Cisco HX Data Platform Security Hardening Guide

Version 4.01rev1

October 4, 2019
Document Information

<table>
<thead>
<tr>
<th>Document Summary</th>
<th>Prepared for</th>
<th>Prepared by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco HX</td>
<td>v.4.01rev1</td>
<td>Field</td>
</tr>
<tr>
<td>Last Modified</td>
<td>7 October 2019</td>
<td>Aaron Kapacinskas</td>
</tr>
<tr>
<td>Previous Version</td>
<td>4.01</td>
<td></td>
</tr>
</tbody>
</table>

Changes in this version:
- Added HX Release model update to HX Patching
- CNSA compliance added to Other Certifications and Procedural Guidelines
- ACVP added to Certification Process
- Added ECC Certificates to Certificate Signing Requests
- Updated Remote syslog-ng configuration file(s) in Appendix E

Intended Use and Audience
This document contains confidential material that is proprietary to Cisco Corporation. The materials, ideas and concepts contained herein are to be used exclusively to assist in the configuration of Cisco corporation’s software solutions.

Legal Notices
All information in this document is provided in confidence and shall not be published or disclosed, wholly or in part to any other party without Cisco’s written permission.
# Contents

Document Information........................................................................................................... 2
  Intended Use and Audience ................................................................................................. 2
  Legal Notices ...................................................................................................................... 2

Prerequisites ........................................................................................................................ 7

Introduction .......................................................................................................................... 7

Secure Product and Development Components ..................................................................... 8
  Development Milestones........................................................................................................ 8
  CSDL Philosophy ................................................................................................................ 8
  CSDL Product Adherence Methodologies ........................................................................... 9

Vulnerability Handling ........................................................................................................... 9
  Tenable IO Scanning ........................................................................................................... 9
  CERT Advisory .................................................................................................................. 10
  VMware ESX Patching ......................................................................................................... 10
  HXDP Patching .................................................................................................................. 11

Additional Vulnerability Testing Measures ........................................................................... 11

Secure Platform “Modules” ................................................................................................... 11
  Control Plane ...................................................................................................................... 11
  Data Security ...................................................................................................................... 11
  Management Security ......................................................................................................... 11

Certification Process ............................................................................................................. 11
  ACVP .................................................................................................................................. 11

Current Certifications .......................................................................................................... 12
  FIPS .................................................................................................................................. 12
  Common Criteria ................................................................................................................ 13

Other Certifications and Procedural Guidelines .................................................................... 14
  ISO 27001 .......................................................................................................................... 14
  FISMA ................................................................................................................................. 14
  FedRAMP ............................................................................................................................. 14
  IAVA ................................................................................................................................... 14
  HIPAA ................................................................................................................................. 14
### HX Components and Environment

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Components</td>
<td>16</td>
</tr>
<tr>
<td>Cisco UCS</td>
<td>17</td>
</tr>
<tr>
<td>Cisco UCS Fabric Interconnects (FIs)</td>
<td>18</td>
</tr>
<tr>
<td>HX Nodes</td>
<td>18</td>
</tr>
<tr>
<td>Management Interfaces: HX Connect and the VMware vCenter Plug-in</td>
<td>20</td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>21</td>
</tr>
<tr>
<td>VMware ESX</td>
<td>21</td>
</tr>
<tr>
<td>VMs</td>
<td>21</td>
</tr>
<tr>
<td>Client Machines</td>
<td>21</td>
</tr>
</tbody>
</table>

### HX Secure Network Environment and Component Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX Connect and the VMware vCenter Plug-in</td>
<td>21</td>
</tr>
<tr>
<td>Port Requirements for Communication</td>
<td>21</td>
</tr>
<tr>
<td>Port Requirements and Logical Traffic Flow for Replication</td>
<td>22</td>
</tr>
<tr>
<td>Unicast and Multicast Requirements</td>
<td>24</td>
</tr>
<tr>
<td>Datastore Access</td>
<td>24</td>
</tr>
<tr>
<td>Installation and ESX Best Practices and Security Considerations</td>
<td>24</td>
</tr>
<tr>
<td>Cisco HX Installer (HX Installer)</td>
<td>24</td>
</tr>
<tr>
<td>Default Passwords</td>
<td>25</td>
</tr>
<tr>
<td>VLANs and vSwitches</td>
<td>25</td>
</tr>
<tr>
<td>FI Traffic and Architecture</td>
<td>27</td>
</tr>
<tr>
<td>UCSM Requirements</td>
<td>27</td>
</tr>
<tr>
<td>VNICS</td>
<td>28</td>
</tr>
<tr>
<td>East-West Traffic</td>
<td>28</td>
</tr>
<tr>
<td>North-South Traffic</td>
<td>28</td>
</tr>
<tr>
<td>Upstream Switch</td>
<td>28</td>
</tr>
<tr>
<td>VLANs</td>
<td>28</td>
</tr>
<tr>
<td>Disjoint L2 Networks</td>
<td>28</td>
</tr>
<tr>
<td>Cisco HyperFlex Edge (HX Edge)</td>
<td>29</td>
</tr>
</tbody>
</table>

### HX Data Security

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Services</td>
<td>29</td>
</tr>
<tr>
<td>SEDs</td>
<td>30</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Key Management</td>
<td>31</td>
</tr>
<tr>
<td>Certificate Signing Requests (CSRs)</td>
<td>31</td>
</tr>
<tr>
<td>Networking Considerations</td>
<td>31</td>
</tr>
<tr>
<td>Encryption Partners</td>
<td>31</td>
</tr>
<tr>
<td>VM Level Encryption</td>
<td>32</td>
</tr>
<tr>
<td>Secure Communications</td>
<td>32</td>
</tr>
<tr>
<td>Usage of NFS in HXDP</td>
<td>32</td>
</tr>
<tr>
<td><strong>HX Management</strong></td>
<td>34</td>
</tr>
<tr>
<td>Management Interfaces</td>
<td>34</td>
</tr>
<tr>
<td>HX Connect</td>
<td>34</td>
</tr>
<tr>
<td>vCenter Plug-in</td>
<td>36</td>
</tr>
<tr>
<td>STCLI</td>
<td>37</td>
</tr>
<tr>
<td>REST APIs</td>
<td>38</td>
</tr>
<tr>
<td>AAA Domains</td>
<td>38</td>
</tr>
<tr>
<td>vCenter</td>
<td>39</td>
</tr>
<tr>
<td>AD Integration</td>
<td>39</td>
</tr>
<tr>
<td><strong>User Management</strong></td>
<td>39</td>
</tr>
<tr>
<td>Cisco HyperFlex User Overview</td>
<td>39</td>
</tr>
<tr>
<td>Local Users</td>
<td>41</td>
</tr>
<tr>
<td>UI Users</td>
<td>41</td>
</tr>
<tr>
<td>CLI Users</td>
<td>42</td>
</tr>
<tr>
<td>Auditing, Logging, Support Bundles</td>
<td>43</td>
</tr>
<tr>
<td>Setting Up Remote Logging for HXPrior to HXDP 4.0.1.a</td>
<td>46</td>
</tr>
<tr>
<td>Setting Up Remote Logging for HXDP 4.0.1.a and Later</td>
<td>46</td>
</tr>
<tr>
<td>Password Requirements</td>
<td>48</td>
</tr>
<tr>
<td>Password Guidelines</td>
<td>49</td>
</tr>
<tr>
<td>Session Timeouts</td>
<td>50</td>
</tr>
<tr>
<td><strong>HX Platform Hardening</strong></td>
<td>51</td>
</tr>
<tr>
<td>US Federal STIG (Secure Technical Implementation Guide) Settings</td>
<td>51</td>
</tr>
<tr>
<td>SSL Certificate Replacement</td>
<td>52</td>
</tr>
<tr>
<td>TLS Weak Cipher Disable</td>
<td>53</td>
</tr>
<tr>
<td>SSH (ESX) Lockdown Mode and Root Logins</td>
<td>53</td>
</tr>
<tr>
<td>Tech Support Mode</td>
<td>54</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Third Party Software Execution on FIs and HXDP</td>
<td>54</td>
</tr>
<tr>
<td>Whitelisting and other STCLI Security Commands</td>
<td>54</td>
</tr>
<tr>
<td>HX Data Platform Firewalling: IP Tables</td>
<td>55</td>
</tr>
<tr>
<td>Replication</td>
<td>57</td>
</tr>
<tr>
<td>Specific ESX Environment Hardening Settings Relevant to HXDP</td>
<td>57</td>
</tr>
<tr>
<td>Specific USC Environment Hardening Settings Relevant to HXDP</td>
<td>57</td>
</tr>
<tr>
<td>References</td>
<td>57</td>
</tr>
<tr>
<td>ESX Hardening Guide</td>
<td>57</td>
</tr>
<tr>
<td>UCS Hardening Guide</td>
<td>57</td>
</tr>
<tr>
<td>Cisco CSDL</td>
<td>57</td>
</tr>
<tr>
<td>Syslog-ng Configuration</td>
<td>57</td>
</tr>
<tr>
<td><strong>Appendix A: Networking Ports</strong></td>
<td>58</td>
</tr>
<tr>
<td><strong>Appendix B: URLs Needed for Smart Call Home, Post Install Scripts, Intersight</strong></td>
<td>62</td>
</tr>
<tr>
<td><strong>Appendix C: ESX Hardening Settings</strong></td>
<td>63</td>
</tr>
<tr>
<td><strong>Appendix D: Acronym Glossary</strong></td>
<td>72</td>
</tr>
<tr>
<td><strong>Appendix E: Sample Syslog-ng Configuration File</strong></td>
<td>73</td>
</tr>
</tbody>
</table>
Prerequisites
We recommend reviewing the release notes, installation guide, and user guide before proceeding with any configuration. The Cisco HyperFlex Data Platform (HXDP) should be installed and functioning per the installation guide. Please contact your Cisco Representative or Cisco Support if assistance is needed.

Introduction
The Cisco HyperFlex Data Platform Security Hardening Guide provides guidance for HyperFlex (HX) users in ensuring that their product is deployed in a more robust and secure manner. It is necessary to understand the architecture and components of the solution in order to complete this properly. This document provides recommended configuration settings and deployment architectures for HXDP-based solutions. It is intended to be used in conjunction with product documentation for deployments where extra consideration for platform security is required. For product documentation, please contact your Cisco representative.
Secure Product and Development Components

Cisco HyperFlex product components are developed, integrated, and tested using the Cisco Secure Development Lifecycle (CSDL). Secure product development and deployment has several components ranging from inherent design and development practices, testing the implementation, and finally a set of recommendations for deployments that maximize the security of the system.

Development Milestones

Each iteration of the product's development addresses needs for ongoing security fixes and general feature enhancements that include security components (new deployment models, changes in management, partner on-boarding, etc.). At every stage of development, the Hardening Guide undergoes potential enhancements relative to findings and new features.

- The HX Hardening Guide has the following components:
  1. VMware ESXi settings
  2. Cisco UCS settings
  3. HX Hardening
- The system is configured in QA to accommodate the relevant settings identified above and run through a typical deployment test.
- The result is a validated set of best practices for security and is communicated through the CSDL process and exposed in the Hardening Guide.

CSDL Philosophy

A poor product design can open the way to vulnerabilities. The CSDL is designed to mitigate these potential issues.

At Cisco, our "secure design" approach requires two types of considerations:

- Design with security in mind
- Use threat modeling to validate the design's security

Designing with security in mind is an ongoing commitment to personal and professional improvement through:

- Training
- Applying the Product Security Baseline (PSB) design principles
- Consider other industry-standard secure design principles
- Be aware of common attack methods and design safeguards against them
- Take full advantage of designs and libraries that are known to be highly secure
- Consider all entry points

We also reduce design-based vulnerabilities by considering known threats and attacks. With threat modeling, we:

- Follow the flow of data through the system.
- Identify trust boundaries where data may be compromised.
- Based on the data flow diagram, generate a list of threats and mitigations from a database of known threats, tailored by product type.
- Prioritize and implement mitigations to the identified threats.

The goal of this effort is to ensure a security mind set at every stage of development:

- Secure Design
Secure Coding
Secure Analysis
Vulnerability Testing
Secure deployments

HX product development focuses on two areas to satisfy the CSDL model:
• Internal Requirements
  • Adhere to the secure development process
• Market based requirements
  • Complete and validate against certifications (Federal)
  • Document and educate (HX Hardening Guide)

CSDL Product Adherence Methodologies
Cisco CSDL adheres to Cisco Product Development Methodology (PDM), ISO27034 and ISO9000 compliance requirements. ISO 27034 standard provides an internationally-recognized standard for application security. Details for ISO 27034 can be found here. The ISO 9000 family of quality management systems standards is designed to help organizations ensure that they meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements related to a product or service. ISO 9000 details are here.

The CSDL process is not a one-time approach to product development. It is recursive, with vulnerability testing, penetration testing, and threat modelling plugging into subsequent development that feeds back into the process. This process follows ISO9000 and ISO27034 standards as part of an internationally recognized set of guidelines. The approaches involved often take a solution-wide methodology. For example, the use of our continually updated CiscoSSL crypto module to guarantee that HX (along with other elements in the Cisco offering) are always secure and meet FIPS certification requirements.

Vulnerability Handling

Tenable IO Scanning
Common Vulnerabilities and Exposures (CVE) scanning is a critical part of most deployments. Many industries and Federal organizations standardize on Tenable IO (formerly Nessus Scanner) to implement various DISA or CIS audits.

• CIS is Center for Internet Security
• DISA is Defense Information Systems Agency

In our CSDL efforts, we use Tenable IO, produced by Tenable, in our development process
• Tenable IO Scanner – https://www.tenable.com/products/tenable-io

The vulnerability scanning workflow is as follows:
• Choose a build to test against (based on dot release development timing)
• Update the scanner signatures and plug-ins for our test date
• Freeze the scanner – line in the sand
• Test → Report → Fix as needed → Rescan → check-in the safe build
• Fixes are immediately scheduled for Critical and High
• CSDL may identify others in Medium and Low and Info that need remediation.

A typical Nessus scan configuration summary might look like this:
• HX 3.0(1b)
• Compliance checks:
  • DISA RHEL 5
  • CIS L2 Ubuntu 16.04 LTS
  • CIS Apache 2.2
• Plug-ins:
  • All plug-ins enabled, same day update
• Sample Report:
  • Output is color coded.
  • 5 Alert Levels: Critical, High, Medium, Low, Info.
  • Notes: System is clean, one low warning, rest are info only.

---

CERT Advisory
Computer Emergency Response Team (CERT) advisories come up as new vulnerabilities are identified. Cisco’s internal CERT team monitors and alerts product groups to potential issues that might affect their respective components. When these items are identified by CERT or are otherwise indicated by vendor partners (VMware, etc.). Patches are either developed or acquired from the respective vendors.

VMware ESX Patching
Patches for VMware are immediately supported if they are within the regularly supported VMware dot release. There are no hard commitments for when support for new VMware dot releases will be available, but there are continuous release onboarding processes that occur within QA for each new VMware release.
HXDP Patching
We begin developing the patch for critical CVEs related directly to HX as soon as they are discovered. The fixes are rolled into an immediate release or a regularly scheduled incremental with turnaround within 90 days, depending on severity.

They HyperFlex release model identifies Long Term Support releases and Feature Releases. Long Term Support releases are supported, maintained and patched for 30 months from initial release.

Additional Vulnerability Testing Measures
Cisco also utilizes an internal tool for threat modeling called ThreatBuilder (v2.1). This tool is used to explicitly map out application components and services and to identify potential attack surfaces and develop line items for direct evaluation. This information along with industry tools are used for vulnerability and exploit testing by Cisco’s ASIG (Advanced Security Initiatives Group). ASIG also uses fuzzing and manual testing as part of their suite of tools.

Secure Platform “Modules”

At a high level, HX system security can be broken down into 3 broad categories. These are the Control Plane, Data Security and Management Security.

Control Plane
The control plane deals with system communication. This is the subsystem that implements FIPS compliant encrypted communication protocol engine for communication that may originate outside of the system, for example, from an administrator. It also deals with inter-component communication between nodes which happens on a trusted, internal, non-routed 10GB network.

Data Security
Securing data in the system is the job of the Secure Encrypted Disk (SED) subsystem. The HX nodes are SED capable, meaning that they can incorporate and function using encrypted disks. Key management for this can be handled locally or via remote KMIP servers in HA configurations.

Management Security
Managing the system through the UI or through the command line requires secure communication mechanisms. This is handled via HTTPS for the vCenter plug-in or for HX Connect (the native HTML 5 UI). SSH for encrypted command line access is also handled. Management security also entails role-based access control as well as auditing and logging of system activities and user input.

Certification Process
Federal compliance and audit-based certifications are a critical component of a standardized and predictable security posture. They are critical in most Federal deployments, especially those dealing with financial and defense arenas. The Cisco Global Certification Team (GCT) works to complete various certifications.

ACVP
The Automated Cryptographic Validation Protocol (ACVP) is part of a NIST program to automate FIPS and Common Criteria testing superseding the process used in the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP). Details can be found here:

https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing
Beginning in CY2020, Cisco will be using ACVP built into the CiscoSSL module for HyperFlex in order to process Federally accepted cryptographic certifications. The process will use a series of ACVP/NIST proxy infrastructure servers to complete the certifications using communication directly to NIST validation servers. The figure below shows the general product architecture used for ACVP.

**Current Certifications**

**FIPS** -- The Federal Information Processing Standard (FIPS) Publication 140-2, is a U.S. government computer security standard used to approve cryptographic modules.

HyperFlex is compliant with FIPS140-2 level 1 via direct implementation of the FIPS compliant CiscoSSL crypto module. The module, once implemented, is vetted by a 3rd party that is federally certified to ascertain compliance status.

- Utilizes CiscoSSL module
  - Already FIPS compliant
  - SSH approved cipher list
  - SSL/TLS implementation
  - Eliminates weak or compromised components
    - Regularly updated
- Lab validates that the module is incorporated correctly
  - Build logs
  - Source access identifying calls to the module
- All admin access points to the cluster are covered here
  - SSH for CLI
  - HTTPS for UI

A comprehensive list of Cisco FIPS compliant products is listed here along with the corresponding reference with NIST.
- Cryptographic Module Validation Program (CMVP) vendor list: [http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)

---

**Common Criteria** for Information Technology Security Evaluation (Common Criteria or CC) is an International standard (ISO/IEC 15408) for computer security certification, currently in v3.1 rev 4.

- System users specify their security functional and assurance requirements through the use of protection profiles, vendors can then make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.
  - Customers have some security needs defined in a set of CC guidelines
  - This is my system, this is what I say it can do to meet those
  - Let’s (vendor and lab) agree on a test, here’s the procedure
  - Here’s my results
  - You (lab) run it on your own and verify
  - Deliver certification

This certification was completed in CYQ4 2017 for EAL2 and is currently available here:

It is currently posted on the Norwegian Common Criteria scheme page here: [http://sertit.no/product/95](http://sertit.no/product/95)
It is also posted at the Common Criteria site: http://www.commoncriteriaportal.org/products/

Completion of Common Criteria for 3.5.2(x) will be available in October 2019. The 3.5 code line is a "long term support" release in the HX release model and will be available, maintained and patched for 30 months from initial release.

**Other Certifications and Procedural Guidelines**

**ISO 27001**
ISO 27001 isn’t a certification for specific pieces of hardware as much as a dozen or so “Best Practices” in the form of checklists/guidelines for how organizations manage their security controls internally. It observes things like Building Access, Password Management, Badging into a Copier to make copies, etc. Training on a frequent basis is a part of the standard.

Cisco is ISO 27001 certified. This is a link to our ISO 27001 certificate: https://www.cisco.com/c/en/us/about/approach-quality/iso-27001.html

**FISMA** (Federal Information Security Management Act) Cisco HyperFlex has not participated in a FISMA audit to date. For FISMA, Federal information systems must meet the minimum-security requirements. These requirements are defined in the second mandatory security standard required by the FISMA legislation, FIPS 200 “Minimum Security Requirements for Federal Information and Information Systems”. Organizations must meet the minimum security requirements by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems”.

**FedRAMP** (Federal Risk and Authorization Management Program) Cisco HyperFlex is not FEDRAMP authorized for cloud based security because Cisco is not a public cloud provider. For FEDRAMP in particular, the onus will fall on the cloud provider (Google/Azure/AWS etc.) unless you mean to include private cloud in a FEDRAMP assessment or authorization. If this is the case, then the private cloud will need to meet the FedRAMP standards and a POC is recommended.

**IAVA** (Information Assurance Vulnerability Alert) patches are routine alerts. They are part of the IAVM (Information Assurance Vulnerability Management) Program and detail vulnerability fixes that are deemed critical for all systems in an environment by the DoD from the DoD CERT list. If a vulnerability is on IAVA’s list, it will get sent to the admins that are signed up by an organization to receive them and they must be fixed to remain in compliance. Tenable IO (see the Vulnerability Scanning section) scans will pick these up and, based on severity, will be remedied in patch releases.

**HIPAA** (Health Insurance Portability and Accountability Act) requires healthcare organizations use data encryption technology to protect sensitive patient information. However, the law does not specify which types of encryption to use in order to accomplish this task. Key management mechanisms are not specifically called out either. In these respects, HXDP satisfies the HIPAA requirements. HXDP, however, is not officially certified with HIPPA because a fully compliant solution includes all elements of the ecosystem. HXDP would qualify as a compliant component.

**NERC CIP** (North American Electric Reliability Corporation Critical Infrastructure Protection) is centered on the physical security and cybersecurity of assets deemed to be critical to the electricity infrastructure. There are currently 11 CIP standards subject to enforcement, governing topics from system security management to recovery plans. NERC CIP compliance is more about policy and procedure than technology, and the responsibility of compliance is on the utility company not the technology provider. So, there’s isn’t an “FERC/NERC compliant HCI”, per se. The idea is identifying capabilities that helps the customer facilitate compliance, and there are multiple HX security features, system configurations and hardening, as well as continuous security monitoring and advisories that are pertinent toward that goal.
A couple of examples (note: not exhaustive):

- **CIP-007-6 R1 – Ports and Services**
  - Requirement: CIP-007-6 Part 1.1 requires to enable only logical network accessible ports that have been determined to be needed by the Responsible Entity.
  - Mitigations: The HX Data Platform Hardening Guide provides guidance on port requirements, STCLI security commands for whitelisting, setting up IPtables on HX nodes to secure network traffic, etc.

- **CIP-007-6 R2 – Security Patch Management**
  - Requirement: CIP-007-6 Part 2.1 requires a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets.
  - Requirement: CIP-007-6 Part 2.2 requires, at least once every 35 calendar days, to evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.
  - Mitigations: proactive PSIRT advisories publish guidance on current security vulnerabilities and mitigations that impact HX

- **CIP-007-6 R4 – Security Event Monitoring**
  - Requirement: CIP-007-6 Part 4.1 requires logging events for identification and investigation of cybersecurity incidents that includes minimally: detected successful logins, detected failed access and login attempts, detected malicious code
  - Mitigations: centralized audit logging in HXDP, position Next Gen Firewall for threat protection

The idea here is a comprehensive audit record and well-defined RBAC roles and division of user duties. Continuous monitoring would be a solution type of responsibility that would be handled with ecosystem components like Tetration and Splunk (analysis of syslog). Here is the overview of NERC information system compliance:

> Energy producers and distributors that make up the bulk electric system for North America have multiple IT security and compliance challenges, which range from protecting consumers' payment card data and complying with the Payment Card Industry Data Security Standard, to adhering to the general internal audit control and disclosure requirements under Sarbanes-Oxley. In addition, utilities and firms that fall under the authority of the Federal Energy Regulatory Commission (FERC) must meet the cyber security standards of the FERC's certified Electric Reliability Operator (ERO), the North American Electric Reliability Corporation (NERC).

> Just as physical surveillance tools such as video cameras are a critical part of physical security controls under NERC, the core technical requirements for cyber security as outlined in NERC CIP Standards 002-009 and other associated guidance from NERC require accountability throughout the authentication, access control, delegation, separation of duties, continuous monitoring and reporting of electronic access to critical infrastructure. And specific requirements from NERC CIP 005, 004, 007 and 008 taken together establish a clear obligation that all electronic access be audited, monitored and archived in such a way that an organization can reproduce detailed privileged user sessions 24 hours per day, 7 days per week. This continuous monitoring requirement would be difficult to achieve with a combination of manual processes and system-level logs, which often do not tie actions to a unique identity.

Additional specific details are available from NERC itself:

https://www.nerc.com/pa/comp/Pages/default.aspx

https://www.nerc.com/pa/comp/guidance/Pages/default.aspx

**CNSA** (Commercial National Security Algorithm) is a schema that is called out by the NSA via this IETF memo:
It describes which algorithms should be in use and what their profiles should look like. It is intended to give guidance for secure and interoperable communications for national security reasons:

“This document specifies a profile of the Certificate Management over CMS (CMC) protocol for managing X.509 public key certificates in applications using the CNSA Suite.”

Cisco supports both elliptic cryptographic certificates (ECC) and RSA certificates so this requirement is met:

“Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH) key pairs are on the curve P-384. FIPS 186-4 [DSS], Appendix B.4, provides useful guidance for elliptic curve key pair generation that SHOULD be followed by systems that conform to this document. RSA key pairs (public, private) are identified by the modulus size expressed in bits; RSA-3072 and RSA-4096 are computed using moduli of 3072 bits and 4096 bits, respectively.”

HyperFlex’s FIPS certification via CiscoSSL implements Federally approved crypto modules to satisfy the complexity requirements as well. The fact sheet here lists the approved algorithms:

CNSA compliance is just a matter of making sure to implement a cryptographic ecosystem according to the CNSA requirements since HX support all the documented methods.

Targeted Certifications

Future targeted certification are always under evaluation with the Global Certification Team. We are planning to re-certify HX with Common Criteria in the HX 3.5 release time frame.

HX Components and Environment

This section details the different components in a typical HX deployment. It is critical to the secure environment that the various parts are hardened as needed.

Solution Components

An HX deployment consists of HX nodes on UCS connected to each other and the upstream switch via a pair of Fabric Interconnects (FIs). There may be one or more cluster and clusters can share the same FIs or be connected to their own, independent set. Clusters can be paired and use HXNR (Native Replication) for protection of VMs. Intervening optimizations appliances may also be deployed to aid with (or monitor or shape) cluster to cluster traffic. The following illustration shows a typical physical layout for this kind of deployment.
 Cisco HX Platform Hardening Guide

Cisco UCS

The physical HX node is deployed on a Cisco UCS 220 or 240 platform in either a hybrid or all flash configuration. A service profile is a software definition of a server and its LAN and SAN network connectivity, in other words, a service profile defines a single server and its storage and networking characteristics. Service profiles are stored in the Cisco 6248/6296 and 6332/6332-16UP Series Fabric Interconnects and are managed via specific versions of UCSM (the...
web interface for the FI) or via purpose written software using the API. When a service profile is deployed to a server, UCS Manager automatically configures the server, adapters, fabric extenders, and fabric interconnects to match the configuration specified in the service profile. This automation of device configuration reduces the number of manual steps required to configure servers, network interface cards (NICs), host bus adapters (HBAs), and LAN and SAN switches.

The service profile for the HX nodes is created during cluster build at install time and is applied to the appropriate devices attached to the FI (identified by PID and associated hardware). These profiles should have their own, easily identifiable name and should not be edited after creation. They are preconfigured by the HX Installer with the settings required for HX to operate securely and efficiently (VLANs, MAC pools, management IPs, QoS profiles, etc.).

It is also worth noting that some larger UCS customer use custom MAC pool and UUID schema for all UCS domain deployments in the data center. Cisco does not support custom naming schemes. HX is an appliance, and to ensure consistent quality, user experience, and full TAC supportability these mundane details have been automated. For UUID, HXDP leverages the hardware derived UUID. For MAC, HXDP has a specific enumeration that cannot be changed.

**Cisco UCS Fabric Interconnects (FIs)**

Cisco UCS FIs are a networking switch or head unit to which the UCS chassis connects. Fabric Interconnects are a core part of Cisco’s Unified Computing System, which is designed to improve scalability and reduce the total cost of ownership of data centers by integrating all components into a single platform, which acts as a single unit. Access to networks and storage is then provided through the UCS fabric interconnect. Each HX node is dual connected, one SFP port to each FI for HA. This ensures that all vNICs on the UCS are dual connected as well, guaranteeing node availability. vNIC configuration is automated during HX installation and should not be altered.

**HX Nodes**

The HX node itself is composed of the software components required to create the storage infrastructure for the system’s hypervisor. This is done via the HX Data Platform (HXDP) that is deployed at installation on the node. The HX Data Platform utilizes PCI pass-through which removes storage (hardware) operations from the hypervisor making the system highly performant. The HX nodes use special plug-ins for VMware called VIBs that are used for redirection of NFS datastore traffic to the correct distributed resource, and for hardware offload of complex operations like snapshots and cloning.

The following illustration shows a typical HX node architecture.
These nodes are incorporated into a distributed cluster as shown below.

Each node contains the following VMNIC and vSwitch architecture for versions prior to HXDP 3.5.x:
For HXDP versions 3.5.x and above, the VMNIC ordering has been changed to the following:

Management Interfaces: HX Connect and the VMware vCenter Plug-in
HX Connect is the native HTML 5.0 UI for the cluster. The HX vCenter plug-in is another management interface available in vCenter once the cluster is deployed. These are separate interfaces. Both are accessed via HTTPS in a web browser and are subject to the same user management (including RBAC) that is available for the CLI or the API.
VMware vCenter
The Cisco HX Data Platform requires VMware vCenter to be deployed to manage certain aspects of cluster creation such as ESX clustering for HA and DRS, VM deployment, user authentication and various datastore operations. The HX vCenter plug-in is a management utility that integrates seamlessly within vCenter and allows comprehensive administration, management, and reporting of the cluster.

It is important to note that all compute and converged nodes must share a single vCenter cluster object for a given cluster. This 1:1 mapping is a requirement today.

Administrator users created in the vCenter can login to the Storage Controller VM CLI using the full name in the following format: <user>@vsphere.local/password. However, read-only users created in the vCenter cannot login to the Storage Controller VM CLI.

VMware ESX
ESX is the hypervisor component in the solution. It abstracts node compute and memory hardware for the guest VMs. HXDP integrates closely with ESX to facilitate network and storage virtualization.

VMs
The HX environment provides storage for the guest VMs deployed in ESX using VLAN segmented networking. The VMs are available for external resources, typical of any elastic infrastructure deployment.

Client Machines
Client machines are defined here as external hosts that need to access resources deployed in HX. These can be anything from end users to other servers in a distributed application architecture. These clients access from external networks and are always isolated from any HX internal traffic by network segmentation, firewalling and whitelisting rules.

HX Secure Network Environment and Component Requirements
The HX networking environment is segmented and isolated to provide out-of-the-box traffic security. This section identifies the networking communication (port) requirements and offers best practices for the Installer along with information regarding FI traffic and ESX networking (vSwitches).

Port Requirements for Communication
The diagram and table below indicate the various components, networking ports, and communication direction for HX.
See Appendix A for a comprehensive table on the port requirements.

Port Requirements and Logical Traffic Flow for Replication

The following ports are opened for inter-cluster communications, during cluster-pairing: 9338, 3049, 9098, 4049, 4059, 8889

These are the ports that are used in HX Replication:

- datasvcmgr_peer = 9338
- scvm (Storage Controller VM) = 3049
- cmap = 4049
- nrnfs = 4059
- replsvc = 9098
• nr (master for coordination) = 8889

Firewall entries are made on the source and destination machine during pairing to allow HX Data Platform access to the system(s) bi-directionally. This traffic needs to be allowed on WAN routers for each HXDP node IP address and cluster CIP-M address.

The following illustration shows the logical traffic flow for replication:

![Diagram showing logical traffic flow for replication]
Unicast and Multicast Requirements

Starting with version 3.0(1a), HXDP no longer uses the UCARP protocol and is 100% unicast traffic moving forward.

For previous versions that did use UCARP, since the well-known multicast address of 224.0.0.18 was used, there is no configuration needed on the switches to be able to support HX. This UCARP protocol falls under the IPv4 multicast link-local scope of 224.0.0.0/24. Link scoped multicast packets are flooded throughout the VLAN and IGMP snooping does not take effect on these multicast groups. Hence there is a very small amount of “management multicast” in use, but nothing that requires any network changes or specific infrastructure to support it.

Datastore Access

Access to the HX datastores by client machines is restricted to mounting by HX nodes only. This access is automatically granted during cluster install when the component nodes are identified. Access is also granted or revoked during expansion or removal respectively, when nodes are added or removed from the system. Access to the datastores for migration or backup purposes may be granted via the command line using the STCLI whitelist command. HX nodes are not listed in the whitelist list because this is a manual, administrative setting for external machine access only. It should only be used during VM ingress/egress from the system as required and the list should be immediately purged once operations are complete.

The mount syntax needs to look like the following in order to work (mount ip:ip:/<datastore> <local dir>/) where the IP is the CIP (not the CIP-M). Here it is in action once the mounting host has been added to the whitelist:

```
kaptain@kaptain-vm:~/temp$ sudo mount 10.a.b.c:10.a.b.c:/ds01 mountpoint/
kaptain@kaptain-vm:~/temp$ su
Password:
root@kaptain-vm:/home/kaptain/temp# cd mountpoint/
root@kaptain-vm:/home/kaptain/temp/mountpoint# ls
auth.log  rhttpproxy.4.gz  vmkernel.4.gz  vprobed.log
clomd.log  rhttpproxy.5.gz  vmkernel.5.gz  vprobe.log
```

Installation and ESX Best Practices and Security Considerations

Before conducting any installation, review and complete the pre-installation checklist maintained here:


Cisco HX Installer (HX Installer)

During initial configuration, the cluster is installed on site using the HX installer. This installer can safely be removed from the environment immediately after cluster creation. It is typical for secure environments to isolate the deployment network during installation. In this scenario, the installer is never externally available during configuration. Since it is removed post deployment, installer threat exposure is minimized.

The following services in vSphere must be enabled after you create the HX Storage Cluster in vCenter:

- DRS
- vMotion
- High Availability

The installer verifies that the cluster components are correct and available as needed. This ensures that the deployment has no gaps that could jeopardize security.

- Ensure firmware and BOM compliance
- Deploy and cluster create (requires UCSM credentials for SED)
  - All nodes should be SED capable—no mixing of SED & non-SED drives
- Server Selection to shows for SED Capable nodes and validates non-SED node configurations
- Creates Service profiles
  - VLANS
  - IP addressing
  - VNIC ordering
  - QoS configuration
  - MAC pools
- Creates ESX vSwitches with appropriate VLANS and address spaces
- Deploys HX Data Platform
- Deploys ESX Plug-ins
- Configures and starts the storage cluster.
- Sets default passwords and generates node-node communication secure certificates

Hard passwords are enforced on HX UI interfaces and HX Data Platform settings during install.

**Default Passwords**

Once the deployment using the installer is complete, make sure that any default passwords are changed or updated. The ESX hypervisor default password is Cisco123. There is no default set for the HXDP nodes since a hard password is enforced at install. Log in to each ESX node via CLI and update the root password as needed using `passwd` root.

**VLANs and vSwitches**

VLANs are created for each type of traffic and for each vSwitch. There are typically 4 vSwitches created during the install with associated VLANS for each. The vSwitches are for ESX management, HX management, ESX Data (vMotion), and HX Data (storage traffic between nodes for the datastores). HX Data Platform Installer creates the vSwitches automatically.

The zones that these switches handle are described below:

- **Management Zone**: This zone comprises the connections needed to manage the physical hardware, the hypervisor hosts, and the storage platform controller virtual machines (HXDP). These interfaces and IP addresses need to be available to staff responsible in administering the HX system, throughout the LAN/WAN. This zone must provide access to Domain Name System (DNS) and Network Time Protocol (NTP) services, and allow Secure Shell (SSH) communication. The VLAN used for management traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching both the Primary Fabric Interconnect (FI-A) and Subordinate Fabric Interconnect (FI-B). In this zone are multiple physical and virtual components:
  - Fabric Interconnect management ports.
  - Cisco UCS external management interfaces used by the servers and blades, which answer via the FI management ports.
  - ESXi host management interfaces.
  - Storage Controller VM management interfaces.
  - A roaming HX cluster management interface.
• **VM Zone:** This zone comprises the connections needed to service network IO to the guest VMs that will run inside the HyperFlex hyperconverged system. This zone typically contains multiple VLANs that are trunked to the Cisco UCS Fabric Interconnects via the network uplinks and tagged with 802.1Q VLAN IDs. These interfaces and IP addresses need to be available to all staff and other computer endpoints which need to communicate with the guest VMs in the HX system, throughout the LAN/WAN.

• **Storage Zone:** This zone comprises the connections used by the Cisco HX Data Platform software, ESXi hosts, and the storage controller VMs to service the HX Distributed File system. These interfaces and IP addresses need to be able to communicate with each other at all times for proper operation. During normal operation, this traffic all occurs within the Cisco UCS domain, however there are hardware failure scenarios where this traffic would need to traverse the network northbound of the Cisco UCS domain. For that reason, the VLAN used for HX storage traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI-A from FI-B, and vice-versa. This zone is primarily jumbo frame traffic therefore jumbo frames must be enabled on the Cisco UCS uplinks. In this zone are multiple components:
  - A vmkernel interface on each ESXi host in the HX cluster, used for storage traffic.
  - Storage Controller VM storage interfaces.
  - A roaming HX cluster storage interface.

• **vMotion Zone:** This zone comprises the connections used by the ESXi hosts to enable vMotion of the guest VMs from host to host. During normal operation, this traffic all occurs within the Cisco UCS domain, however there are hardware failure scenarios where this traffic would need to traverse the network northbound of the Cisco UCS domain. For that reason, the VLAN used for HX storage traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI-A from FI-B, and vice-versa.

These vSwitches and their associated port groups are tied to a pair of VNICS on each node in an active/standby mode for HA. They typical networking configuration is shown below:
For an in-depth discussion of Virtual Distributed Switches (VDS) with HX, see the following resource:


The question often arises, “In a multi-cluster setup, does each HX cluster need to have separate VLAN/Subnets for the storage management and storage data interfaces?” In other words, would there be issues if the same VLAN/subnet is used for each cluster for storage management and storage data interfaces on the controller VM? It is recommend that a unique data VLAN per cluster is used as a best practice. This ensures data is secured within the cluster and there isn’t contention or broadcast traffic from other clusters on the same network.

However, this isn’t a hard requirement and it is possible to put multiple clusters on the same storage VLAN, but you risk performance issues in heavily loaded environments. It is worth noting that for deployments using releases prior to HXDP 3.0, clusters require that the cluster management IP (CIP) have a unique IP in the last octet. For example, if you have a /16 subnet, don’t use 172.16.100.10 and 172.16.101.10 as two cluster management IPs within the same VLAN. The installer has a check to detect this, but you should avoid this situation altogether.

**FI Traffic and Architecture**
Traffic through the FIs comes in two general flavors. Intra-cluster traffic (between nodes), and extra-cluster traffic (client machine or replication related). All of the FI configurations are managed, accessed, and modified through Cisco UCS Manager (UCSM).

**UCSM Requirements**
UCSM is the interface used to set up the FIs for Cisco UCS Service Profiles and for general hardware management. During installation, the HX Installer verifies that the appropriate UCSM build is in place for HX and that the hardware is running a supported firmware version. You are given the option to upgrade these at installation if needed.
Cisco recommends disabling Serial over LAN (SoL) once the deployment is complete since it is no longer needed for ESX configuration. It is also recommended to change any default or simple passwords that were used. Be aware that if you disable SoL, cluster expansion will fail during the Hypervisor Configuration step. You will need to re-enable before continuing.

VNICs
For an in-depth discussion of vNIC see the following:

The VNICs for each vSwitch are in a predefined order and should not be altered in UCSM or ESX. Any changes to these (including active/standby status) could affect HX functionality.

East-West Traffic
East-West traffic on the FI is networking traffic that goes between HX nodes. This traffic is local to the system and does not travel out of the FI to the upstream switch. This has the advantage of being extremely fast by virtue of its low latency, low hop count, and high bandwidth. It also means that this traffic is not subject to external inspection since it never leaves the local system.

North-South Traffic
North-South traffic on the FI is networking traffic that goes outside the FI to an upstream switch and/or router. North-South traffic occurs during external client machine access to HX hosted VMs or for HX access to external services (NTP, vCenter, SNMP etc.). This traffic may be subject to VLAN settings upstream.

Upstream Switch
Configure the upstream switches to accommodate non-native VLANs. HX Installer sets the VLANs as non-native by default.

VLANs
Use a separate subnet and VLANs for each of the networks.

Do not use VLAN 1, the default VLAN, because it can cause networking issues, especially if Disjoint Layer 2 configuration is used. Use a different VLAN.

Disjoint L2 Networks
Please make sure to read and understand the following disjoint layer two document if this is a requirement in your environment:


You can just add new vNICs for your use case. We support the manual addition of vNICs and vHBAs to the configuration. Please see the HX VSI CVD:
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/HX171_VSI_ESXi6U2.html for step by step instructions on how to do this safely. Follow the same procedures outlined in the CVD. Please do not use pin groups, as
it may not properly prune the traffic and can cause connectivity issues as the designated receiver may not be set correctly.

**Cisco HyperFlex Edge (HX Edge)**
Typical HX Edge deployments use a trunk port configuration on the top of rack switch(es). VLAN trunking should limit the allowed VLANs to those required for the HyperFlex services and user VMs. By default, the switches will allow all VLANs to pass and could pose a security risk of allowing unfettered network access. See the Cisco HyperFlex Edge Deployment Guide for sample configurations that use "switchport trunk allowed VLAN" commands.

For HX Edge configurations with the add-in PCIe Quad port NIC, ensure any unused Ethernet ports remain disconnected from any virtual switches in ESXi. This will prevent unauthorized access to the virtual switching environment.

SED deployments are currently not supported with HyperFlex Edge. VM encryption by virtue of 3rd party encryption clients will work to encrypt the VMs deployed on Edge. Vormetric and Gemalto Safenet provide such clients. VMware vSphere 6.5 also incorporates a VM encryption capability that should work but has not yet been officially qualified.

**HX Data Security**
HX data-at-rest security is accomplished via Secure Encrypted Disks (SEDs) and is managed by Cisco HX Connect in conjunction with UCSM and local or remote key stores using the Key Management Interoperability Protocol v1.1. The Encryption FAQ contains a comprehensive treatment of the subject with respect to HX:


**Encryption Services**
An encrypted cluster is created at build time. It currently cannot be converted after the fact. The components for an encrypted cluster consist of the SED capable HX nodes with UCSM and the Key Management Infrastructure.

- Data is only as secure as the encryption keys.
- Key management is the tasks involved with protecting, storing, backing up and organizing keys.
Specialized vendors provide enterprise key management offerings.

SEDs

SEDs provide native data-at-rest encryption, typically using AES 256. All qualified disks are FIPS 140-2 Level 2 validated components for data-at-rest encryption. The hardware encryption is built-in, thereby incurring no deployment overhead. The performance is comparable non-SED system and is transparent to data optimization functions (dedupe, compression).

Several encryption keys are associated with a SED implementation:

- Media Encryption Key – data is always stored in encrypted form
- Key Encryption Key secures the media encryption key

SEDs provide a mechanism for secure erase ensuring security during decommission:

Secure cluster Expansion

- Only SED capable node can be added to HX Cluster with SEDs
- Local key – seamless secure expansion
- Remote key – secure expansion requires lockstep with certificates/key management
- Certificates required to add new node securely
- Deployment will show warning and include steps to proceed and link to UI for certificate download
- User follows steps to upload certificate(s) and continue the deployment

SED on HX Edge is not currently supported (see the HX Edge section above).

HXDP 3.0 release introduced support for Microsoft Hyper-V as a cluster hypervisor. SEDs are currently not supported with Hyper-V.

Can access to the SEDs via the CVM be an attack vector if the CVM is compromised? In other words, since the control VM has direct ownership over the HX node disks (through VMDirectPath IO), and since the drives are self-encrypting, does this mean you effectively have unencrypted raw access to the disks through that login? Technically you can access data directly from the root shell, however, you would not be able to do much with this access. Since data is striped per disk, per node, and across file tree vnodes even, you would not be able to reconstruct the data into anything meaningful. You would only have small bits of information in various disks on various nodes. If this is still a concern, you can certainly encrypt via software (see Encryption Partners below) at the VM level, thereby mitigating any fractional data reads from even a compromised CVM.

The ESXi boot volume is not encrypted and there is not an option to encrypt this drive. There is no user data stored on this device. Theft of or raw access to this drive would only expose the ESXi operating system. The CVM root drive is separate from the data drives. The HX system/log drive is not encrypted and there is not an option to encrypt this drive. There is no user data stored on this drive. Theft of or raw access to this drive would only expose time stamps and block locations of the cache and capacity drives, both of which are encrypted.
Key Management
Configuring encryption services supports both local and remote key configurations. If you are not using local keys then you need to configure a KMIP server. KMIP server key handling is performed via encryption partners (Thales Vormetric and Gemalto Safenet). The server specifics are entered using the Encryption workflow in HX Connect.

Key Management best practices:
- Always deploy at least two KMIP servers, clustered for high-availability
- No agents or software to deploy for key management
- Configure key backup and recovery
- Self-signed and CA signed certificates can be used

Workflows supported:
- Disable/Enable
- Re-key
- Secure Erase

Certificate Signing Requests (CSRs)
A component of the remote encryption workflow generates CSRs. CSRs need to be downloaded and signed. Signing can be "self" which refers to signing the CSR with a key you have generated yourself and installed on your KMIP infrastructure. If you are using a Certificate Authority (CA) then you will need to get the CSRs signed with your validated key from the CA.

HyperFlex supports RSA certificates and, by virtue of use of the CiscoSSL module, also supports ECC (Elliptic Curve Cryptography) certificates. RSA is currently the industry standard for public-key cryptography and is used by most SSL/TLS certificates.

A popular alternative first proposed in 1985, is Elliptic Curve Cryptography using a different formulaic approach to encryption. While RSA is based on the difficulty of factoring large integers, ECC relies on discovering the discrete logarithm of a random elliptic curve.

Networking Considerations
When using a KMS (Key Management Server) for remote key management, some additional networking ports may need to be opened. Port 443 is required for policy configuration between the control VMs and UCSM. Additionally, port 5696 is required for TLS communication between the CMIC of each node and the KMS server itself for secure information exchange. See Appendix A.

Encryption Partners
Cisco HX partners with two industry-leading encryption and KMIP service providers.

Gemalto Safenet:
- Enterprise Key Management (EKM) solution
- Single, centralized platform for managing cryptographic keys and applications
- Simultaneously manage multiple, disparate encryption appliances and associated keys through a single, centralized key management platform
- Also provides a high performance encrypt/decrypt engine when combined with SafeNet's Data Protection portfolio

Thales Vormetric:
• Data Security Manager solution
• Single, centralized platform for managing cryptographic keys and applications
• Simultaneously manage multiple, disparate encryption appliances and associated keys through a single, centralized key management platform.
• Also, provides a transparent encryption client for guest VMs.

Note: KMIP 1.1 compliant key managers should work but require qualification.

Two Versions of Vormetric Data Security Manager

VM Level Encryption
VM software encryption works above the HXDP storage layer. Encryption at a VM level of granularity is available with our partner solutions. Note that you can expect there will no longer be any deduplication space savings, since encryption at this level necessarily “makes unique” all data sent to the storage subsystem.

Vormetric Transparent Client

Gemalto:

ESX 6.5 VM encryption:

Secure Communications

All communication occurring with the HX platform management interfaces is FIPS compliant using SSH or HTTPS. See the section on Management Security above.

Usage of NFS in HXDP

The HX Data Platform uses a proprietary variant of NFSv3 to present an HX controlled files system to the hypervisor using a plugin called IOvisor. Each node runs an IOvisor instance in order to properly allocate the correct read and write resources in the distributed architecture. This communication path is completely internal, and available only between the hypervisor and the HX CVM present in each node that manages access to the underlying distributed storage. All other components in the system are disallowed from mounting the resource presented by the IOvisor.
Each CVM physically controls the underlying storage hardware and participates in allocating this resource to the
distributed file system within which the datastores are created. The diagram below describes the logical placement of the
HX IOvisor within the node architecture.

Inside HX Data Platform Node

VM IO is destined for the configured datastore, which is an abstracted container for the storage subsystem. This container
is an NFS datastore created on the HX platform. The VMware storage stack utilizes an NFSv3 client to mount the
datastore, presented up from the IOvisor.

The IOvisor, sometimes referred to as the SCVM client, lives as a process in user space inside ESXi and can be thought
of as a simple NFS proxy. It behaves as a server for the VMware NFS client, while looking like a client to the controller
VMs.

The IOvisor is very thin code, on the order of 2000 lines of code. It is designed to be a stateless router for IO and has a
very small footprint. It is installed into ESXi as a VMware installation bundle (VIB) that is auto-deployed during cluster
installation. As such, it is set up to only allow mounts from cluster nodes. This allowed mapping is only updated during
node failure or expansion events.

The IOvisor looks at the incoming NFS request and determines which distributed resource it belongs to. The IO routing
process can be visualized in the figure below. Notice that NFS is maintained internal to the ESXi-HX CVM communication
path only, and is never exposed to the guest VMs or any other outside resource.
The IO must be directed via the IOvisor to the correct physical node (pNode). Each controller VM queries the Cluster Resource Manager (CRM) via the cluster IP to retrieve the pNode mappings. The communication occurs via a special NFS procedure that has been added as an extension to the base NFS protocol. The mapping table is then cached locally so there is minimal traffic to the cluster IP. The deterministic process to route to the correct node leaves the IOvisor as a stateless IO proxy.

**HX Management**

There are four relevant management interfaces to consider with HX. There are the UI interfaces (native and vCenter plug-in) and there is the CLI and the REST API.

**Management Interfaces**

**HX Connect**

HX Connect is a native UI for managing the HX cluster. This includes configuring replication and encryption along with some VM management functions.
HX Connect has a security warning banner that can be disabled on a global basis by the administrator(s).

The session to the interface is encrypted via FIPS compliant SSL communications. The mechanics of the session are described below and caution should be taken by the administrator(s) when logging out of sessions to ensure that all tokens are revoked and sessions are terminated.

Session architecture:
1. When a user logs in server provides an access token to the user. This access token is used to validate this user and do all subsequent actions.
2. Idle Timeout is by default set to 30 minutes. You can change/view this idle timeout in UI in user settings (Click on the top right user icon and you will see the user setting.)
3. Idle timeout is global and can be changed or viewed by a user with admin role.
4. If an admin user changes the idle timeout it will be reflected for all the users.
5. From HX Connect perspective, if a user is not doing any activity on the GUI and is idle then after 30 minutes (default idle timeout), the user is logged out.
6. Once the user logs out, the access token is revoked.

Details of the transaction:
Session Management happens at the HX Connect browser end, and token management happens in AAA [backend]. Once a user logs in, a session starts. The “start of session” implies that HX Connect creates a cookie and installs it in the browser.

This cookie is removed under the following circumstances:

1. When user logs out explicitly.
2. When idle timeout occurs.
3. When user closes the browser completely.
If you log in using HX Connect (session starts):

1. You share the same session if you open another tab in browser window.
2. You share the same session if you open another window from the browser you logged-in.

In addition, this means that if you login using HX Connect and open another window or tab and navigate to the CIP-M, and then logout, you log out from all tabs and windows.

Please note that the cookie is not removed when:

1. User closes a tab.
2. User closes a window in the browser [however, the browser process is still running, i.e. another widow of this browser is still alive].

This means that the login session is still active in the above two cases.

Associated with the session is a token. This is managed by AAA. This token will be invalidated when the user logs out.

*If you close the browser completely without logging out, you will no longer have a session, but the token will be alive. Therefore, it is recommended that you logout before closing the browser.*

Multiple Sessions for same user are supported if user logs in:

1. From different machines.
2. From different kinds of browser [such as, Chrome and Safari] on the same machine.

HX Connect also provides a support bundle collection interface that allows the user to collect and download all system component logs, including audit files. These can then be examined or uploaded to support.

**vCenter Plug-in**

The vCenter plug-in is an https accessible UI available after logging in to vCenter. The portlet to access the plug-in is in the summary page for the cluster or accessible in the VC inventory list. The besides providing an admin interface for datastore creation and cluster consumption overviews, the plug-in has a monitor tab that permits event and task browsing along with hardware status.
The plug-in’s right click context menu also allows the administrator to create VAAI offloaded snapshots of VMs, perform cloning operations, and generate system wide support bundles for log collection. These can then be examined or uploaded to support.

Plug-in session mechanics operate in the same manner as vCenter sessions and are managed by editing the appropriate vCenter configuration files.

**STCLI**
A session via FIPS compliant SSH cipher suites is used to access the CLI (STCLI). All administrative functions along with some extra options are available via the CLI. See the HX STCLI reference for an exhaustive list.


A warning banner can be configured on the control VM (HXDP) for display on access using the MOTD functionality available in the base OS. This can also be done for ESX.

- At the control VM CLI add a file called /etc/update-motd.d/00-springpath-motd
- At the ESX CLI use the web or C# client to set config/etc.issue for the DCUI and config/etc.motd for SSH both under advanced options. Alternatively, use /etc/issue for DCUI and /etc/motd for SSH.
- There is no customization on the vSphere Web client logging into vCenter.

The STCLI security subset of commands enables the administrator to configure external machines to access the datastore, configure the root password, synchronize SSH keys across the nodes or enable, set, and disable encryption. Access should not be granted unless the external system is trusted. Access should be revoked when move/copy/migration operations are complete.

**STCLI security**
usage: stcli security [-h] {password,whitelist,ssh,encryption} ...

REST APIs
Cisco HXDP comes with a comprehensive REST based API for use in developing custom software that can access the system. The built-in REST API:

- Contains well-documented syntax and examples with REST API explorer
- Secure token based access with RBAC and auditing
- Accessed Via: http://<Cluster-IP>/apiexplorer

Starting with HXDP 4.0.1a, a subset of the REST API entries are reserved for STIG specific functions. The following is a list of the current set:

- configure_stig_parameters
- configure_stig_parameters_host
- configure_stig_parameters_vm
- configure_stig_parameters_vCenter
- remove_stig_parameters
- check_stig_parameters

Examine the API explorer discussed above for more detailed explanations of the values passed and returned by these STIG API calls.

AAA Domains
Authentication, authorization and accounting (AAA) is managed by HX depending on the access method. HX Data Platform supports Role-Based Access Control (RBAC). AAA is implemented with Open Authorization (OAuth), Security
Assertion Markup Language (SAML), or Lightweight Directory Access Protocol (LDAP). It is integrated with the ESX cluster authentication mechanism. HX Connect and the STCLI primarily use this database for user authentication. Access to HX Connect or the STCLI is also available using a local admin account in the event that vCenter is unavailable. Beginning in HX 3.5(1a) the local root user is no longer available for HX Connect logins.

vCenter
vCenter maintains a set of user accounts and roles in a database. vCenter itself can be integrated with an external AD or LDAP user management system. HX RBAC integrates directly to this mechanism. See the HX RBAC documentation for configuration steps.

AD Integration
You can join a Platform Services Controller appliance or a vCenter Server Appliance with an embedded Platform Services Controller to an Active Directory domain and attach the users and groups from this Active Directory domain to your vCenter Single Sign-On domain.


User Management
RBAC settings configure users with one or more roles. Roles are assigned privileges to act on a resource. For example, one role has a privilege to perform virtual machine power on, another role has a privilege to only monitor a virtual machine. Users are created through vCenter. vCenter supports Active Directory (AD) users and groups. Two roles are supported with HX. Privileges associated with these roles cannot be modified.

- **Administrator:**
  - Most tasks that can be performed on a HX Storage Cluster require administrator privileges.
  - Administrative users grant privileges to the roles.
  - Administrator users have access to the HX Data Platform interfaces: HX Connect, HX Data Platform Plug-in, the Storage Controller VM command line for running STCLI commands, and HX Data Platform REST APIs.

- **Read-only:**
  - This role allows users to monitor status and summary information through HX Connect and the HX Data Platform Plug-in.
  - Read Only users have access to the HX Data Platform interfaces: HX Connect and the HX Data Platform Plug-in.

Cisco HyperFlex User Overview
The user types (updated for HX 3.5(1a)) allowed to perform actions on or view content in the HX Data Platform, include:

- **admin**—A predefined user included with HX Data Platform. The password is set during HX Cluster creation. Same password is applied to root. This user has read and modify permissions.

- **root**—A predefined user included with HX Data Platform. The password is set during HX Cluster creation. Same password is applied to admin. This user has read and modify permissions.

- **administrator**—A created HX Data Platform user. This user is created through vCenter and assigned the RBAC role, administrator. This user has read and modify permissions. The password is set during user creation.

- **read-only**—A created HX Data Platform user. This user is created through vCenter and assigned the RBAC role, read-only. This user only has read permissions. The password is set during user creation.
<table>
<thead>
<tr>
<th>HX Interface</th>
<th>admin</th>
<th>root</th>
<th>hx_admin</th>
<th>hx_readonly</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX Data Platform Installer</td>
<td>Required</td>
<td>Optional</td>
<td>Not valid</td>
<td>Not valid</td>
</tr>
<tr>
<td>HX Connect</td>
<td>Can perform most HX tasks.</td>
<td>Not Valid</td>
<td>Can perform most HX tasks.</td>
<td>Can only view monitoring information.</td>
</tr>
<tr>
<td>Storage Controller</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can only run non-interactive stcli commands to view status.</td>
</tr>
<tr>
<td>VM with stcli command line</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HX REST API</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can only run status level REST APIs.</td>
</tr>
</tbody>
</table>

- User Management Terms
- Audit Logs for AAA Accounting
You can use REST APIs with read only user. If you have a read-only user, (s)he can perform only GET operations. They will receive an access error if they perform PUT, POST, or DELETE operations. This is present in 2.6 and 3.0 onwards for VMware clusters. The non-read only users are called admin users. They are CVM users and users belonging to administrator group in vCenter.

Local Users
The RBAC users created for UI access also have STCLI access. However, the cluster maintains a separate administrative account called root that is created at install time. This root user has full privileges to the system and hard passwords are enforced during creation. This root user can be used separately from the vCenter RBAC user database to access the STCLI or HX Connect. This account can be disabled after which any STCLI access is “sandboxed”. Read only users that access the CLI are also sandboxed. Users can still perform administrative commands with the use of “sudo” if needed. Knowledge of the secure, hard root password is required.

If required, the root account can be disabled using the following steps:

1. edit the file /etc/ssh/sshd_config
2. Locate the line “PermitRootLogin yes”
3. Change the line to “PermitRootLogin no”
4. Save the file
5. restart SSH

The vCenter based administrator account is still allowed, and the user must use sudo for commands that require higher privileges. All STCLI commands should work fine without sudo.

Users created on the system locally using “useradd” are all root users for the local node with the same privileges but are not synchronized across nodes or maintained at the cluster level. They can be created by SSHing to the HXDP for a cluster node. Create a new HXDP root user using: useradd –G root NewRoot then set the password using the passwd NewRoot command. This procedure would need to be repeated on each node for this user to access the other HXDPs with this new account. It is not recommended that you create local node root users.

UI Users
Create new users for HX using vCenter with roles. This applies to the HX vCenter Plug-in and HX Connect UIs.

1. Log into the GUI plug-in for the cluster and select Administration under the Home icon.
CLI users are authenticated using the RBAC infrastructure for the cluster. Local HXDP cluster users (root) are authenticated with the cluster-maintained account. Any other root user created using useradd at the cli is maintained locally for the node itself. Creating these types of users is not recommended.

To change the password for the STCLI cluster root user:
- `stcli security password`

To set or change the password for the local node root user:
- `passwd root`

To set or change the vCenter maintained administrative user password (see UI users above):
- `log in to vCenter`
- `select Administration→Users and Groups`
- `Edit the password for the user`

**Auditing, Logging, Support Bundles**

An audit trail, maintained in a set of audit logs, is a security-relevant chronological set of records that provide documentary evidence of the sequence of activities that have affected the system. They contain records of system changes at any time a specific operation, procedure, or event occurs. A full set of logs for the entire system can be gathered with a support bundle. However, STCLI and REST command are recorded continuously and can be examined by looking at just a few files instead of the generating a comprehensive log dump. STCLI commands use the REST architecture to execute their commands so they are also capture in the REST log. These audit records are maintained on each node of the system and are contained primarily in the following files on each node in the `/var/log/springpath` directory:

- `stMgr.log`
- `audit-rest.log`

Auditing is required for compliance purposes and for forensic examination of system activity. A typical audit-rest.log entry will look like this:

```
2017-06-29-23:26:38.096 - Audit - 127.0.0.0.1 -> 127.0.0.0.1 -- create /aaa/v1/auth?grant_type=password; 201; null 3341ms
```


What sources are captured:
- GUI -- REST API auditing – Any calls to REST
  - A method to audit UI usage as well as 3rd party integrated software
  - `/var/log/springpath/Audit-rest.log`
- STCLI (RBAC) auditing
- STCLI calls utilize the API
- Audit trail records will have the keyword “Audit”.
- Collect all such Audit trail records and save it

The cluster root user or a node root user can manipulate the audit logs. Read-only users or any other RBAC user account cannot alter the logs files

Replication log files that can be used for auditing traffic or general troubleshooting are listed below:
Support Bundles for the HX system can be generated in two ways. There are menu interfaces to generate them in both HX Connect and the vCenter Plug-in UI.

1) Generating the Support Bundle using vCenter:
2) Similarly, the Support Bundle can be generated in HX Connect:
If Auto Support has not been configured during install, be sure to configure it now. This can be done via HX Connect (see the Support menu in the above illustration) or via STCLI using STCLI services ASUP. Auto Support enables:

- HTTP based auto-support data collection for proactive case creation
- Continuous monitoring thru auto-support for 30+ events to detect early problems
- Critical events integrated with Smart Call Home
- Auto-generate SRs (tickets)
- Email notifications for critical events

The log bundle in vCenter includes the plug-in log file and is located in the regular vCenter log location. For Windows the default is C:\ProgramData\VMware\vCenterServer\logs. For VCSA (vCenter Server Appliance) the default log location is /var/log/vmware.

### Setting Up Remote Logging for HX Prior to HXDP 4.0.1.a

The various audit logs are available for each node and specific to that node. The CIP-M maintains logs for the local node and any command access to this node via the CIP-M. If you need to consolidate the logs for all components for simplified auditing, this can be done with syslog. You will need to build a syslog infrastructure with a syslog server at (preferably) an external location that each node can access. You will then configure syslog-ng on each HXDP node, rsyslog.d on each ESXi node, and finally the syslog destination on UCSM. These will each act as syslog clients with the remote syslog server as the destination.

For syslog-ng configuration see this documentation and check the references section at the end of this paper: [https://syslog-ng.com/open-source-log-management](https://syslog-ng.com/open-source-log-management)

### Setting Up Remote Logging for HXDP 4.0.1.a and Later

Beginning with HXDP 4.0.1a, HyperFlex includes a built-in syslog mechanism. Using the HX Connect Remote Logging wizard, you are able to enter the information required for each HX Cluster node to send its audit log records to a centralized remote server. You are required to have a remote log collection server built and accessible by the management interfaces on each cluster node. See Appendix E for a sample syslog-ng configuration file used for an Ubuntu-based log collector.

By clicking the gear symbol in the top right of the HX Connect UI, you can select remote logging. You will be presented with the following:
This is the default configuration and it is for unencrypted transport over TCP using port 6514. The port is configurable, however you must use either plain text or encrypted transport. If you select the drop-down you are given the option to change the connection type to TLS (encrypted).
The wizard then prompts you to upload a client certificate and key pair. This certificate and key will be used for each node to securely communicate with the remote log collection server. If the certificate is CA signed, it does not need to be uploaded.

If using self-signed certificates on the remote server, place them under `/etc/syslog-ng/CA`. Regardless of connection type selected, the system will attempt to connect to the remote server immediately. The server certificate will automatically be placed into the trusted certificate store on the syslog-ng client nodes.

The following syntax can be used with openssl to generate a self-signed certificate and key for both the client system and the remote server in the absence of a CA certificate:

```bash
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

**Password Requirements**

Hard passwords are required for the cluster root user during installation. This password can be updated using the CLI from any node. SSH to the node and issue `stcli security password`.

Passwords for users maintained in the vCenter authentication database can have password difficulty set based on vCenter configuration. See your vCenter documentation for this.
Local node users created using “useradd” will be subject to warnings based on the password settings in /etc/pam.d/common-password, however since only root users can be created locally, these can be bypassed. It is not recommended to create local node root users for this reason.

Password Guidelines
The storage controller VM password for the predefined users admin and root are specified during HX Installer deployment. After installation, you can change passwords through the stcli command line.

<table>
<thead>
<tr>
<th>Component</th>
<th>Permission Level</th>
<th>Username</th>
<th>Password</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX Data Platform OVA</td>
<td>root</td>
<td>root</td>
<td>Cisco123</td>
<td></td>
</tr>
<tr>
<td>HX Data Platform Installer VM</td>
<td>root</td>
<td>root</td>
<td>Cisco123</td>
<td></td>
</tr>
<tr>
<td>HX Connect</td>
<td>administrator or read-only</td>
<td>User defined through vCenter.</td>
<td>User defined through vCenter.</td>
<td>Requires leading local/ for login: local/admin or local/root</td>
</tr>
<tr>
<td>HX Storage Controller VM</td>
<td>root</td>
<td>User defined during HX installation.</td>
<td>As specified during HX installation.</td>
<td>Must match across all nodes in storage cluster. Use the stcli command when changing the password after installation.</td>
</tr>
<tr>
<td>vCenter</td>
<td>admin</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> default. SSO enabled. As configured, MYDOMAIN\name or <a href="mailto:name@mydomain.com">name@mydomain.com</a></td>
<td>SSO enabled. As configured.</td>
<td>Ensure the vCenter credentials meet the vSphere 5.5 requirements if the ESX servers are at version 5.5. Read only users do not have access to HX Data Platform Plug-in.</td>
</tr>
<tr>
<td>Component</td>
<td>Permission Level</td>
<td>Username</td>
<td>Password</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
<td>----------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>ESX Server</td>
<td>root</td>
<td>SSO enabled.</td>
<td>SSO enabled.</td>
<td>Must match across all ESX servers in storage cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As configured.</td>
<td>As configured.</td>
<td></td>
</tr>
<tr>
<td>Hypervisor</td>
<td>root</td>
<td>root</td>
<td>As specified during HX installation.</td>
<td>Use vCenter or esxcli command when changing the password after HX installation.</td>
</tr>
<tr>
<td>UCS Manager</td>
<td>admin</td>
<td>As configured.</td>
<td>As configured.</td>
<td></td>
</tr>
<tr>
<td>FI</td>
<td>admin</td>
<td>As configured.</td>
<td>As configured.</td>
<td></td>
</tr>
</tbody>
</table>

You are free to change root/admin password anytime using stcli on any one CVM. The HXDP command line performs password synchronization with the other nodes in the cluster. This will not adversely affect any operations.

**Session Timeouts**

vCenter session timeouts are managed by vCenter configuration settings. Idle timeouts for TLS connections when using the HyperFlex plug-in are set in the following file making the noted changes:

- vSphere Web Client sessions terminate after 120 minutes by default. You can change this default in the webclient.properties file, as discussed in the vCenter Server and Host Management documentation.
- Login to the vCenter host system and navigate to this properties file. The location of this file depends on the base operating system on which vCenter is installed.
- Edit the file to include the line `session.timeout = value` where value is the timeout value in minutes. For example, to set the timeout value to 60 minutes, include the line `session.timeout = 60`.
- Restart the service

Alternatively:

- In the vSphere Web Client, navigate to the vCenter Server instance.
- Select the Manage tab.
- Under Settings, select General.
- Click Edit.
- Select Timeout settings.
- In Normal operations, type the timeout interval in seconds for normal operations.

**HX Connect**

Idle session timeouts for HX Connect sessions can be set in the dashboard view under the administrative icon.
**CLI**

The idle timeout for an STCLI session can be set on each HXDP. SSH to the STCLI of each node and navigate to the `/etc/ssh/sshd_config`. Uncomment and change the `ClientAliveInterval` by setting a time. Once editing is complete, restart the sshd services. `ClientAliveInterval 60` would drop the connection after 60 seconds of inactivity.

**Manually Clearing Sessions**

To clear session data associated with a given user immediately you can run this command from any CVM while logged in as root:

```bash
> python /opt/springpath/clearsession.py root
```

Users can run into this situation if they close the browser session without logging out.

---

**HX Platform Hardening**

This section provides information on setting specific configurations for HX, ESX and UCS to further enhance system security.

**US Federal STIG (Secure Technical Implementation Guide) Settings**

Cisco implements relevant Secure Technical Implementation Guide (STIG) settings as defined by the Defense Information Security Agency (DISA) for several aspects of the HXDP ecosystem. The STIG adherence is accomplished through implementation of settings explicitly called out in the following DISA STIGS:

- `U_General_Purpose_Operating_System_V1R4_SRG`
- `U_VMware_vSphere_6-0_ESXi_V1R4_STIG`
- `U_VMware_vSphere_6-0_vCenter_Server_for_Windows_V1R4_STIG`
- U_VMware_vSphere_6-0_Virtual_Machine_V1R1_STIG

These can be found and downloaded from the Federal DISA site here. These STIG settings are automated via script and are generally available starting in HXDP v3.5. Please note that DISA STIGs are dynamic, and as such, will be updated frequently, so you can expect this list to change. The corresponding automation in HXDP will follow suit. Some of these settings, while desirable for secure daily operation, have potential repercussions for cluster upgrade and expansion. As such, some settings may need to be temporarily disabled to accommodate changes of this nature. See the administration guide for your version of HXDP for instructions on running STIG automation and caveats around them for certain cluster operations.

Some settings derived from the DISA STIG set have become the default. For example, to improve our security posture, starting with HXDP 3.0, it is now the default to set promiscuous mode, forged transmits, and MAC change to REJECT in ESXi. Any new cluster install on v3.0 or greater and any upgrades to v3.0 or greater should have these settings automatically applied. There are some versioning caveats, however.

You may not manually set these to reject before HXDP 3.0 as it is not compatible with management clustering. Please upgrade to HXDP 3.0 or later if these settings are required. The lesson here is to verify your version with respect to the STIG settings that are applied. Settings that ship with a specific version have been thoroughly tested with that version.

A technote on the STIG settings can be found here:


Note that the STIG scripts must be run from each CVM node. SSH to each CVM management IP and change to the following path:

/usr/share/springpath/storfs-misc/hx-scripts

From this location run the stig_security_settings.py script. Note that this script has default configuration values in the stig_config.ini file located in the same directory. These may be edited as needed, but will no longer match the vetted settings. Every setting set by the STIG script is idempotent, so multiple executions of the script will not adversely affect the system and you can reset your compliance baseline at any time by running it if things have changed in the interim.

Beginning with HXDP 4.0.1a, a subset of the REST API contains STIG related entries. See the section on REST APIs above.

**SSL Certificate Replacement**

During Cisco HyperFlex deployment, a set of local certificates is generated between the components to allow for trusted communication. Many organizations have their own certificate authority already in place. It is recommended that you replace the default SSL Certificates with your certificates. The following TechZone article describes the steps for installing self-signed certificates in detail. The process is the same for CA signed certificates, except a trusted entity will sign instead.

TLS Weak Cipher Disable

Some environments require a subset of the default TLS ciphers to be disabled. This procedure to do this must be performed on each controller VM.

On each controller VM, edit /etc/nginx/conf.d/springpath.conf and change the line starting with ssl_protocols:

```
#ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_protocols TLSv1.2;
```

Save the file and exit your editor (vi). Restart nginx using `service nginx restart` from the CVM CLI.

Strict TLS 1.2 support cannot be enabled prior to HXDP 3.0. There are ecosystem interop issues between UCSM, HXDP vCenter, and HXDP DR functionality that prevent this. Starting with HXDP 3.0, across the board all components are strict TLS 1.2 implementations. All of 3.0 and above is strictly TLS 1.2, including new provisioning and upgrades from 2.x to 3.x. From 3.0 onwards, HXDP does not support anything less than TLS 1.2.

SSH (ESX) Lockdown Mode and Root Logins

ESX SSH lockdown mode can be enabled on each ESX node of the HX cluster. This applies only to a post-install system. SSH traffic must not be blocked during install. Lockdown of SSH for ESXi is supported in HXDP 2.5 and above. The following constraints apply to the deactivation of remote SSH access to the system for versions prior to 3.5(1a):

1. HX Snapshots for VMs are disabled (redo-log based snapshots still function).
2. The source VM for a ReadyClone operation must remain powered off for a cloning operation. Once the operation is complete, the source VM can be powered back on. Clones themselves are unaffected.
3. System upgrades are disabled until SSH is re-enabled.

SSH needs to be enabled before cluster expansion can take place. It can be disabled again afterwards.

In HXDP 3.0 and above, snapshots and native replication do not use SSH to interface with ESXi; i.e., neither “root” nor “hxuser” based SSH logins are performed. With respect to logins to hostd (ESXi), for vSphere API access, only “hxuser” is used. Root login is only used during cluster creation, node expansion, and initial installation.

Lockdown Mode in HX 3.5(1a) is either Disabled, Normal or Strict. When Lockdown is enabled, the ESXi host can only be accessed through the vCenter server or the Direct Console User Interface (DCUI). Enabling Lockdown mode affects which users are authorized to access host services. Once Lockdown mode is enabled, and if root or administrator@vsphere.local or any other use is not part of the Exception user list, SSH to that ESX is not allowed. Similarly, if the host has been removed from the vCenter for some reason, adding the host back to vCenter is not allowed.

Here is an overview of the features:
Lockdown Mode exists in three states:
- Disabled → Can SSH to host
- Normal → Can connect through DCUI or VC
- Strict → Can connect only using VC

Upgrade checks whether Lockdown Mode is enabled
- If enabled, prompts the user to disable for upgrade to proceed
- Upgrade will not proceed even in normal Lockdown mode

Normal vs. Strict mode have additional different behaviors and exceptions. For a comprehensive examination of system behavior in each mode and for troubleshooting guidelines for Lockdown, see the HyperFlex Installation Guide.

Tech Support Mode
Available starting in HX 3.5(1a), Tech Support Mode, also called “Controller Access Over SSH”, is specifically designed to allow for CVM troubleshooting.

- Tech Support Mode is enabled by default
  - Allows SSH access to the CVM management interface
- Tech Support Mode can be disabled
  - SSH to CVM management IP is disallowed
- Status of Tech Support Mode is listed in the status banner at the top of System Information in HX Connect
- If Tech Support Mode is disabled, the user will be prompted to enable it for upgrades to proceed

Third Party Software Execution on FIs and HXDP
Cisco does not support the installation of 3rd party software on either Fabric Interconnects (FIs) or on HXDP nodes (ESXi or HX CVM). For FI’s, external software is not supported by virtue of the UCSM kernel-space type management shell. It is not possible to load or run any applications. For HXDP, Cisco does not recommend or support the installation and/or execution of 3rd party applications. In the current release (4.0.X) it is recommended that you use HXDP’s tech support mode along with ESXi’s lock down mode at the same time in order to safeguard against accidental or malicious attempts to run external applications on the HX CVM or the node hypervisor. In a future release, HXDP will have a kernel space shell making this precaution redundant.

Whitelisting and other STCLI Security Commands
The HX datastores are a protected resource only mountable by HX nodes participating in the cluster (either by installation or by expansion). These protected datastore(s) cannot be mounted by other systems unless they are whitelisted. To whitelist a system for the cluster, ssh to a node and use the stcli security whitelist commands:

```
Remove systems from the list when not in immediate use.

root@SpringpathControllerEWA35H09RF:~# stcli security
usage: stcli security [-h] {password,whitelist,ssh,encryption} ...

root@SpringpathControllerEWA35H09RF:~# stcli security password
usage: stcli security password [-h] {set} ...
```
root@SpringpathControllerEWA35H09RF:~# stcli security whitelist
usage: stcli security whitelist [-h] {list,add,remove,clear} ...

root@SpringpathControllerEWA35H09RF:~# stcli security ssh
usage: stcli security ssh [-h] {resync} ...

root@SpringpathControllerEWA35H09RF:~# stcli security encryption
usage: stcli security encryption [-h] {ucsm-ro-user} ...

root@SpringpathControllerEWA35H09RF:~#

HX Data Platform Firewalling: IP Tables
Each HXDP node maintains a set of IP Tables firewall entries. This serves to explicitly set traffic that is allowed to communicate in and out with the HXDP node. The table is maintained automatically and shouldn't have to be edited. These entries are listed for reference below. They are also automatically updated when HX Native Replication is enabled so that cluster-cluster traffic is permitted.

root@ucs-stctlvm-137-1:~# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p tcp --tcp-flags rst rst -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p udp --dport 427 -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p udp --dport 427 -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p udp --dport 427 -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p udp --dport 427 -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p udp --dport 427 -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p udp --dport 427 -j ACCEPT
-A INPUT -d 10.a.b.c/32 -i eth0 -p udp --dport 8125 -j ACCEPT
-A INPUT -d 10.a.b.d/32 -i eth0 -p udp --dport 8125 -j ACCEPT
-A INPUT -d 10.a.b.e/32 -i eth1 -p udp --dport 8125 -j ACCEPT
-A INPUT -s 10.a.b/g/32 -d 10.a.b.l/32 -i eth1 -j ACCEPT
-A INPUT -s 10.a.b/g/32 -d 10.a.b.e/32 -i eth1 -j ACCEPT
-A INPUT -s 10.a.b/f/32 -d 10.a.b.l/32 -i eth1 -j ACCEPT
-A INPUT -s 10.a.b/h/32 -d 10.a.b.e/32 -i eth1 -j ACCEPT
-A INPUT -s 10.a.b/i/32 -d 10.a.b.e/32 -i eth1 -j ACCEPT
-A INPUT -s 10.a.b/j/32 -d 10.a.b.l/32 -i eth1 -j ACCEPT
Cisco HX Platform Hardening Guide

-A INPUT -s 10.a.b/j32 -d 10.a.b.e/32 -i eth1 -j ACCEPT
-A INPUT -s 10.a.b.k/32 -d 10.a.b.l/32 -i eth1 -j ACCEPT
-A INPUT -s 10.a.b.k/32 -d 10.a.b.e/32 -i eth1 -j ACCEPT
-A INPUT -p udp -m udp --dport 32768:65535 -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -j DROP

root@ucs-stctlvm-137-1:~# iptables -L
Chain INPUT (policy ACCEPT)
  target prot opt source destination
  ACCEPT all -- anywhere anywhere
  ACCEPT all -- anywhere anywhere cstate RELATED,ESTABLISHED
  ACCEPT tcp -- anywhere ucs139-cip-m.eng.test-domain.com tcp dpt:https
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:https
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:https
  ACCEPT tcp -- anywhere ucs139-cip-m.eng.test-domain.com tcp dpt:8888
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:8888
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:8888
  ACCEPT tcp -- anywhere ucs139-cip-m.eng.test-domain.com tcp dpt:ssh
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:ssh
  ACCEPT tcp -- anywhere ucs139-cip-m.eng.test-domain.com tcp dpt:http
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:http
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:http
  ACCEPT tcp -- anywhere ucs139-cip-m.eng.test-domain.com tcp dpt:ntp
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:ntp
  ACCEPT tcp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com tcp dpt:ntp
  ACCEPT udp -- anywhere ucs139-cip-m.eng.test-domain.com udp dpt:svrloc
  ACCEPT udp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com udp dpt:svrloc
  ACCEPT udp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com udp dpt:svrloc
  ACCEPT udp -- anywhere ucs139-cip-m.eng.test-domain.com udp dpt:8125
  ACCEPT udp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com udp dpt:8125
  ACCEPT udp -- anywhere ucs-stctlvm-137-1.eng.test-domain.com udp dpt:8125
  ACCEPT all -- ucs-stctlvm-139.eng.test-domain.com ucs139-cip.eng.test-domain.com
  ACCEPT all -- ucs-stctlvm-139.eng.test-domain.com ucs-stctlvm-137.eng.test-domain.com \ ACCEPT all -- ucs139-v.eng.test-domain.com ucs139-cip.eng.test-domain.com
  ACCEPT all -- ucs139-v.eng.test-domain.com ucs-stctlvm-137.eng.test-domain.com \ ACCEPT all -- ucs136-v.eng.test-domain.com ucs139-cip.eng.test-domain.com
  ACCEPT all -- ucs136-v.eng.test-domain.com ucs-stctlvm-137.eng.test-domain.com \ ACCEPT all -- ucs137-v.eng.test-domain.com ucs139-cip.eng.test-domain.com
  ACCEPT all -- ucs137-v.eng.test-domain.com ucs-stctlvm-137.eng.test-domain.com \ ACCEPT all -- ucs-stctlvm-138.eng.test-domain.com ucs139-cip.eng.test-domain.com
  ACCEPT all -- ucs-stctlvm-138.eng.test-domain.com ucs-stctlvm-137.eng.test-domain.com \ ACCEPT all -- ucs138-v.eng.test-domain.com ucs139-cip.eng.test-domain.com
  ACCEPT all -- ucs138-v.eng.test-domain.com ucs-stctlvm-137.eng.test-domain.com \ ACCEPT udp -- anywhere anywhere udp dpts:32768:65535
  ACCEPT icmp -- anywhere anywhere
  DROP all -- anywhere anywhere
Chain FORWARD (policy ACCEPT)
  target prot opt source destination \n
Chain OUTPUT (policy ACCEPT)
  target prot opt source destination \n
Cisco HX Platform Hardening Guide Page 56
Replication
Replication setting changes are maintained globally once replication is enabled on the cluster. Firewall entries are updated for ports needed for replication (see Networking Requirements above).

When replication is enabled, a new NIC is non-disruptively added to HXDP. This NIC is assigned an IP address in a new replication VLAN. The HX Service Profile on the FI (via UCSM) is automatically updated.

Replication traffic is not encrypted on the wire from the cluster. Secure replication requires an IPSEC capable WAN connection or relies on a trusted network. Data on the wire is always compressed so it’s general appearance is not plain text.

Specific ESX Environment Hardening Settings Relevant to HXDP
See Appendix B for a set of ESX hardening configuration settings. These items are general recommendations from the UCS verified ESX hardening guide.

Specific USC Environment Hardening Settings Relevant to HXDP
The UCSM build used for the system must match the supported UCSM version in the preinstall checklist.

[HyperFlex_preinstall_checklist_link]

Refer to the UCS Hardening guide specifically for settings relevant to the build you are running.

References

ESX Hardening Guide
- ESX [https://www.vmware.com/security/hardening-guides.html]

UCS Hardening Guide

Cisco CSDL

Syslog-ng Configuration
- Syslog-ng configuration: [https://www.techrepublic.com/article/how-to-use-syslog-ng-to-collect-logs-from-remote-linux-machines/]

[HyperFlex_preinstall_checklist_link]
# Appendix A: Networking Ports

The following table lists the ports required for component communication for the HyperFlex solution.

<table>
<thead>
<tr>
<th>Component</th>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Server</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td></td>
<td>123</td>
<td>UDP</td>
<td>Each ESX Node</td>
<td>Time Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Each SCVM Node</td>
<td>Time Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UCSM</td>
<td>Time Server</td>
<td></td>
</tr>
<tr>
<td><strong>HX Installer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td></td>
<td>22</td>
<td>TCP</td>
<td>HX Installer</td>
<td>Each ESX Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>Each SCVM Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>CIP-M</td>
<td>Cluster Mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>UCSM</td>
<td>UCSM mgmt addresses</td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td>80</td>
<td>TCP</td>
<td>HX Installer</td>
<td>Each ESX Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>Each SCVM Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>CIP-M</td>
<td>Cluster Mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>UCSM</td>
<td>UCSM mgmt addresses</td>
</tr>
<tr>
<td>HTTPS</td>
<td></td>
<td>443</td>
<td>TCP</td>
<td>HX Installer</td>
<td>Each ESX Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>Each SCVM Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>CIP-M</td>
<td>Cluster Mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>UCSM</td>
<td>UCSM mgmt addresses</td>
</tr>
<tr>
<td>vSphere SDK</td>
<td></td>
<td>8089</td>
<td>TCP</td>
<td>HX Installer</td>
<td>Each ESX Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9333</td>
<td>TCP</td>
<td>HX Installer</td>
<td>Each ESX Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>CIP-M</td>
<td>Cluster Mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>UCSM</td>
<td>UCSM mgmt addresses</td>
</tr>
<tr>
<td>Heartbeat</td>
<td></td>
<td>902</td>
<td>TCP/UDP</td>
<td>HX Installer</td>
<td>vCenter, Each ESX Node</td>
<td>Cluster Data Network</td>
</tr>
<tr>
<td>ICMP</td>
<td></td>
<td></td>
<td></td>
<td>HX Installer</td>
<td>ESX/CVM Ips</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td><strong>Mail Server</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td></td>
<td>25</td>
<td>TCP</td>
<td>Each SCVM Node</td>
<td>Mail Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CIP-M</td>
<td>Mail Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UCSM</td>
<td>Mail Server</td>
<td></td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Poll</td>
<td></td>
<td>161</td>
<td>UDP</td>
<td>Monitoring</td>
<td>UCSM</td>
<td></td>
</tr>
<tr>
<td>SNMP Trap</td>
<td></td>
<td>162</td>
<td>UDP</td>
<td>UCSM</td>
<td>Monitoring Server</td>
<td></td>
</tr>
<tr>
<td><strong>Name Server</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td></td>
<td>53</td>
<td>TCP/UDP</td>
<td>Each ESX Node</td>
<td>Name Server</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Each SCVM Node</td>
<td>Name Server</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CIP-M</td>
<td>Name Server</td>
<td>Cluster Mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UCSM</td>
<td>Name Server</td>
<td></td>
</tr>
<tr>
<td><strong>vCenter</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Source</td>
<td>Destination</td>
<td>Direction</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>----------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>vCenter</td>
<td>Each SCVM Node</td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td></td>
<td>CIP-M</td>
<td></td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>HTTPS (plugin)</td>
<td>443</td>
<td>TCP</td>
<td>vCenter</td>
<td>Each ESX Node</td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td></td>
<td>CIP-M</td>
<td></td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>HTTPS (VC SSO)</td>
<td>7444</td>
<td>TCP</td>
<td>vCenter</td>
<td>Each SCVM Node</td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td></td>
<td>CIP-M</td>
<td></td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>HTTPS (plugin)</td>
<td>9443</td>
<td>TCP</td>
<td>vCenter</td>
<td>Each ESX Node</td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td></td>
<td>CIP-M</td>
<td></td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>CIM Server</td>
<td>5989</td>
<td>TCP</td>
<td>vCenter</td>
<td>Each ESX Node</td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td></td>
<td>CIP-M</td>
<td></td>
<td>Bidirectional</td>
<td></td>
</tr>
<tr>
<td>Heartbeat</td>
<td>902</td>
<td>TCP/UDP</td>
<td>vCenter</td>
<td>Each ESX Node</td>
<td>Introduced in ESXi 6.5</td>
<td></td>
</tr>
</tbody>
</table>

**User**

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>TCP</td>
<td>User</td>
<td>Each ESX Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>Each SCVM Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>CIP-M</td>
<td>Cluster Mgmt</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>HX Installer</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>UCSM</td>
<td>UCSM mgmt addresses</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>vCenter</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>SSO Server</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>User</td>
<td>Each SCVM Node</td>
<td>Mgmt addresses</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>CIP-M</td>
<td>Cluster Mgmt</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>UCSM</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>HX Installer</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>vCenter</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>User</td>
<td>Each SCVM Node</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>CIP-M</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>UCSM</td>
<td>UCSM mgmt addresses</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>HX Installer</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>vCenter</td>
<td></td>
</tr>
<tr>
<td>HTTPS (SSO)</td>
<td>7444</td>
<td>TCP</td>
<td>User</td>
<td>vCenter</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td>User</td>
<td>SSO Server</td>
<td></td>
</tr>
<tr>
<td>HTTPS (plugin)</td>
<td>9443</td>
<td>TCP</td>
<td>User</td>
<td>vCenter</td>
<td></td>
</tr>
<tr>
<td>KVM</td>
<td>2068</td>
<td>TCP</td>
<td>User</td>
<td>UCSM</td>
<td>UCSM mgmt addresses</td>
</tr>
</tbody>
</table>

**SSO Server**

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS (SSO)</td>
<td>7444</td>
<td>TCP</td>
<td>SSO Server</td>
<td>Each ESX Node</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>SSO Server</td>
<td></td>
<td></td>
<td>SSO Server</td>
<td>Each SCVM Node</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>SSO Server</td>
<td></td>
<td></td>
<td>SSO Server</td>
<td>CIP-M</td>
<td>Bidirectional</td>
</tr>
<tr>
<td><strong>Stretch Witness</strong></td>
<td>Port</td>
<td>Protocol</td>
<td>Service</td>
<td>Node(s)</td>
<td>Communication Details</td>
</tr>
<tr>
<td>---------------------</td>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td>---------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Zookeeper</td>
<td>2181</td>
<td>TCP</td>
<td>Witness</td>
<td>Each CVM Node</td>
<td>Bidirectional, Mgmt Addresses</td>
</tr>
<tr>
<td></td>
<td>2888</td>
<td>TCP</td>
<td>Witness</td>
<td>Each CVM Node</td>
<td>Bidirectional, Mgmt Addresses</td>
</tr>
<tr>
<td></td>
<td>3888</td>
<td>TCP</td>
<td>Witness</td>
<td>Each CVM Node</td>
<td>Bidirectional, Mgmt Addresses</td>
</tr>
<tr>
<td>Exhibitor (Zookeeper Lifecycle)</td>
<td>8180</td>
<td>TCP</td>
<td>Witness</td>
<td>Each CVM Node</td>
<td>Bidirectional, Mgmt Addresses</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>Witness</td>
<td>Each CVM Node</td>
<td>Potential Future Req.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>Witness</td>
<td>Each CVM Node</td>
<td>Potential Future Req.</td>
</tr>
<tr>
<td><strong>Replication</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Services Manager Peer</td>
<td>9338</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional, Include Cluster Mgmt IP as well</td>
</tr>
<tr>
<td>Replication for CVM</td>
<td>3049</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional, Include Cluster Mgmt IP as well</td>
</tr>
<tr>
<td>Cluster Map</td>
<td>4049</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional, Include Cluster Mgmt IP as well</td>
</tr>
<tr>
<td>NR NFS</td>
<td>4059</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional, Include Cluster Mgmt IP as well</td>
</tr>
<tr>
<td>Replication Service</td>
<td>9098</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional, Include Cluster Mgmt IP as well</td>
</tr>
<tr>
<td>NR Master for Coordination</td>
<td>8889</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional, Include Cluster Mgmt IP as well</td>
</tr>
<tr>
<td><strong>UCSM</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption etc.</td>
<td>443</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>CIMC OOB</td>
<td>Bidirectional for each UCS node</td>
</tr>
<tr>
<td>KVM</td>
<td>81</td>
<td>HTTP</td>
<td>User</td>
<td>UCSM</td>
<td>OOB KVM</td>
</tr>
<tr>
<td>KVM</td>
<td>743</td>
<td>HTTPS</td>
<td>User</td>
<td>UCSM</td>
<td>OOB KVM Encrypted</td>
</tr>
<tr>
<td><strong>Misc</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypervisor Service</td>
<td>9350</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional, Include Cluster Mgmt IP as well</td>
</tr>
<tr>
<td>CIP-M Failover</td>
<td>9097</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Bidirectional for each CVM to other CVMs</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Source</td>
<td>Destination</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>RPC Bind</td>
<td>111</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>CVM outbound to Installer</td>
</tr>
<tr>
<td>Installer</td>
<td>8002</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Installer</td>
<td>stDeploy makes connection, any request with uri /stdeploy</td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>8080</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>Any request with uri /auth/</td>
</tr>
<tr>
<td>Auth Service</td>
<td>8082</td>
<td>TCP</td>
<td>Each CVM Node</td>
<td>Each CVM Node</td>
<td>hxRoboControl deployments</td>
</tr>
<tr>
<td>syslog-ng</td>
<td>6514</td>
<td>TCP</td>
<td>CIMC from each node</td>
<td>Remote syslog-ng collector</td>
<td>Log aggregation</td>
</tr>
<tr>
<td>TLS</td>
<td>5696</td>
<td>TCP</td>
<td>CIMC from each node</td>
<td>KMS Server</td>
<td>Key Exchange</td>
</tr>
<tr>
<td>SED Cluster</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>Each CVM Mgmt IP inluding CIP-M</td>
<td>UCSM A/B and VIP</td>
<td>Policy Configuration</td>
</tr>
<tr>
<td>TLS</td>
<td>5696</td>
<td>TCP</td>
<td>CIMC from each node</td>
<td>KMS Server</td>
<td>Key Exchange</td>
</tr>
</tbody>
</table>

The following links are relevant specifically to ESXi and vCenter:

ESX 6.0 port requirements:  
https://kb.vmware.com/s/article/2106283

vCenter 6.0 Port requirements  
https://kb.vmware.com/s/article/2106283

Please note that the following ports are shown as open but not needed for installation or general operation:

TCP port 81: HTTP KVM direct to CIMC (UCSM credentials required)  
TCP port 743: HTTPS KVM direct to CIMC (UCSM credentials required)  
TCP port 8888: Storage data network port for file system rebuilds  
TCP port 843: UCS Central port on the FI for application integration  
Note the UDP ports 427 (Service Location Protocol) and 8125 (Graphite) are open on the SCVM. Ports 32k-65k are also open for SCVM outbound communication. These UDP ports can be seen in the IP Tables ACCEPT syntax above.
Appendix B: URLs Needed for Smart Call Home, Post Install Scripts, Intersight

**Smart Call Home (SCH):**

root@hx-6-s cvm-01:~# stcli services sch show
proxyPort: 8080
enableProxy: True
enabled: True
proxyPassword:
proxyUser:
cloudEnvironment: production
proxyUrl: proxy.esl.cisco.com
emailAddress: dummy_address@cisco.com
portalUrl:
cloudAsupEndpoint: https://diag.hyperflex.io/
root@hx-6-s cvm-01:~#

**Post Install:**

root@Cisco-HX-Installer-Appliance:~# vi /usr/share/springpath/storfs-misc/hx-scripts/update.sh
#!/bin/sh
FILENAME="hx-tools.zip"
URL="http://cs.co/hx-scripts"
cd /usr/share/springpath/storfs-misc/hx-scripts
wget --no-check-certificate -q -T1 -t1 $(URL) -O $(FILENAME) > /dev/null 2>&1
if [ $? -gt 0 ]; then
    echo "Could not download latest tools. Please verify internet connection"
    rm -f $(FILENAME) > /dev/null 2>&1
    exit 1
fi
unzip -oj $(FILENAME) > /dev/null 2>&1
rm -f $(FILENAME) > /dev/null 2>&1
echo "Scripts successfully updated"

**Intersight Device connector:** wss://svc.ucs-connect.com
## Appendix C: ESX Hardening Settings

ESX hardening settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi.apply-patches</td>
<td>Keep ESXi system properly patched</td>
<td>By staying up to date on ESXi patches, vulnerabilities in the hypervisor can be mitigated. An educated attacker can exploit known vulnerabilities when attempting to attain access or elevate privileges on an ESXi host.</td>
</tr>
<tr>
<td>ESXi.audit-exception-users</td>
<td>Audit the list of users who are on the Exception Users List and whether they have administrator privileges</td>
<td>In vSphere 6.0 and later, you can add users to the Exception Users list from the vSphere Web Client. These users do not lose their permissions when the host enters lockdown mode. Usually you may want to add service accounts such as a backup agent to the Exception Users list. Verify that the list of users who are exempted from losing permissions is legitimate and as needed per your environment. Users who do not require special permissions should not be exempted from lockdown mode.</td>
</tr>
<tr>
<td>ESXi.config-ntp</td>
<td>Configure NTP time synchronization</td>
<td>By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC), you can make it simpler to track and correlate an intruder’s actions when reviewing the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.</td>
</tr>
<tr>
<td>ESXi.config-persistent-logs</td>
<td>Configure persistent logging for all ESXi host</td>
<td>ESXi can be configured to store log files on an in-memory file system. This occurs when the host’s <code>/scratch</code> directory is linked to <code>/tmp/scratch</code>. When this is done only a single day’s worth of logs are stored at any time. In addition, log files will be reinitialized upon each reboot. This presents a security risk as user activity logged on the host is only stored temporarily and will not persistent across reboots. This can also complicate auditing and make it harder to monitor events and diagnose issues. ESXi host logging should always be configured to a persistent datastore.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ESXi.config-snmp</td>
<td>Ensure proper SNMP configuration</td>
<td>If SNMP is not being used, it should remain disabled. If it is being used, the proper trap destination should be configured. If SNMP is not properly configured, monitoring information can be sent to a malicious host that can then use this information to plan an attack. Note: ESXi 5.1 and later supports SNMPv3 which provides stronger security than SNMPv1 or SNMPv2, including key authentication and encryption.</td>
</tr>
<tr>
<td>ESXi.disable-mob</td>
<td>Disable Managed Object Browser (MOB)</td>
<td>The managed object browser (MOB) provides a way to explore the object model used by the VMkernel to manage the host; it enables configurations to be changed as well. This interface is meant to be used primarily for debugging the vSphere SDK. In Sphere 6.0 this is disabled by default.</td>
