Project 2016-02
CIP P Modifications

Webinar on Standard Drafting Team Considerations for the Use of Virtualization in the CIP Environment
April 18, 2017
• NERC Antitrust Guidelines
  - It is NERC’s policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

• Notice of Open Meeting
  - Participants are reminded that this webinar is public. Notice of the webinar was posted on the NERC website and the access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.
• Opening Remarks and Introduction of Presenters
• Administrative Items
  ▪ Antitrust and Disclaimers
  ▪ Webinar Format
• Standard Drafting Team
• Hypervisors
• What is multi-tenancy?
• Questions and Answers
<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-Chair</td>
<td>Christine Hasha</td>
<td>Electric Reliability Council of Texas</td>
</tr>
<tr>
<td>Co-Chair</td>
<td>David Revill</td>
<td>Georgia System Operations Corporation</td>
</tr>
<tr>
<td>Members</td>
<td>Steven Brain</td>
<td>Dominion</td>
</tr>
<tr>
<td></td>
<td>Jay Cribb</td>
<td>Southern Company</td>
</tr>
<tr>
<td></td>
<td>Jennifer Flandermeyer</td>
<td>Kansas City Power and Light</td>
</tr>
<tr>
<td></td>
<td>Tom Foster</td>
<td>PJM Interconnection</td>
</tr>
<tr>
<td></td>
<td>Richard Kinas</td>
<td>Orlando Utilities Commission</td>
</tr>
<tr>
<td></td>
<td>Forrest Krigbaum</td>
<td>Bonneville Power Administration</td>
</tr>
<tr>
<td></td>
<td>Philippe Labrosse</td>
<td>Hydro-Quebec TransEnergie</td>
</tr>
<tr>
<td></td>
<td>Mark Riley</td>
<td>Associated Electric Cooperative, Inc.</td>
</tr>
</tbody>
</table>
Virtualization Webinar Summary

1. **Hypervisors**
   - Template Considerations
   - Why VM guest need to be treated as CyberAsset
   - Security Patches address ongoing Hypervisor Vulnerabilities

2. **What is multi-tenancy?**
   - Define Multi-tenancy, Tenants, Overlay, and Underlay
   - Building a multi-tenant environment
   - Introduce ESZ Concept
Hypervisor Templates - VDI Use Cases

Master Image – Windows 10
Hypervisor Templates - VDI Use Cases

Master Image – Windows 10

Assumes patched state from master image when created

TIME

Master Image

VM Topology

Matt’s VM

Master Image

VLAN 20

Virtual Switch
Hypervisor Templates - VDI Use Cases

Master Image – Windows 10

Assumes patched state from master image when created

Matt

Matt Logs out, gets deleted

VM Topology

Master Image

VLAN 20

Virtual Switch
Hypervisor Templates - VDI Use Cases

Master Image – Windows 10

Matt
- Assumes patched state from master image when created
- Matt logs out, gets deleted

Philippe
- Assumes patched state from master image when created

VM Topology
- Philippe’s VM
- Matt’s VM
- Master Image

VLAN 20
Virtual Switch
Hypervisor Templates - VDI Use Cases

- Master Image – Windows 10
- Matt
  - Assumes patched state from master image when created
  - Matt logs out, gets deleted
- Philippe
  - Assumes patched state from master image when created

Patched During Regular Patch Cycle

VM Topology:
- Philippe’s VM
- Matt’s VM
- Master Image

VLAN 20
Virtual Switch
HV Templates - Dormant Images

Gold Image – Windows Server

VM Topology

VLAN 90
VLAN 20

Virtual Switch
HV Templates - Dormant Images

Use Cloning Process to create new server

Gold Image – Windows Server

Unpatched Windows Server

VM Topology

- VLAN 90
- VLAN 20

Virtual Switch
HV Templates - Dormant Images

1. Use Cloning Process to create new server
2. Apply Patches
3. Unpatched Windows Server
4. New Server Windows Server

Gold Image – Windows Server

VM Topology
- VLAN 90
- VLAN 20
- Virtual Switch
CIP Considerations for the Gold Images

- Patched During Regular Patch Cycle
- Use Cloning Process to create new server
- Apply Patches
- Unpatched Windows Server
- New Server Windows Server

VM Topology
- VLAN 90
- VLAN 20
- Virtual Switch
Considerations for Templates in CIP-010

- **Baseline Templates**
  - Could be created for Database Servers, Webservers, etc
  - Contains no specific application settings but is up to date with security patches and baselined software packages for rapid deployment

- **CIP-010 Part 1.1 requires the development of a baseline configuration individually or by group, demonstration of compliance for the VMs could be achieved by using the baseline configuration of the Master Image, all baseline configuration elements being identical to the master image for all instances created.**
VM’s as Software on Cyber Assets
VM’s as Software on Assets: Ports/Services
VM’s as Software on Assets: Ports/ Services

Cyber Asset Asset #1

Cyber Asset Asset #2

Ports/Services List
VMHost Ports
Guest #1 Ports
Guest #2 Ports

VMHost

Guest #1

Guest #2

MIGRATION

 Ports/Services List
VMHost Ports
Guest #2 Ports
VM’s treated as CA’s: Ports/ Services
VM’s treated as Software on bare-metal HV: Malware Prevention
VM’s treated as Software on bare-metal HV: Malware Prevention

- Bare-Metal Hypervisor
  - Has access to a factory provisioned set of resources and isolated Codebase

- Console VM
  - Has access to configure and monitor through vendor proprietary mechanism

- Resource Scheduler
  - Has access to all physical Resources (CPU, Mem) and has an isolated Codebase

- VM
  - Has access to Administrator configured Resources (CPU, Mem, etc.)
  - Separate Codebase

- VLAN 30 MGT
- VLAN 20
VM's treated as Software on bare-metal HV: Malware Prevention

- Bare-Metal Hypervisor
  - Has access to a factory provisioned set of resources and isolated codebase

- Console VM
  - Has access to configure and monitor through vendor proprietary mechanism

- Resource Scheduler
  - Has access to all physical resources (CPU, Mem) and has an isolated codebase

- VM
  - Has access to administrator configured resources (CPU, Mem, etc.)
  - Separate codebase

- VLAN 30 MGT
  - VLAN 20
VM’s treated as Software on bare-metal HV: Malware Prevention

- Bare-Metal Hypervisor
  - Has access to a factory-provisioned set of resources and isolated codebase

- Console VM
  - Has access to configure and monitor through vendor proprietary mechanism

- Resource Scheduler
  - Has access to all physical resources (CPU, Mem) and has an isolated codebase

- VM
  - Has access to administrator configured resources (CPU, Mem, etc.)
  - Separate codebase

- VLAN 30 MGT

- VLAN 20
VM’s treated as Software on bare-metal HV: Malware Prevention

- Has access to a factory provisioned set of resources and isolated codebase
- Has access to configure and monitor through vendor proprietary mechanism
- Has access to all physical resources (CPU, Mem) and has an isolated codebase
- Has access to administrator configured resources (CPU, Mem, etc)
- Separate codebase
VM’s treated as Software on bare-metal HV: Malware Prevention
VM’s treated as Software on Hosted HV: Malware Prevention

- VLAN 30 MGT
  - Has access to all Resources
  - Resource schedule runs Inside of OS

- Hosted Hypervisor

- VM
  - Has access to Administrator configured Resources (CPU, Mem, etc)
  - Separate Codebase

- VLAN 20
Hypervisors and VM’s should be treated as discrete cyber assets

- It is difficult to keep proper redundancy strategies in place with hypervisors when treating VM’s as software on the CA
- Bare-metal hypervisors have strong separation using an independent resource scheduler that prevents malware from accessing the backplane. Hosted platforms do not have this separation and require additional steps to maintain security such as management plane isolation
- Malware detection considerations need to be applied direction to all operating systems involved. Applying them at the hypervisor is not sufficient to ensure security
• Because the hypervisor ensures the separation of guests, it needs to be patched regularly:
  - Security patches address ongoing Hypervisor vulnerabilities such as VM escape attacks
  - Hypervisor is a Cyber Asset; afforded same controls including physical security
  - NIST bare-metal hypervisors have a smaller attack surface (SP800-125 chapter 2)
    - Reduced devices drivers
    - Management Plane Separation
1. **Hypervisors**
   - Template Considerations
   - Why VM guest need to be treated as PCA's
   - Security Patches address ongoing Hypervisor Vulnerabilities

2. **What is multi-tenancy?**
   - Define Multi-tenancy, Tenants, Overlay, and Underlay
   - Building a multi-tenant environment
   - Introduce ESZ Concept
Multi-Tenancy Definitions

- **Multi-Tenancy** - an environment where a shared infrastructure serves multiple tenants.
- **Tenants** – discrete groups of applications, functions, or environments that share a common resource with specific privileges or security levels that consume resources from the shared infrastructure. The instances (Tenants) are logically isolated but physically interconnected.
- **Underlay Network** – A network that supports Overlay Networks. It does not trust the overlay network.
- **Overlay Network** – A network utilized by Tenant. It is unaware that the underlay network exists.
- **Centralized Management System** - A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management or patch management.
Multi-Tenancy: Management and Data Plane Isolation

Data Plane
- VLAN 10
- VLAN 20
- External Router

Out of Band Management Plane
- Centralized Management Tools
- Hypervisors
- Firewall
- Switches
- Storage Arrays
- iSCSI Storage Array
- VLAN 30 MGT
- VLAN 70 STORAGE
Multi-Tenancy: Basic Physical Devices

