

WHITE PAPER – JANUARY 2017

FLEXPOD[®] DATACENTER VALIDATED ARCHITECTURE WITH VMWARE VSPHERE 6.0 FOR FEDRAMP 2.1

**SUITABILITY TO ASSIST AGENCIES AND CLOUD
SERVICE PROVIDERS IN FEDRAMP DEPLOYMENTS**

COALFIRE OPINION SERIES
FINAL VERSION 1.0



FlexPod[®] 
A Cisco and NetApp Solution

COALFIRESM



North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

Introducing FedRAMP	4
The NetApp and Cisco Converged Infrastructure Platform for FedRAMP (FlexPod® Datacenter Validated Architecture)	4
Objectives of This White paper.....	5
Links to FlexPod Datacenter and Other Reference Materials	6
Executive Overview of the Validated Architecture for FedRAMP	7
Coalfire Opinion Regarding the Suitability of the FlexPod Datacenter Validated Architecture for FedRAMP 2.1	7
Technical Details of the FlexPod Datacenter for FedRAMP	9
The Cloud Deployment model for the FlexPod DataCenter – General System Description / Function or Purpose.....	9
CSP and Tenant Architecture.....	9
Information System Components and Boundaries	10
System Environment – Hardware/Software/Network Inventories, Data Flows, and Services.....	14
Hardware Inventory	14
Software Inventory	14
Network Inventory	15
System Data Flow	15
Creation of a Lab Reference Instance For Testing	17
Reviewing the FlexPod Datacenter Lab Instance – The Coalfire Simulated Audit	18
Review Methods	18
FedRAMP “Moderate” NIST 800-53r4 Sections Not Reviewed.....	18
Observations and Findings.....	19
Access Control (AC).....	19
Audit and Accountability (AU)	22
Security Assessment and Authorization (CA)	25
Configuration Management (CM)	26
Contingency Planning (CP)	29
Identification and Authentication (IA)	30
Media Protection (MP).....	32
Risk Assessment (RA)	33
System and Services Acquisition (SA).....	35
System and Communications Protection (SC).....	36
System and Information Integrity (SI)	38

Other Observations (Other)	40
Summary of the Simulated Audit Findings.....	41
Coalfire Opinion	42
A Comment Regarding Regulatory Compliance	42

INTRODUCING FEDRAMP

The US Federal Risk and Authorization Management Program (FedRAMP) was created to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA) and to promote an accelerated adoption of secure cloud solutions by federal agencies.

The Office of Management and Budget now requires all executive federal agencies (and a number of de-facto adopters in other agencies and entities) to use FedRAMP to validate the security of cloud services. Leveraging the National Institute of Standards and Technology (NIST) 800-53 revision 4 standard, FedRAMP is the program that certifies that a cloud service provider (CSP) meets that standard.

Cloud Service Providers (CSP) desiring to sell services to a federal agency can take three paths to demonstrate FedRAMP compliance: earn a Provisional Authority to Operate (P-ATO) from the Joint Authorization Board (JAB); receive an Authority to Operate (ATO) from a federal agency; or work independently to develop a CSP Supplied Package that meets program requirements. Each of these paths requires a stringent technical review by the FedRAMP Program Management Office (PMO) and an assessment by an independent third-party organization that is accredited by the program.

FedRAMP authorizations are granted at three impact levels based on NIST guidelines—low, medium, and high. These levels rank the impact that the loss of confidentiality, integrity, or availability could have on an organization—low (limited effect), medium (serious adverse effect), and high (severe or catastrophic effect).

THE NETAPP AND CISCO CONVERGED INFRASTRUCTURE PLATFORM FOR FEDRAMP (FLEXPOD® DATACENTER VALIDATED ARCHITECTURE)

Introducing

FlexPod® Datacenter is a data center architecture that is predesigned and built on the Cisco Unified Computing System (Cisco UCS), Cisco Nexus switch family, and NetApp® Fabric-Attached Storage (FAS) systems. FlexPod is designed to run a multitude of virtualization solutions and be an ideal platform for enterprise workloads. Easily scaled up for greater performance and capacity by adding network, compute, and storage resources as needed, FlexPod can, like the name implies, truly be sized to fit the diverse objectives of real-world solutions. It can also be scaled out for both virtualized and non-virtualized environments that need multiple consistent deployments by rolling out additional FlexPod stacks.

FedRAMP objectives may be ideally suited to the FlexPod Datacenter solution for both implementation as a common element in a Cloud Service Provider (CSP) support infrastructure or as a reproducible “block” of compute, storage, and networking, specifically delivering workloads in a large-scale CSP deployment. Scale up and scale out flexibility is inherent in nearly all CSP missions, with key objectives of FedRAMP being reusability and leveraging established security in the CSP infrastructure. In fact, a FlexPod deployment for FedRAMP endeavors to support both workload and CSP infrastructure roles in a single Pod deployment.

This dual-role objective (CSP infrastructure with embedded workload) is the use-case we investigated in this review. It represents the most challenging objective, and is a very likely real-world scenario for actual CSPs.

FlexPod Datacenter Overview

Designed for non-disruptive operations (NDO), FlexPod Datacenter embodies redundant storage, compute, and network elements that have been constructed and orchestrated for the continuous uptime required by

CSPs. Virtualized infrastructures, which typically deliver a multitude of applications, each with diverse requirements for operations, software upgrade, scale-up, and scale-out during their lifecycle, pose a particularly difficult target for any converged infrastructure. FlexPod Datacenter provides true NDO for this objective through clever implementation of redundancy, use of the VMware vSphere 6 vMotion services, and a suite of tools to facilitate the processes.

The following diagram depicts the architecture of the FlexPod Datacenter, as reviewed:

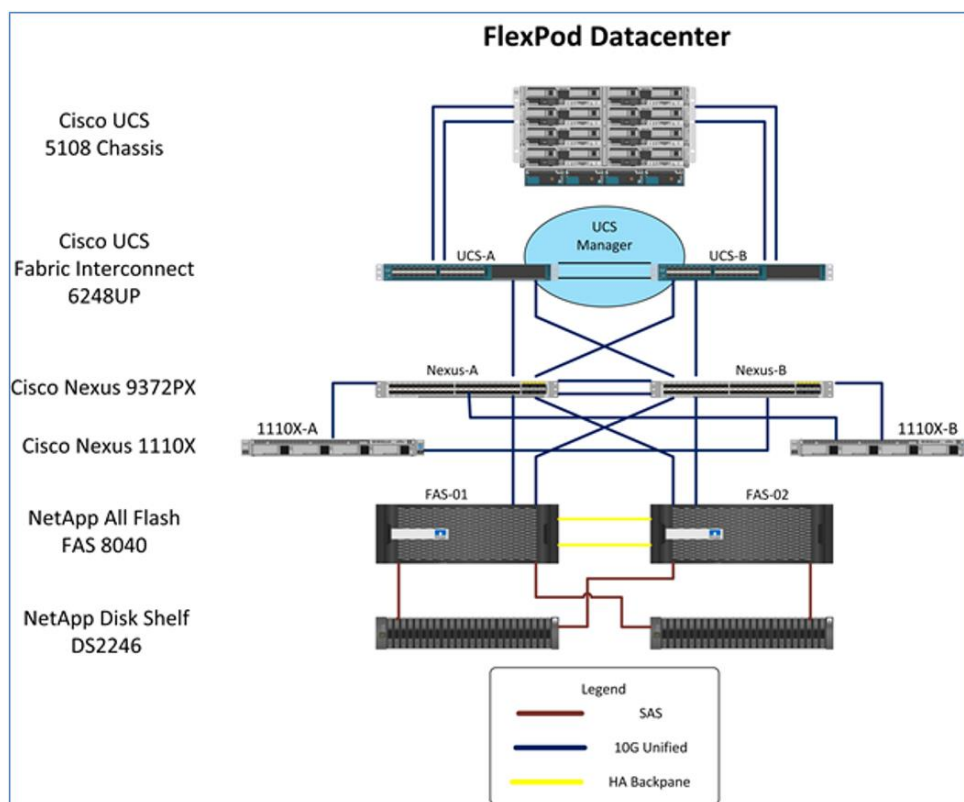


Figure 1 - FlexPod Datacenter Architecture Overview

Note: The Cisco Nexus 1110X is now end of sale. A Cisco Nexus 1000v software switch may be deployed in the Virtual Infrastructure without the Nexus 1110X switches or with the new replacement Cisco Cloud Services Platform 2100 deployed in a HA configuration.

OBJECTIVES OF THIS WHITE PAPER

The primary objective for this white paper is to render an opinion on the suitability of FlexPod Datacenter to assist Agencies (Tenant) and Cloud Service Providers (CSPs) in their FedRAMP deployments. It is the intent of the authors to use the following process to illustrate our findings and satisfy these objectives:

- State the CSP and Tenant objectives
- Provide an overview of FlexPod Datacenter
- Illustrate the specifics of our lab instance of FlexPod Datacenter
- Present the Hybrid Use Case for a conjoined CSP and Tenant in a single FlexPod
- Reveal our methodology
- Perform a FedRAMP “simulated audit”

- Document our findings on a per-control basis
- Make relevant statements about each Control Family and the particulars of the FlexPod implementation that may support meeting objectives of said control(s)
- State our opinion

Although the opinion itself may be helpful, this paper also contains a representative overview of many aspects of the FedRAMP process and program. It is a secondary objective of this white paper to inform a newcomer to FedRAMP the technical approach to using converged infrastructure to construct the CSP and Agency workloads.

A note regarding the use of the term “Validated”: NetApp and Cisco have introduced the phrases “... validated design” and “... (pre)validated architecture”, etc. to refer to their programs for rapid deployment using a factory-configured FlexPod Datacenter. Our review of FlexPod in this document is not an actual FedRAMP validation – the use of the term “Validated” refers only to the Cisco / NetApp program.

Since the review of the FlexPod Datacenter Validated Architecture was not being conducted on an actual FedRAMP CSP running an actual Agency workload, we only focused on the technical controls for FedRAMP “moderate” and did not review organizational processes, training, procedures, written supporting materials, nor other non-technical controls called out for in the NIST SP800-53r4-based guidance. Those controls only pertain to the actuality of an implementation for a real Agency/CSP workload.

Links to FlexPod Datacenter and Other Reference Materials

The joint Cisco and NetApp development of FlexPod Datacenter is supported by a wealth of detailed documentation, which defines and discloses significant technical details about the solution. It is out of the scope of this white paper to reproduce all but a tiny amount of this volume of material.

We recommend that you review this helpful reference material:

- 1) National Institute of Standards and Technology, U.S. Department of Commerce, Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Revision 4) is available at:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- 2) Federal Risk and Authorization Management Program (FedRAMP) official program website is found here: <https://www.fedramp.gov>
- 3) The Cisco FlexPod design zone site may be found here:
http://www.cisco.com/c/en/us/solutions/enterprise/data-center-designs-cloud-computing/landing_flexpod.html
- 4) NetApp Validated Designs for FlexPod are located at:
<http://www.netapp.com/us/solutions/flexpod/datacenter/validated-designs.aspx>
- 5) The NetApp Verified Architecture document depicting elements of the lab deployment and titled FlexPod Datacenter FedRAMP Readiness with VMware vSphere 6.0, HyTrust CloudControl and DataControl – NVA Design and Deployment is located here:
<http://www.netapp.com/us/media/nva-0031.pdf>
- 6) Coalfire Systems, Inc. corporate 3PAO FedRAMP site may be located at this URL:
<https://www.coalfire.com/Solutions/Audit-and-Assessment/FedRAMP>

EXECUTIVE OVERVIEW OF THE VALIDATED ARCHITECTURE FOR FEDRAMP

Our objective for this project was to review the FlexPod® Datacenter for efficacy to assist federal agencies and Cloud Service Providers in successful deployments using FlexPod.

In our assessment, we confirmed the NetApp designers' objectives to create a joint Cloud Service Provider (CSP) and Agency (Tenant) lab instance for our validation exercise. Noting this was a likely scenario for their FedRAMP customers and representative of a superset of the simpler "CSP only" and "Agency only" FlexPod workloads, we observed that the Tenant workload area would support the construction of a hypothetical three-tier (data-base, application, and web delivery) application base. Since this was a general simulation, no actual Agency application was hosted.

With advisory assistance from Coalfire Systems, NetApp constructed a laboratory instance of FlexPod Datacenter, running the VMware™ vSphere ESXi 6.0 and vCenter Servers™ with HyTrust's CloudControl® and DataControl® applications, which were used to enhance basic vSphere 6.0 and supply richer support for the intended NIST SP 800-53r4 "moderate" FedRAMP controls.

A simulated audit was performed on this laboratory build, which paralleled the Third Party Assessment Organization (3PAO) activities, to assess selected technical controls ("moderate" level Access Control (AC), Audit and Accountability (AU), Security Assessment and Authorization (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Media Protection (MP), Risk Assessment (RA), System and Services Acquisition (SA), System and Communications Protection (SC), and System and Information Integrity (SI) families). The simulated audit consisted of a combination of supplied Request for Information (RFI) material review and actual observation of consoles and configuration screens during several on-line review sessions conducted by Coalfire personnel on actions performed by NetApp security engineers and collected during WebEx sessions.

Coalfire then analyzed the findings, following the guidance provided by the FedRAMP "moderate" NIST control targets. Breaking the technical controls out by section, each control was assessed in the lab instance and determined to Support, Partially Support, or Not Support the FedRAMP baseline requirements.

One hundred seventeen (117) controls in the test instance were found to either Support or Partially Support the FedRAMP "moderate" baseline requirements. This represented approximately 42% (117 of 282) of the technical controls required for FedRAMP "moderate" baseline compliance. Please note: the lab validation instance was devoid of an actual application and of supporting services that would be present in the construction of a real CSP – many of the 165 remaining technical controls would be satisfied by including wireless networking, portable, or removable storage and mobile devices.

COALFIRE OPINION REGARDING THE SUITABILITY OF THE FLEXPOD DATACENTER VALIDATED ARCHITECTURE FOR FEDRAMP 2.1

It is the opinion of the authors that the FlexPod Datacenter solution as reviewed **is effective** in providing significant and substantial support for the objectives and requirements of both CSPs and federal agencies in pursuit of a FedRAMP "Ready" Product.

Our opinion is based on observations and analysis of the testing performed on the fall 2016 Research Triangle Park (RTP) North Carolina laboratory test instance of FlexPod Datacenter with VMware vSphere 6.0, HyTrust CloudControl and DataControl, as documented, configured, and reviewed against an objective FedRAMP 2.1 NIST-influenced "moderate" baseline. This opinion is also dependent on a number of underlying presumptions (caveats), which are enumerated in detail in the larger "Coalfire Opinion" section.

of this white paper, including: adherence to vendor best practices; hardening of configurations; presence of an actual (not hypothetical) workload; certain underlying CSP services being present; alignment of technical controls with actual CSP/Agency missions, roles, responsibilities, policies, procedures, baselines, mandates, etc.; physical and organizational controls; presence of staff at the CSP; actual federal agency users subscribing to an actual application/service; etc.

TECHNICAL DETAILS OF THE FLEXPOD DATACENTER FOR FEDRAMP

The FedRAMP authorization process requires that the Agencies and Cloud Service Providers supply written technical evidence of security compliance to their selected Third Party Assessment Organizations (3PAO) using a series of program authorized templates. This process is required for both the initial assessment (step 1 of 3) and the “Ongoing Assessment & Authorization” (step 3 of 3) used perpetually to maintain the FedRAMP authorization for continued operation.

In the document phase of this FedRAMP assessment process, one of the most crucial documents is the system specific instance of the *FedRAMP High/Moderate/Low System Security Plan* or SSP. Each intended FedRAMP product has its own SSP that contains technical details about the specific Agency/CSP system under assessment. In conjunction with a suite of other assessment documents (current templates may be found at <https://www.fedramp.gov/resources/templates-2016/>), the SSP informs the assessors and other FedRAMP entities about the technical security plan for the new system.

The following section contains a brief subset of information from a representative SSP (*Please note: this excerpt of the SSP is written in the present tense, indicating the state of systems at the moment in time the SSP was prepared*).

THE CLOUD DEPLOYMENT MODEL FOR THE FLEXPOD DATACENTER – GENERAL SYSTEM DESCRIPTION / FUNCTION OR PURPOSE

FlexPod Datacenter is a converged infrastructure solution, supporting the Platform as a Services (PaaS) cloud model, and is comprised of FlexPod Datacenter infrastructure running VMware vSphere virtualization software, HyTrust CloudControl and HyTrust DataControl software. This integrated environment provides secure data management capabilities to host multiple tenants that are completely isolated from each other.

CSP AND TENANT ARCHITECTURE

In order to create the most general architecture for validation and provide for a use case that can inform both Agency-centric and Cloud Service Provider-centric missions, the FlexPod Datacenter implementation is designed to simulate a likely CSP hosting an Agency. This case can represent many of the technical nuances common in both missions. Again, please note that no actual workload resides in the Agency tenant – it just provided for a typical three-tier virtualization platform that would be capable of hosting an actual Agency application.

The FlexPod Datacenter system provides all the storage, network, and compute resources that would be required to host multiple tenants. Secure isolation is provided in every layer of the solution stack to ensure that no tenant is aware of the presence of another tenant residing on the same physical infrastructure.

In addition to providing secure isolation, the data of the tenants is secured by encrypting the virtual machine data while at rest and in motion. The control over encryption and key management resides with the tenant and not the service provider, thus reducing chances of insider attacks from the service provider.

INFORMATION SYSTEM COMPONENTS AND BOUNDARIES

Depicted in the following diagram are the Information System components and logical boundaries to those components. Additional narrative on the details are provided in the section below.

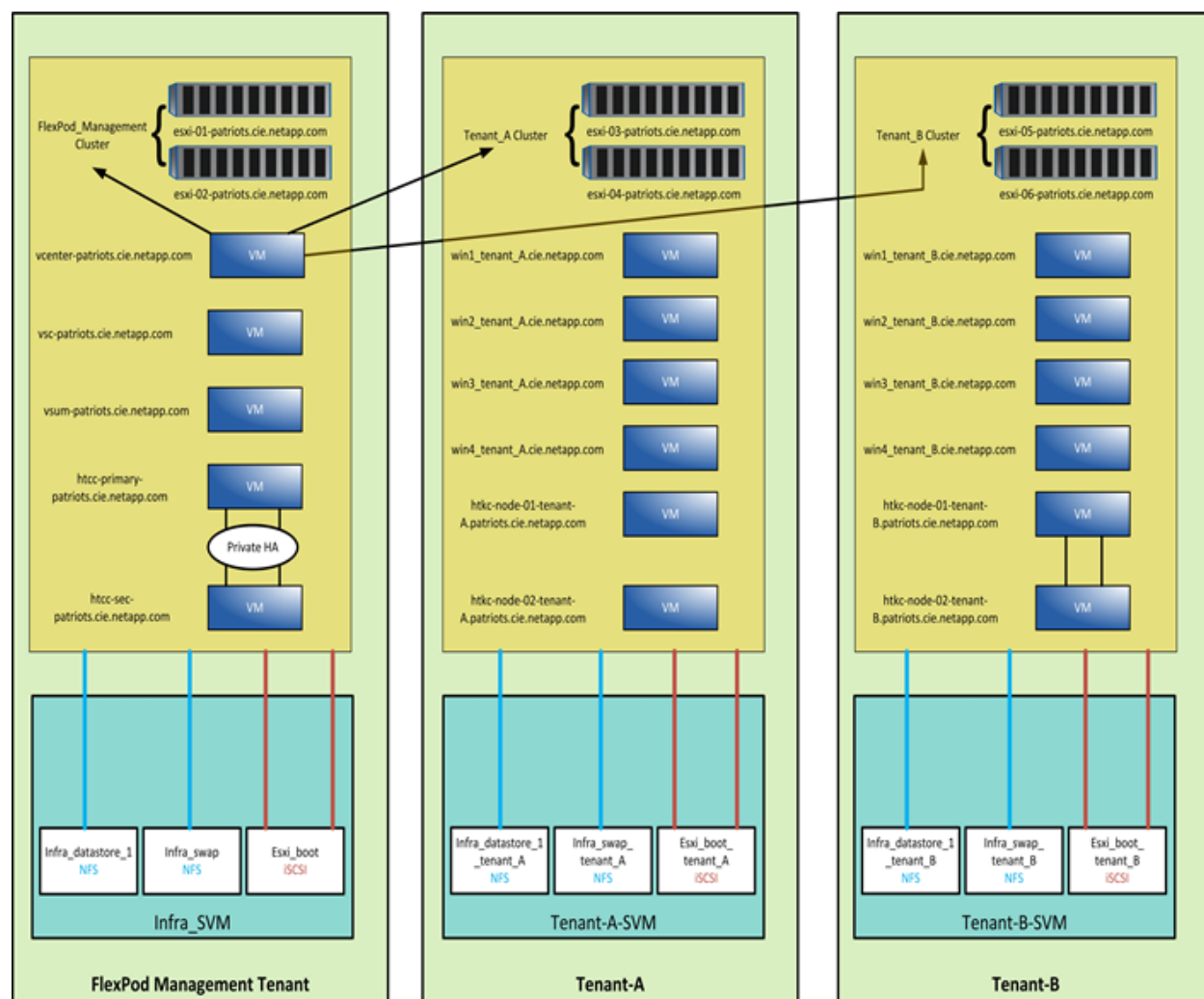


Figure 2 - FlexPod Datacenter Information Systems and Boundaries

These are the major components that comprise the Information System:

VMware vSphere

This information system uses VMware vSphere as the hypervisor platform. ESXi hosts are installed on Cisco UCS servers and a VMware vCenter server was deployed to manage the Virtual Infrastructure.

3 Virtual clusters were created and each cluster was provided by two ESXi servers. The clusters (in bold) were used for the purposes below:

FlexPod_Management Cluster – Hosts the virtual machines that are used to manage the overall infrastructure.

Tenant_A Cluster – Hosts the Virtual Machines belonging to Tenant-A. A few Windows Virtual Machines will be running within this cluster. A clustered instance of HyTrust KeyControl will be deployed within each tenant to handle VM disk encryption.

Tenant_B Cluster – Is a host to the Virtual Machines belonging to Tenant-B. A few Windows Virtual Machines will be running within this cluster. A clustered instance of HyTrust KeyControl will be deployed within each tenant to handle VM disk encryption.

The data stores created within each cluster/tenant are private to the tenant and will not be accessible from other ESXi hosts or Virtual Machines from a different cluster.

A Nexus 1000v distributed virtual switch is used to handle all the virtual machine networking. Dedicated port-groups and VMkernels are created to handle the data traffic of the VLANs that belong to the tenants.

NetApp FAS and Data ONTAP

NetApp Fabric Attached Storage (FAS) is the storage system that caters to all the data storage requirements of the tenants. Data ONTAP is the operating system of the storage hardware through which all storage configurations are setup.

In order to host multiple tenants, a storage feature called 'Storage Virtual Machines (SVM)' is used. A SVM is a logical storage controller that manages its own set of storage resources and access control. As part of our deployment, 3 SVMs are deployed on top of the physical storage system FAS – Tenant-A-SVM, Tenant-B-SVM, and the Infra-SVM -- which provides all resources needed for the management of the infrastructure.

Some of the important resources provided by the SVMs are Logical Data Volumes to store data, Data Interfaces to handle traffic, data access control to a required set of users and end-points, isolation from other SVMs, protocol support, etc.

The NetApp FAS storage is deployed as a two node active-active switchless cluster. When a node in the system fails, the surviving node will start to serve the data on behalf of the failed node. The two nodes referred to in this system are 'fas-01' and 'fas-02'. The storage cluster is referred to as 'fas'.

The protocols used to build this system are NFS and iSCSI. All three SVMs are configured to handle NFS and iSCSI traffic. Multiple NFS and iSCSI logical interfaces are created for handling the data traffic. Logical interfaces are assigned to different dedicated VLANs and those VLANs will not be routable to other VLANs. Thus, all the traffic within a VLAN will not be able to move to a different VLAN.

The FAS system is connected to a pair of Cisco Nexus switches in a multi-path configuration in order to provide data services to the applications residing in the virtual infrastructure.

Cisco Nexus 9000 Switches

The Cisco Nexus 9000 series switches are used as the backbone Layer 2 network infrastructure for the FlexPod Datacenter solution. A pair of Cisco Nexus switches are deployed in a multi-path configuration and are designed to handle traffic failover when a switch fails. Each switch defines its own network fabric – nexus-A ↔ Fabric-A and nexus-B ↔ Fabric-B. The configuration of both the switches is similar and the same set of VLANs and port-channels are created on both switches, which will facilitate failover of traffic.

The VLANs configured for a tenant's networking will not be routable; devices/end-points operating on a different VLAN will not be able to access it.

Each tenant is provided with a Management VLAN that would be uplinked to the core network; the Management VLANs of the tenants will not be able to communicate with each other, as they are restricted by modifying the access lists in the core network switch.

Cisco Unified Computing System (UCS)

The compute infrastructure for the FlexPod solution is provided by the UCS; the ESXi servers are installed on the UCS Blade servers. The UCS Manager is used to configure the entire compute infrastructure.

Two fabric interconnects, 'ucs-a' and 'ucs-b', are setup in a cluster configuration and the UCS Manager software runs on them. The Fabric Interconnects manage the underlying UCS Blades and Rack Mount servers.

The compute resources/UCS Blades are placed into logical containers called 'Organizations (Org)'. The 'Org' provides a granular view of how the resources are allocated to each tenant. Each 'Org' will maintain its own set of Service Profiles, which define how the blades should operate. The Service Profiles contain all information about the boot process, location of the boot OS, network interfaces for the OS, Multipathing, etc. If a UCS Blade is not associated to a Service Profile, it is a stateless device.

The service profiles are configured to provide High-Availability in the form of redundant adapters for both SAN and NAS traffic and also present multiple paths to the target devices via the Nexus 9000 switches.

Cisco Nexus 1110X

A pair of Cisco Nexus 1110X switches are deployed in a Primary/Secondary configuration. A Nexus 1000v instance is deployed as a distributed virtual switch (dvs) on them and is used to manage all the Virtual Infrastructure networking. A distributed port-group is assigned for each VLAN configured in the system and Uplink port-groups are created for all traffic segments that need to connect to the ESXi physical ports from the dvs.

HyTrust CloudControl (HTCC)

HyTrust CloudControl (HTCC) is deployed in the mapped mode and as a cluster configuration. In the mapped mode, all the hosts that need to be protected by HTCC are configured with a Published IP (PIP); this PIP is used by users/clients to access the hosts.

HTCC is deployed as a transparent proxy and sits between the users and all management interfaces to the protected hosts. From this central vantage point, it intercepts and logs all administrative requests coming via the PIP and enforces role-and resource-based policies that protect workloads from unauthorized access.

A private cluster network is setup on a dedicated VLAN for the HTCC cluster nodes to communicate with each other.

HTCC is integrated with an Active Directory/Domain instance to leverage the user identities and privileges extended to each user. In addition, HTCC provides its own set of access controls using the users that can be configured to have specific privileges in the Virtual Infrastructure space.

HyTrust DataControl (HTDC)

HyTrust DataControl provides encryption of Virtual Machine data while it is in motion and at rest. The main components of HyTrust DataControl are HyTrust KeyControl (HTKC) and Policy Agent.

The HTKC is deployed in a cluster configuration with two nodes within each tenant.

Each tenant controls its own clustered instance of HTKC to ensure that the encryption and management of encryption keys is handled by the tenant themselves. The service provider is not given any control over the encryption process, which reduces the chances of insider attacks.

HTDC will protect the Virtual Machines that are running on the same vSphere Cluster as the HTDC itself.

Active Directory/ Domain Services

Active Directory/Domain services are provided to the information system through an external source. The AD/DNS is not deployed within the FlexPod Infrastructure.

SYSTEM ENVIRONMENT – HARDWARE/SOFTWARE/NETWORK INVENTORIES, DATA FLOWS, AND SERVICES

Another element taken from the SSP is a comprehensive detailed report of all hardware, software, and network components used within the FedRAMP candidate system and a clear understanding of data flow and service delivery. Comprehensive and detailed information about the system environment is typically voluminous and is out scope for the nature of this document. This section includes a representative sample for the observed FlexPod Datacenter implementation.

Hardware Inventory

Principal hardware components for the tested FlexPod Datacenter include the following:

Table 1 - Hardware Component Inventory

COMPONENT	QUANTITY
NetApp All Flash FAS 8040	1 HA Pair
DS2246 Disk Shelves	2
SSD 800GB	48 Drives
Cisco Nexus Switches 9372PX	2
Cisco UCS Fabric Interconnects 6248UP	2
Cisco UCS 5108 Chassis	1
Cisco B200M4 Blades	6
Cisco VIC1340	1 per B200M4 Blade
Cisco Nexus 1110X	2

Software Inventory

In our NetApp RTP, NC laboratory instance of the FlexPod Datacenter for FedRAMP, the following software inventory was found:

Table 2 - Software Component Inventory

COMPONENT	VERSION
NetApp Data ONTAP Operating System	8.3.2P2
Cisco Nexus NX-OS	7.0(3)I1(3)
Cisco UCS Manager	3.1(1h)
Cisco eNIC	2.3.0.7
Cisco fNIC	1.6.0.25
VMware vSphere vCenter	6.0U1b
VMware vSphere ESXi	6.0U1b
NetApp Virtual Storage Console (VSC)	6.2
HyTrust Cloud Control	5.0
HyTrust Data Control	3.2.1
1000v	5.2(1)SV3(1.5b)

Network Inventory

The Cisco Nexus 9000 and 1110X series switches as constructed as part of the FlexPod infrastructure in our lab instance were:

Table 3 - Network Inventory

COMPONENT	QUANTITY
Cisco Nexus Switches 9372PX	2
Cisco Nexus 1110X	2

**Note: also listed above under the Hardware and Software Inventories*

System Data Flow

As another required part of the SSP, data flow within the FlexPod Datacenter architecture is depicted in the following illustration:

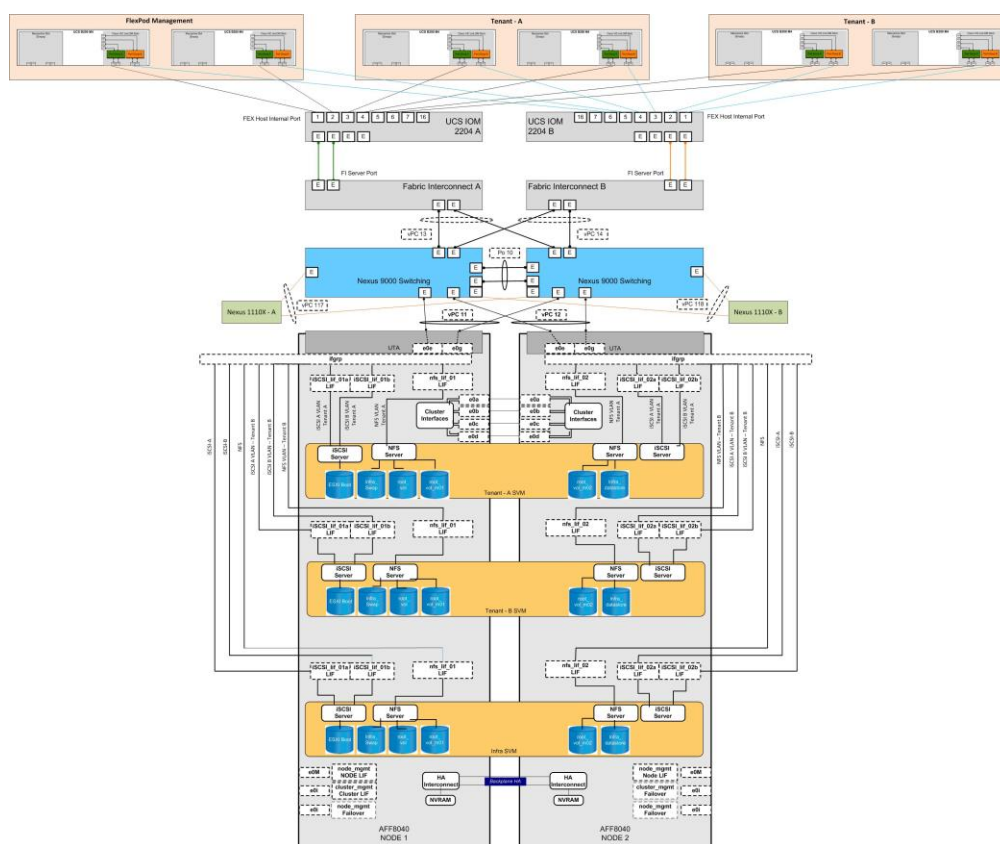


Figure 3 - FlexPod Datacenter Data Flow and Logical Components Interconnected for our Multi-tenant RTP Lab

The use of HyTrust CloudControl delivers extended policy segregation, isolating the CSP from tenants (A and B) for the purposes of management and Role-Based-Access-Control (RBAC). This resource permits the CSP to participate in gross infrastructure moves/adds/changes, while potentially disallowing management and control of the tenant workload.

This model is flexible enough to either permit or deny virtually any role for the CSP. In the most restrictive case, tenants entirely self-manage, enforced by CloudControl, and, in the most permissive case, the CSP may have joint control with their tenants. The following figure shows that relationship:

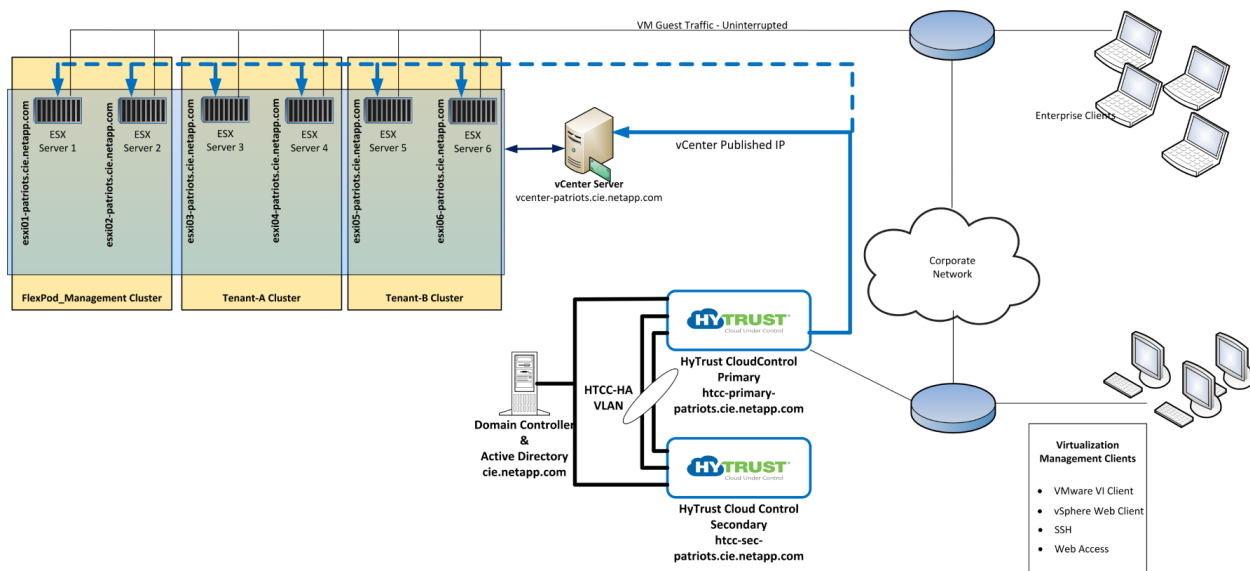


Figure 4 - HyTrust CloudControl Management and Data Relationship

HyTrust's DataControl is used for image management of the virtual machine images with support for encryption and, via Intel TXT/TPM extensions, support for geo-tagging and enforcement of geographic limitation on which data centers are permitted to operate specific tenant virtual machines. Although the on-board options for geo-tagging CPU support were not present in our RTP Lab instance, inclusion of these modules would be a trivial enhancement and a very useful feature for FedRAMP CSPs.

Encrypted Image support was tested and is reflected in this overview of Key Management data-flow and DataControl components:

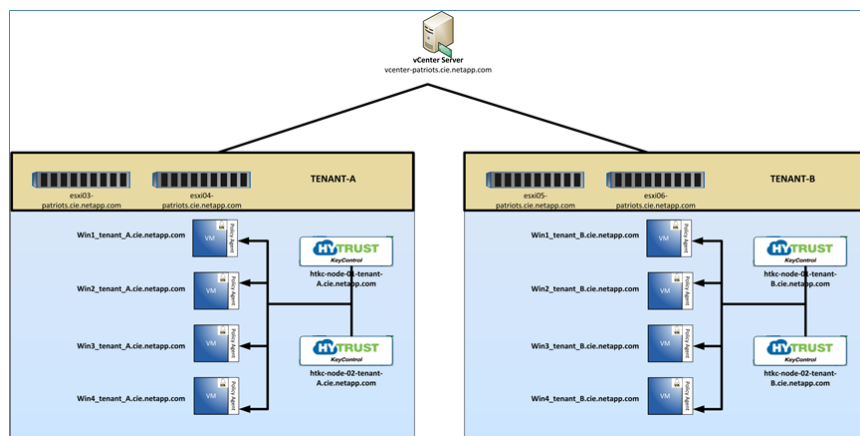


Figure 5 - HyTrust DataControl/Key Management Infrastructure

CREATION OF A LAB REFERENCE INSTANCE FOR TESTING

NetApp constructed a laboratory instance of FlexPod Datacenter, running the multiple VMware™ vSphere ESXi 6.0 hypervisors, VMware vCenter Server™, and HyTrust's CloudControl® and DataControl® applications, which were used to enhance basic vSphere 6.0 and supply richer support for NIST SP 800-53r4 FedRAMP 2.1 controls. Targeting specifically FedRAMP “Moderate” controls, NetApp’s lab deployment of the FlexPod consisted of the installation and refinement of a three tenant design – one tenant for the CSP and second and third tenants for the notional Agency workloads. Coalfire worked with NetApp to review and refine this design through a series of advisory engagements to help the NetApp lab team clarify their objectives and create the deployment in preparation for a simulated audit of the FlexPod Datacenter.