</tr>
<tr>
<td>ESXi.firewall-enabled</td>
<td>Configure the ESXi host firewall to restrict access to services running on the host</td>
<td>Unrestricted access to services running on an ESXi host can expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to only allow access from authorized networks.</td>
</tr>
<tr>
<td>ESXi.set-account-auto-unlock-time</td>
<td>Set the time after which a locked account is automatically unlocked</td>
<td>Multiple account login failures for the same account could possibly be a threat vector trying to brute force the system or cause denial of service. Such attempts to brute force the system should be limited by locking out the account after reaching a threshold. In case, you would want to auto unlock the account, i.e. unlock the account without administrative action, set the time for which the account remains locked. Setting a high duration for which account remains locked would deter and severely slow down the brute force method of logging in.</td>
</tr>
<tr>
<td>ESXi.set-account-lockout</td>
<td>Set the count of maximum failed login attempts before the account is locked out</td>
<td>Multiple account login failures for the same account could possibly be a threat vector trying to brute force the system or cause denial of service. Such attempts to brute force the system should be limited by locking out the account after reaching a threshold.</td>
</tr>
</tbody>
</table>

As per the guidelines: Ensure proper configuration and security settings are applied to the ESXi platform to harden it against potential threats.
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi.set-dcui-access</td>
<td>Set DCUI.Access to allow trusted users to override lockdown mode</td>
<td>Lockdown mode disables direct host access requiring that admins manage hosts from vCenter Server. However, if a host becomes isolated from vCenter Server, the admin is locked out and can no longer manage the host. If you are using normal lockdown mode, you can avoid becoming locked out of an ESXi host that is running in lockdown mode, by setting DCUI.Access to a list of highly trusted users who can override lockdown mode and access the DCUI. The DCUI is not running in strict lockdown mode.</td>
</tr>
<tr>
<td>ESXi.set-dcui-timeout</td>
<td>Audit DCUI timeout value</td>
<td>DCUI is used for directly logging into ESXi host and carrying out host management tasks. The idle connections to DCUI must be terminated to avoid any unintended usage of the DCUI originating from a left-over login session.</td>
</tr>
<tr>
<td>ESXi.set-password-policies</td>
<td>Establish a password policy for password complexity</td>
<td>ESXi uses the pam_passwdqc.so plug-in to set password strength and complexity. It is important to use passwords that are not easily guessed and that are difficult for password generators to determine. Password strength and complexity rules apply to all ESXi users, including root. They do not apply to Active Directory users when the ESX host is joined to a domain. Those password policies are enforced by AD.</td>
</tr>
<tr>
<td>ESXi.set-shell-interactive-timeout</td>
<td>Set a timeout to automatically terminate idle ESXi Shell and SSH sessions</td>
<td>If a user forgets to log out of their SSH session, the idle connection will remain open indefinitely, increasing the potential for someone to gain privileged access to the host. The ESXiShellInteractiveTimeOut allows you to automatically terminate idle shell sessions.</td>
</tr>
<tr>
<td>ESXi.set-shell-timeout</td>
<td>Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run</td>
<td>When the ESXi Shell or SSH services are enabled on a host they will run indefinitely. To avoid having these services left running set the ESXiShellTimeOut. The ESXiShellTimeOut defines a window of time after which the ESXi Shell and SSH services will automatically be terminated.</td>
</tr>
<tr>
<td>ESXi.TransparentPageSharing-intra-enabled</td>
<td>Ensure default setting for intra-VM TPS is correct</td>
<td>Acknowledgement of the recent academic research that leverages Transparent Page Sharing (TPS) to gain unauthorized access to data under certain highly controlled conditions and documents VMware’s precautionary measure of restricting TPS to individual virtual machines by default in upcoming ESXi releases. At this time, VMware believes that the published information...</td>
</tr>
</tbody>
</table>
VMs that do not have the `sched.mem.pshare.salt` option set cannot share memory with any other VMs.

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vCenter.verify-nfc-ssl</strong></td>
<td>Enable SSL for Network File copy (NFC)</td>
<td>NFC (Network File Copy) is the name of the mechanism used to migrate or clone a VM between two ESXi hosts over the network. <em><strong>By default, NFC over SSL is enabled (i.e.: &quot;True&quot;) within a vSphere cluster but the value of the setting is null.</strong></em> Clients check the value of the setting and default to not using SSL for performance reasons if the value is null. This behavior can be changed by ensuring the setting has been explicitly created and set to &quot;True&quot;. This will force clients to use SSL.</td>
</tr>
<tr>
<td><strong>VM.disable-console-copy</strong></td>
<td>Explicitly disable copy/paste operations</td>
<td>Copy and paste operations are disabled by default. However, if you explicitly disable this feature audit controls can check that this setting is correct.</td>
</tr>
<tr>
<td><strong>VM.disable-console-drag-n-drop</strong></td>
<td>Explicitly disable copy/paste operations</td>
<td>Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct. The default value is null. Setting this to true is just for audit.</td>
</tr>
<tr>
<td><strong>VM.disable-console-gui-options</strong></td>
<td>Explicitly disable copy/paste operations</td>
<td>Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct.</td>
</tr>
<tr>
<td><strong>VM.disable-console-paste</strong></td>
<td>Explicitly disable copy/paste operations</td>
<td>Copy and paste operations are disabled by default, however, if you explicitly disable this feature, audit controls can check that this setting is correct.</td>
</tr>
<tr>
<td>VM.disable-disk-shrinking-shrink</td>
<td>Disable virtual disk shrinking</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Shrinking a virtual disk reclaims unused space in it. The shrinking process itself, which takes place on the host, reduces the size of the disk's files by the amount of disk space reclaimed in the wipe process. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes—that is, users and processes without root or administrator privileges—within virtual machines have the capability to invoke this procedure. A non-root user cannot wipe the parts of the virtual disk that require root-level permissions. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature. Repeated disk shrinking can make a virtual disk unavailable. Limited capability is available to non-administrative users in the guest.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VM.disable-disk-shrinking-wiper</th>
<th>Disable virtual disk shrinking</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shrinking a virtual disk reclaims unused space in it. VMware Tools reclaims all unused portions of disk partitions (such as deleted files) and prepares them for shrinking. Wiping takes place in the guest operating system. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes—that is, users and processes without root or administrator privileges—within virtual machines have the capability to invoke this procedure. A non-root user cannot wipe the parts of the virtual disk that require root-level permissions. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature. Repeated disk shrinking can make a virtual disk unavailable. Limited capability is available to non-administrative users in the guest.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VM.disable-hgfs</th>
<th>Disable HGFS file transfers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certain automated operations such as automated tools upgrades use a component in the hypervisor called &quot;Host Guest File System&quot; and an attacker</strong></td>
<td></td>
</tr>
</tbody>
</table>
could potentially use this to transfer files inside the guest OS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Suggested Hardening</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.disconnect-devices-floppy</td>
<td>Disconnect unauthorized devices</td>
<td>Ensure that no device is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connected to a virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machine if it is not</td>
</tr>
<tr>
<td></td>
<td></td>
<td>required. For example, serial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and parallel ports are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rarely used for virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machines in a datacenter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>environment, and CD/DVD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>drives are usually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connected only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>temporarily during software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>installation. For less</td>
</tr>
<tr>
<td></td>
<td></td>
<td>commonly used devices that</td>
</tr>
<tr>
<td></td>
<td></td>
<td>are not required, either</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the parameter should not be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>present or its value must</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be FALSE. NOTE: The parameters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>listed are not sufficient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to ensure that a device is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usable; other required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>parameters specify how</td>
</tr>
<tr>
<td></td>
<td></td>
<td>each device is instantiated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any enabled or connected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>device represents a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>potential attack channel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When setting is set to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE, functionality is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disabled, however the device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>may still show up within</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the guest operation system.</td>
</tr>
<tr>
<td>VM.disconnect-devices-parallel</td>
<td>Disconnect unauthorized devices</td>
<td>Ensure that no device is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connected to a virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machine if it is not</td>
</tr>
<tr>
<td></td>
<td></td>
<td>required. For example, serial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and parallel ports are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rarely used for virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machines in a datacenter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>environment, and CD/DVD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>drives are usually</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connected only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>temporarily during software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>installation. For less</td>
</tr>
<tr>
<td></td>
<td></td>
<td>commonly used devices that</td>
</tr>
<tr>
<td></td>
<td></td>
<td>are not required, either</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the parameter should not be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>present or its value must</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be FALSE. NOTE: The parameters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>listed are not sufficient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to ensure that a device is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usable; other required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>parameters specify how</td>
</tr>
<tr>
<td></td>
<td></td>
<td>each device is instantiated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any enabled or connected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>device represents a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>potential attack channel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When setting is set to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE, functionality is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disabled, however the device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>may still show up within</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the guest operation system.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Details</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VM.disconnect-devices-serial</td>
<td>Disconnect unauthorized devices</td>
<td>Ensure that no device is connected to a virtual machine if it is not required. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE. NOTE: The parameters listed are not sufficient to ensure that a device is usable; other required parameters specify how each device is instantiated. Any enabled or connected device represents a potential attack channel. When setting is set to FALSE, functionality is disabled, however the device may still show up within the guest operation system.</td>
</tr>
<tr>
<td>VM.limit-setinfo-size</td>
<td>Limit informational messages from the VM to the VMX file</td>
<td>The configuration file containing these name-value pairs is limited to a size of 1MB. This 1MB capacity should be sufficient for most cases, but you can change this value if necessary. You might increase this value if large amounts of custom information are being stored in the configuration file. The default limit is 1MB; this limit is applied even when the sizeLimit parameter is not listed in the .vmx file. Uncontrolled size for the VMX file can lead to denial of service if the datastore is filled.</td>
</tr>
<tr>
<td>VM.prevent-device-interaction-connect</td>
<td>Prevent unauthorized removal, connection and modification of devices</td>
<td>In a virtual machine, users and processes without root or administrator privileges can connect or disconnect devices, such as network adaptors and CD-ROM drives, and can modify device settings. Use the virtual machine settings editor or configuration editor to remove unneeded or unused hardware devices. If you want to use the device again, you can prevent a user or running process in the virtual machine from connecting, disconnecting, or modifying a device from within the guest operating system. By default, a rogue user with non-administrator privileges in a virtual machine can: 1. Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive 2. Disconnect a network adaptor to isolate the</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VM.prevent-device-interaction-edit</td>
<td>Prevent unauthorized removal, connection and modification of devices</td>
<td>In a virtual machine, users and processes without root or administrator privileges can connect or disconnect devices, such as network adaptors and CD-ROM drives, and can modify device settings. Use the virtual machine settings editor or configuration editor to remove unneeded or unused hardware devices. If you want to use the device again, you can prevent a user or running process in the virtual machine from connecting, disconnecting, or modifying a device from within the guest operating system. By default, a rogue user with non-administrator privileges in a virtual machine can: 1. Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive 2. Disconnect a network adaptor to isolate the virtual machine from its network, which is a denial of service 3. Modify settings on a device</td>
</tr>
</tbody>
</table>
| VM.restrict-host-info     | Do not send host information to guests                                    | By enabling a VM to get detailed information about the physical host, an adversary could potentially use this information to inform further attacks on the host. If set to “True” a VM can obtain detailed information about the physical host. *The default value for the parameter is False but is displayed as Null. Setting to False is purely for audit purposes.*  
This setting should not be TRUE unless a particular VM requires this information for performance monitoring. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM.verify-network-filter</td>
<td>Control access to VMs through the dvfilter network APIs. An attacker might compromise a VM by making use of the dvFilter API. Configure only those VMs to use the API that need this access. This setting is considered an &quot;Audit Only&quot; guideline. If there is a value present, the admin should check it to ensure it is correct.</td>
</tr>
<tr>
<td>VM.verify-PCI-Passthrough</td>
<td>Audit all uses of PCI or PCIe passthrough functionality. Using the VMware DirectPath I/O feature to pass through a PCI or PCIe device to a virtual machine results in a potential security vulnerability. The vulnerability can be triggered by buggy or malicious code running in privileged mode in the guest OS, such as a device driver. Industry-standard hardware and firmware does not currently have sufficient error containment support to make it possible for ESXi to close the vulnerability fully. There can be a valid business reason for a VM to have this configured. This is an audit-only guideline. You should be aware of what virtual machines are configured with direct passthrough of PCI and PCIe devices and ensure that their guest OS is monitored carefully for malicious or buggy drivers that could crash the host.</td>
</tr>
<tr>
<td>vNetwork.limit-network-healthcheck</td>
<td>Enable VDS network healthcheck only if you need it. Network Healthcheck is disabled by default. Once enabled, the healthcheck packets contain information on host#, vds# port#, which an attacker would find useful. It is recommended that network healthcheck be used for troubleshooting, and turned off when troubleshooting is finished.</td>
</tr>
<tr>
<td>vNetwork.restrict-netflow-usage</td>
<td>Ensure that VDS Netflow traffic is only being sent to authorized collector IPs. The vSphere VDS can export Netflow information about traffic crossing the VDS. Netflow exports are not encrypted and can contain information about the virtual network making it easier for a MITM attack to be executed successfully. If Netflow export is required, verify that all VDS Netflow target IP's are correct.</td>
</tr>
<tr>
<td>vNetwork.restrict-port-level-overrides</td>
<td>Restrict port-level configuration overrides on VDS. Port-level configuration overrides are disabled by default. Once enabled, this allows for different security settings to be set from what is established at the Port-Group level. There are cases where particular VM's require unique configurations, but this should be monitored so it is only used when authorized. If overrides are not monitored, anyone who gains access to a VM with a less...</td>
</tr>
</tbody>
</table>
secure VDS configuration could surreptitiously exploit that broader access.

Appendix D: Acronym Glossary

AAA - authentication, authorization and accounting
AD – Active Directory
API – Application Programming Interface
CC – Common Criteria
CERT – Computer Emergency Response Team
CIMC – Cisco Integrated Management Console
CIP – Cluster IP (data)
CIP-M – Cluster IP Management
CIS – Center for Internet Security
CLI – Command Line Interface
CSDL – Cisco Secure Development Lifecycle
CVM – Control Virtual Machine
CMVP – Cryptographic Module Validation Program
CSR – Certificate Signing Request
DISA – Defense Information Systems Agency
DNS – Domain Name Service
DSM – Vormetric Data Security Manager
DRS – Distributed Resource Scheduler
EAL – Evaluation Assurance Level
FedRAMP – Federal Risk and Authorization Management Program
ESX - ESXi replaces Service Console (a rudimentary operating system) with a more closely integrated OS. ESX/ESXi is the primary component in the VMware Infrastructure software suite. The name ESX originated as an abbreviation of Elastic Sky X
FI – Fabric Interconnect
FIPS – Federal Information Processing Standard
FISMA -- Federal Information Security Management Act
FQDN – Fully Qualified Domain Name
HX/HXDP – HyperFlex/HyperFlex Data Platform
ISO – International Standards Organization
KMIP – Key Management Interoperability Protocol
KMS – Key Management Server
KVM – Keyboard Video Mouse
LAN – Local Area Network
MAC – Media Access Control (unique identifier)
NERC -- North American Electric Reliability Corporation Critical Infrastructure Protection
NTP – Network Time Protocol
OOB – Out of Band
POC – Proof of Concept
QoS – Quality of Service
REST – Representational State Transfer
RHEL – Red Hat Enterprise Linux
SCH – Smart Call Home
SCVM – Storage Control Virtual Machine
SED – Self Encrypting Drive
SL – Smart Licensing
SLP – Service Location Protocol
SNMP – Simple Network Monitoring Protocol
SSH – Secure Shell
SSL – Secure Sockets Layer
SSO – Single Sign On
STCLI – Storage Command Line Interface
TLS – Transport Layer Security
TPM – Trusted Platform Module
UCARP – Userland Common Address Redundancy Protocol
UCS – Unified Computing System
UCSM – UCS Manager
UI – User Interface
VLAN – Virtual Local Area Network
VM – Virtual Machine
vNIC – Virtual Network Interface Card
vWAAS – Virtual Wide Area Application Services (WAN acceleration device)
WAN – Wide area Network

Appendix E: Sample Syslog-ng Configuration File

Sample syslog-ng collection server configuration file. Note that HX defaults to port 6514 for syslog-ng traffic. The config file(s) below uses port 6515 for encrypted TLS transport. The default location for this file in Ubuntu is: `/etc/syslog-ng/syslog-ng.conf`

It is recommended to back up the original configuration file using the following:
`#> sudo cp /etc/syslog-ng/syslog-ng.conf /etc/syslog-ng/syslog-ng.conf.BAK`

Here is a sample syslog-ng.conf that works for TLS secure shipping. It imports configuration files from `/etc/syslog-ng/conf.d`

```
@version: 3.5
@include "scl.conf"
@include "$scl-root/system/tty10.conf"
```

kaptain@kaptain-syslog:/etc/syslog-ng$ cat syslog-ng.conf

Cisco HX Platform Hardening Guide
options {
    time-reap(30);
    mark-freq(10);
    keep-hostname(yes);
};
source s_local { system(); internal(); };
# source s_network {
#    syslog(transport(tcp) port(6514));
#};
# source tls_source {
#    network(ip(0.0.0.0) port(6515)
#        transport("tls")
#        tls( key-file("/etc/syslog-ng/cert.d/serverkey.pem")
#             cert-file("/etc/syslog-ng/cert.d/servercert.pem")
#             ca-dir("/etc/syslog-ng/ca.d")
#        ); }
#};
destination d_local {
    file("/var/log/syslog-ng/messages_${HOST}"); }
destination d_logs {
    file("/var/log/syslog-ng/logs-enc.txt"
        owner("root")
        group("root")
        perm(0777)
    );
    log { source(s_local); destination(d_logs); }
}

###
# Include all config files in /etc/syslog-ng/conf.d/
###
@include "/etc/syslog-ng/conf.d/"

kaptain@kaptain-syslog:/etc/syslog-ng/conf.d$ cat audit.conf
## Audit Logging Configuration ##
source demo_tls_src {
    tcp(ip(0.0.0.0) port(6515)
        tls{
            key-file("/etc/syslog-ng/cert.d/serverkey.pem")
            cert-file("/etc/syslog-ng/cert.d/servercert.pem")
            peer-verify(optional-untrusted)
        }
    );
}

filter f_auditor_rest { match("hx-audit-rest" value("MSGHDR")); }
filter f_device_conn { match("hx-device-connector" value("MSGHDR")); }
filter f_stssomgr { match("hx-stSSOMgr" value("MSGHDR")); }
filter f_ssl_access { match("hx-ssl-access" value("MSGHDR")); }
filter f_hxmanager { match("hx-manager" value("MSGHDR")); }
filter f_hx_shell { match("hx-shell" value("MSGHDR")); };
filter f_stcli { match("hx-stcli" value("MSGHDR")); };
filter f_hxcli { match("hx-cli" value("MSGHDR")); };

destination d_audit_rest { file("/var/log/syslog-ng/audit_rest.log"); };
destination d_device_conn { file("/var/log/syslog-ng/hx_device_connector.log"); };
destination d_stssomgr { file("/var/log/syslog-ng/stSSOMgr.log"); };
destination d_ssl_access { file("/var/log/syslog-ng/ssl_access.log"); };
destination d_hxmanager { file("/var/log/syslog-ng/hxmanager.log"); };
destination d_stcli { file("/var/log/syslog-ng/stcli.log"); };
destination d_hxcli { file("/var/log/syslog-ng/hxcli.log"); };

log { source(demo_tls_src); filter(f_audit_rest); destination(d_audit_rest); flags(final); };
log { source(demo_tls_src); filter(f_device_conn); destination(d_device_conn); flags(final); };
log { source(demo_tls_src); filter(f_stssomgr); destination(d_stssomgr); flags(final); };
log { source(demo_tls_src); filter(f_ssl_access); destination(d_ssl_access); flags(final); };
log { source(demo_tls_src); filter(f_hxmanager); destination(d_hxmanager); flags(final); };
log { source(demo_tls_src); filter(f_hx_shell); destination(d_hx_shell); flags(final); };
log { source(demo_tls_src); filter(f_stcli); destination(d_stcli); flags(final); };
log { source(demo_tls_src); filter(f_hxcli); destination(d_hxcli); flags(final); };

it would be possible to use the same system for both TCP and TLS log transport (for example, from 2 different systems). The files above have the TCP part commented out, but if you wanted to configure it you would just create one more file like audit.conf in /etc/syslog-ng/conf.d and name it something like audit_tcp.conf with the configuration as mentioned in the documentation. However, syslog-ng won't allow the same property / identifier name like 'demo_tls_src' (which would be the same in both TCP and TLS configurations above if the file was simply copied over) so it would need to be renamed (e.g., 'demo_tcp_src').