- HyperVisor
- Storage Array
- Switch
- Firewall
Multi-Tenancy: Centralized Management Systems

- Layer 2 Switch – Out of Band
- VLAN 30 MGT
- Centralized Management Tools
- HyperVisor
- Storage Array
- Switch
- Firewall
Multi-Tenancy: Adding Tenant Networks

Centralized Management Tools

Layer 2 Switch – Out of Band

VLAN 30 MGT

HyperVisor

Storage Array

Switch

Firewall

VLAN 10

VLAN 20

Physical Interface
Multi-Tenancy: Adding Tenant Networks

Tenant Topology

Centralized Management Tools

VLAN 30 MGT

HyperVisor

Storage Array

Switch

Firewall

VLAN 10

VLAN 20

Physical Interface
Multi-Tenancy : Add Some Storage

Tenant Topology

Centralized Management Tools

Layer 2 Switch – Out of Band

VLAN 30 MGT

HyperVisor

Storage Array

Switch

Firewall

Logical Disk #1

Logical Disk #2

Mask #1

Mask #2

LUN Masking

VLAN 10

VLAN 20

Physical Interface

VLAN 10

VLAN 20
Multi-Tenancy: Add some VM’s
Multi-Tenancy: Add a Firewall

Tenant Topology

Centralized Management Tools

VLAN 30 MGT

HyperVisor
Guest #1
Guest #2
Virtual Switch
VLAN 10
VLAN 20

Storage Array
Logical Disk #1
Logical Disk #2
LUN Masking

Switch
VLAN 10
VLAN 20
Physical Interface

Firewall
Firewall Services
VLAN 10
VLAN 20
VLAN 50
P. Int
• Multi-Tenancy Considerations
  - VM Infrastructures are designed to support Multi-Tenancy from the ground up and should be considered to be Multi-Tenant environments even if there is only one Tenant
  - Tenant Systems should not have access to the management plane (Logical Isolation at a minimum, Physical is best)
  - Underlay hardware assumes the highest level of security because it required for all Tenants to perform their functions
  - Tenants “Transit” the Underlay, but have no means of accessing it
The SDT is considering the creation of a construct called an Electronic Security Zone to describe controls used to separate Tenants with logical isolation

- This concept would be used to separate the management plane from the data plane
- The concept can be used to create other ESZ’s within an ESP (Such as to isolate outbound communication, or to split a storage array)
- Devices that support multi-tenancy need to use the management ESZ to communicate with their Centralized Management System(CMS)
- Not limited to networking concepts, can be used to model any type of logical control
ESZ Example: Management Plane Isolation

Layer 2 Switch – Out of Band

Management ESZ

Centralized Management Tools

VLAN 30 MGT

HyperVisor

Storage Processor

Switch

Firewall

Guest #1

Guest #2

Virtual Switch

LUN Masking

Physical Interface

Data Plane ESZ

Firewall Services
ESZ Example: DMZ Separation

Management ESZ

Centralized Management Tools

Layer 2 Switch – Out of Band

VLAN 30 MGT

HyperVisor

VLAN 10
Guest #1
Virtual Switch
ESZ PROD

VLAN 20
Guest #2
ESZ DMZ

Storage Processor

Mask #1
LUN Masking
ESZ PROD

Mask #2
ESZ DMZ

Switch

VLAN 10
ESZ PROD

VLAN 20
ESZ DMZ

Physical Interface

VLAN 10A

Firewall

VLAN 10
P. Int
ESZ PROD

VLAN 20
P. Int
ESZ DMZ

Firewall Services
ESZ Example: DMZ Separation

Management ESZ

Data Plane

VLAN 10

VLAN 20

ESZ PROD

ESZ DMZ

External Router

Layer 2 Switch – Out of Band

HyperVisor

VLAN 10

VLAN 20

ESZ PROD

ESZ DMZ

Guest #1

Guest #2

VLAN 10

VLAN 20

Mask #1

Mask #2

LUN Masking

Physical Interface

VLAN 10

VLAN 20

P. Int

P. Int

VLAN 10

VLAN 20

Firewall Services

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ

ESZ PROD

ESZ DMZ
ESZ Example: DMZ Separation

Diagram showing a network with VLANs 10, 20, SCADA, ICCP, and a firewall.
ESZ Example: ESZ vs ESP
ESP and ESZ Interaction?
The SDT is considering the creation of a construct called an Electronic Security Zone to describe controls used to separate Tenants with logical isolation

- This concept would be used to separate the management plane from the data plane
- The concept can be used to create other ESZ's within an ESP (Such as to isolate outbound communication, or to split a storage array)
- Devices that support multi-tenancy need to use the management ESZ to communicate with their Centralized Management System (CMS)
- Not limited to networking concepts, can be used to model any type of logical control
Questions and Answers