost.

References
- Cisco Application Centric Infrastructure:
- Microsoft Windows Azure Pack integration: