March 20, 2018

Managing virtual networks and other resources in a mixed managed domains

Harish B Kamath
Hewlett Packard Enterprise

Brajendra Kum Bajpai
Hewlett Packard Enterprise

Param Jeet Singh
Hewlett Packard Enterprise

Mohit Gera
Hewlett Packard Enterprise

Managing virtual networks and other resources in a mixed managed domains

Abstract

HPE OneView is a resource model based infrastructure management appliance which automates deployment, provisioning and integration of compute, storage, and networking infrastructure in a data center. APIC is a policy based manageability appliance for Cisco ACI fabric and offers services to manage policies on a collection of resources of a data center. Cisco ACI interfaces with VMware and automates creation of virtual networks for VMware environment. Cisco ACI also integrates with OpenStack and Microsoft systems for network automation requirements. Keeping OneView resources current with Cisco ACI policies is complex, time consuming and error prone task. Realizing this through an automated mechanism is equally complex involving mechanism to handle large volume of policy updates, ability to handle with low latency, work with message bursts and operate with undefined frequencies.

Compute modules or blades are physically interfaced to the data center network via interconnect module (ICM). Compute modules may be a bare-metal server or a hypervisor based system that carries traffic over virtual networks from VMs.

Traffic from compute modules are transported into ICM over s-channels or downlink ports over virtual networks which is further switched to external network via an uplink port. The uplink port may further be interfaced to leaf switch of Cisco ACI for carrying the network beyond. Configurations across the participating nodes should be in alignment in order to establish a path between the two end points.

OneView manages composable infrastructure using a resource model scheme and is responsible to define VLANs in ICM for usage by uplink ports and downlink ports. APIC, Cisco ACI controller enables users to define and manage policies for usage across Cisco ACI infrastructure. vCenter, manageability component for VMWare's ESXi, allows management of resources in the hypervisor environment.

APIC, OneView and vCenter are three different management layers consisting of resources/policies which require to be in alignment. Additionally, vCenter when integrated into APIC infrastructure results into automation of creating, defining policies/resources in APIC and vCenter. Few of these policies may be commissioned through a recursion process, e.g., VLANs may be created when connectivity to server has been established.

APIC policies that are of interest to OneView may be applied at Fabric level or applied onto interfaces, networks, etc., and is managed through Managed Information Tree object. OneView manages through a resource model approach containing resources such as Logical Interconnect, Uplink Set, VLANs, and more.

In a few configuration scenarios, resolving interdependence, sequencing plays an important aspect to realize the policies or resources.

In this methodology we automate creation of OneView resources and have it in compliance with APIC policies and VMware resources through discovery process, relationship building and through the actions of remediation. Automation may be manually triggered or through an event mechanism. WebSocket based mechanism provided to interface with HTTP(s) enables subscribers to handle policy updates asynchronously.

As an example, APIC administrators' action has resulted into generation and creation of one or more VLANs onto an ACI-Leaf interface and also deploying corresponding set of VLANs into VMWare environment. This methodology would walk through the correlated set of APIC policies and also establish relationship with corresponding OneView resources e.g., Logical Interconnect Group, Logical Interconnect, Uplink Set, VLAN, etc., in order to remediate one or more resources of OneView.

High level flow of information may be provided as below:

1. Get a snapshot of hierarchical & associated set of Policies from Policy Management Infrastructure (APIC as example, inclusive of VMWare)

2. Get a resource listing from OneView ('Policy' used for APIC & VMWare, 'Resource' used for OneView)

3. Construct a management information tree using Policies and Resources data
    Identify policies and resources as nodes of management information tree e.g., Tenant, application profile, uplink set
    For all policies and resources
    Correlate policy with resources
    If a nodal type
    Construct node object
    Inject node object at a corresponding hierarchical level
    Evaluate to report compliance status on node object
    Update compliance status to self and parent hierarchy where applicable
    If node is non-compliant, construct a remediation list
    e.g., network non-compliance in uplink set could result into adding a network into the VLAN-pool, uplink set and compliance status update
4. Subscribe to events on resource updates of OneView
5. Subscribe to events on policy updates of APIC
6. On receipt of an event
    Serialize Event Handling:
    If the event type of the message is in process then retry to process after an interval
    Else start a task to handle the event
7. Event Handler:
    Distinguish and ingest events from OneView and APIC
    Traverse the management information tree to locate the impacted node corresponding to the event
    Correlate event data against the node object

If object does not exist, inject a new node object at a corresponding hierarchical level
Else Update node object with message contents (could be to flag remove of the node)
If event type is applicable to multiple nodes, update related nodes
e.g., add network event on an APIC interface could result into reference to Uplink set, VLAN-pool & network-set object
Evaluate to report compliance status on the new/updated node object
Update compliance status to self and parent hierarchy where applicable
If node is non-compliant, construct a remediation list

8. For all elements of remediation list
If the element type is in execution retry to execute with an interval
Else start a task to Remediate OneView resources

9. For all updated node objects
If node object status is 'remove'
Delete OneView resource, if applicable
Delete node from the management information tree

APIC provides a mechanism to asynchronously monitor a collection of policies applicable to one or more connects (users) and via WebSocket mechanism. This is achieved by following the steps below -
a) Creation of WebSocket
b) Subscribing to identified list of policies
c) Associating subscribed list of policies over WebSocket

Policy updates received on the WebSocket channel is processed to drop or have it consumed by policy processors for additional set of actions. WebSocket channel processor is driven by a rule table, that inspects policy descriptions to purpose any actions and for the type of actions to be performed. As example scenarios -
1. A policy update on adding a VLAN onto a Tenant would result into deciphering the policy description, mapping onto corresponding OneView resource in order to create an object model
2. A Tenant in APIC contains Application Profiles, End-Point Groups, associated domain relationship, associated VLANs and more. A delete message related to End-Point Group result into policy updates for the hierarchy of policies below it and may be arriving in any sequence. This scheme drops the message when already processed by higher level

3. VLAN pool may be associated with one or more Tenants. Policy update to a VLAN pool would result into multiplicative effect by having it propagated to additional set of Tenants and also resulting into VMM related policy hierarchy
4. A creation of End-Point Group in ACI would result into three messages. Message-1 and Message-2 with an operation status of creation, and Message-3 with an operation status of Modified. The policy type belonging to Message-1 create operation has an effect of creating End-Point Group in ACI while other two messages essentially brings in a state change to End Point Group. In one scenario, the processor processes Message-1, while Message-2 and Message-3 are dropped. In another scenario, the processor processes Message-1 and Message-3 and drop Message-2.

The behavior of various policies and its application context is realized in a table form to introduce a data driven behavior for yielding statelessness, better performance and efficiency into the system.

The system sustains through subscription id changes caused by network disruptions, time-outs, etc., and thus provide seamless experience for message handling once subscribed.

High level logic

Create WebSocket connection with Policy Manager (APIC)
Periodically refresh WebSocket connections or refresh due to network issues

Identify list of global policy types e.g., Infrastructure, VMM Domain
Prepare groups of sub policy types

For each Tenant Policy Type
Prepare groups of sub policy types

For each group
Subscribe on a group (collection of sub policy types) over a WebSocket connection
Build a subscription_key for a given subscription_id

Periodically refresh policy specific subscriptions
Update subscription_key association with subscription_id when changed

On exceptions as a result of WebSocket issues, internal resource constraints or any incompatibilities, messages are internally generated

Listen to subscriptions
Parse the received message
Lookup for subscription_id and corresponding subscription_key
Perform action based on the table contents using policy type, status and other message parts where applicable
Actions performed may be to drop, replicate & queue, queue, etc., using subscription_key

Advantages
1. Ability to introduce blade and compute nodes with ease into the data center network specifically when working across management domains - vCenter, OneView & Cisco APIC
2. Minimizes human effort, eliminates human errors and skill needs at the time of deployment
3. Reduces time to deploy a Synergy infrastructure significantly
4. Ability to keep OneView resources current and active w.r.t other management domains
5. Automatically synchronizing resources of OneView with multiple policy management domains
6. Obtaining live compliance report against direct and indirect resources or policies across management domains

Disclosed by:

Harish B Kamath – Hewlett Packard Enterprise

Brajendra Kum Bajpai – Hewlett Packard Enterprise

Param Jeet Singh – Hewlett Packard Enterprise

Mohit Gera – Hewlett Packard Enterprise