NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Virtualization Overview

Project 2016-02 – CIP Modifications

RF Workshop
CIP SDT Members
June 2020

RELIABILITY | ACCOUNTABILITY




Agenda

- Virtualization Overview
- Clarification for Permitted Architectures
- Additional Capabilities Enabled
- CIP Standards Impact

Virtualization Overview

- What is Virtualization?
  - Comparison to the Interconnected BES
- Reliability Benefits
- Security Benefits

Disclaimer

Virtualization changes to CIP standards are to ***ENABLE*** *new methods/models*

NOT

REQUIRE *Them*

Clarification for permitted architectures

Clarification – Hypervisors and Storage Systems

Hypervisors are the EMS of Virtualized infrastructure

- What is a Hypervisor?
- Why use Hypervisors?
- Challenges for CIP Compliance
- Changes Made

Clarification – Virtual Machines

Virtual Machines are a now “Form” of computing

- What is a Virtual Machine?
- Why use Virtual Machines?
- Challenges for CIP Compliance
- Changes Made

Clarification – Containers

Containers are an even newer “Form” of computing

- What is a Container?
- Why use Containers?
- Challenges for CIP Compliance
- Changes Made

Clarification – Super ESPs

What do Super ESPs have to do with Virtualization?

- What is a Super ESP?
- Why would you need a SuperESP?
- Challenges for CIP Compliance
- Changes Made

Clarification – Management

Management of the infrastructure, like Dispatch

- What is a:
  - Management System?
  - Management Interface?
  - Management Module?
- Why are Management Systems used?
- Challenges for CIP Compliance
- Changes Made

Additional Capabilities Enabled

Additional Capabilities – Zero Trust

Enhanced and Automated Access Control through Zero Trust

- What is Zero Trust?
- Why use Zero Trust
- Challenges for CIP Compliance
- Changes Made

Additional Capabilities – Hardware and Software Reduction

Hardware and Software Reduction through Logical Isolation and common trust levels

- What can be reduced?
- Why take advantage of Hardware and Software Reduction
- Challenges for CIP Compliance
- Changes Made

Additional Capabilities – Network Access Control

Automated control and compliance through Network Access Control

- What is a Network Access Control?
- Why use Network Access Control
- Challenges for CIP Compliance
- Changes Made

CIP Standards Impact

- Technical Standards impact:
  - CIP-005 – biggest impact
  - CIP-007 – minor impact
  - CIP-010 – moderate impact
- Definitions
- Conforming changes to other Standards

2016-02 SDT Virtualization Updates

- Drafting Technical Rationale and Implementation Guidance for each:
  - CIP-005
  - CIP-007
  - CIP-010

- Mini Webinars are the focus of outreach
- Link to Project 2016-02 Related files page.

2016-02 SDT Meeting Schedule

- Weekly Conference Calls – Thursdays 3:00 – 5:00 p.m. eastern
- Periodic Mini Webinars
  - Virtualization Overview - Completed
  - ERC/IRA – Completed
  - Hypervisors and Storage Systems – Completed
  - VM and Containers – Completed
  - SuperESP – July 2, 2020
  - Management Systems – TBD
  - Hardware and Software Reduction, Network Access Control, Automation of Compliance and Evidence Gathering – TBD

Q&A Objectives

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the Standard Drafting Team.

Questions and Answers

Jordan Mallory
Jordan.Mallory@nerc.net