The lab was created in the NetApp RTP, NC facility in the United States and consisted of a FlexPod Datacenter converged infrastructure system with specifications provided earlier in this document.

Layered on top of the FlexPod Datacenter hardware was an installation of systems components for the VMware vSphere 6.0 suite and subsequent deployment of clusters, logical separation of storage and networking resources to prepare the three tenant (CSP, Tenant A, Tenant B) design. Added to the VMware ESXi hypervisor and vCenter Server platform were HyTrust's CloudControl and DataControl components.

This test lab instance of the FlexPod was restricted to single DNS support and isolated from the Internet (Edge) due to lab construction guidelines and policies at NetApp. This meant that access to this test instance was only possible through NetApp jump station facilities used for common access to the RTP lab. Although Internet access to/from the FlexPod was not configured in this particular lab instance, simple modification of access lists in the core network would enable this for a tenant if desired.

Asset naming for storage, compute, and networking elements was formulated specifically for this FedRAMP mission and designed to make clear illustration of purpose and function and be descriptive for the review process.

FlexPod includes a rigorous update management environment to create “locked” configurations where system software, firmware, and components are all kept to a “reference” standard. For this FedRAMP build, update management was a key objective and Cisco UCS Director with orchestration support, NetApp FAS storage management, and other components of the update management suite for FlexPod were used.

In preparation for testing, the FlexPod Datacenter was reviewed by Coalfire, and “gaps” in the design intent and actual deployment were corrected to ready the system for our simulated audit.

REVIEWING THE FLEXPOD DATACENTER LAB INSTANCE – THE COALFIRE SIMULATED AUDIT

In performance of the simulated audit, selected technical controls (see the “Objective of the White Paper” section above) from the Access Control (AC), Audit and Accountability (AU), Security Assessment and Authorization (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Media Protection (MP), Risk Assessment (RA), System and Services Acquisition (SA), System and Communications Protection (SC), and System and Information Integrity (SI) families were investigated. Our method consisted of a combination of supplied Request for Information (RFI) material review and actual observation of consoles and configuration screens as revealed during several on-line review sessions performed using WebEx. To conduct the on-line review sessions, NetApp engineers navigated to particular areas of investigation shown on management and reporting consoles using remote access technologies, while the Coalfire reviewer collected confirmation details by capturing screen-shots of the key information for the control being investigated. Some of this material is presented in the Observations and Findings section of this white paper.

REVIEW METHODS

Coalfire then analyzed the findings, following the guidance provided by the FedRAMP Moderate System Security Plan (SSP) Template (in raw form and in a “...FlexPod Datacenter ... version 8”), FedRAMP Revision 4 Annual Assessment Controls Template, and other “best practice” materials. Breaking the technical controls out by section, each control (for instance CM-2(2), *Configuration Management/Baseline Configuration, Automation Support for Accuracy/Currency*) was assessed in the lab instance and determined to support (solid Harvey Ball ‘●’), partially support (half-full Harvey Ball ‘◐’), not support (red empty Harvey Ball ‘○’), or does not apply to (blank) the desired control. Within each control family in the Coalfire Observations and Findings, specific comments are also included to make statements about assumptions, nuances of the collected materials, or other noteworthy items.

FedRAMP “Moderate” NIST 800-53r4 Sections Not Reviewed

Without the presence of an actual CSP or Agency, a number of controls are infeasible due to the absence of an application, a risk-avoidance posture, policies, procedures, staff, management, a facility, etc. Our simulated audit will have a number of categories that cannot be assessed nor validated. These include:

Awareness and Training (AT), Incident Response (IR), Maintenance (MA), Physical and Environmental Protection (PE), Planning (PL), and Personnel Security (PS), having these controls:

Table 4 - Control Families Not Reviewed and Control Counts

CONTROL FAMILY	CONTROL FAMILY NAME	TOTAL CONTROLS	TECH CONTROLS
AT	Access Control Policy and Procedures	5	3
IR	Incident Response	18	11
MA	Maintenance	11	9
PE	Physical and Environmental Protection	20	19
PL	Planning	6	4
PS	Personnel Security	9	8

The simulated audit will focus solely on technical controls that were present in the laboratory build of the FlexPod Datacenter instance.

Within the examined controls sections, several of non-technical controls are listed in the tables. Control number 1 of each family (for instance, AC-1, *Access Control Policies and Procedures*) always references a non-technical control to assess the presence of appropriate policies and procedures for that control family. It is noted as “Non-tech” in our validation tables, but included for completeness.

OBSERVATIONS AND FINDINGS

We have focused on control families that have one or more technical controls and included them in this section. Each control family is described and followed by a table of our findings. The FedRAMP guidance for test procedures and the ID, Control Names, and other information were derived from the May 20, 2016 workbook titled, [FedRAMP-Moderate-Test-Workbook-2016-05-20-v03-00.xlsx](https://www.fedramp.gov/resources/templates-2016/), which is available at <https://www.fedramp.gov/resources/templates-2016/>.

At the top of each Findings table, on the row listing the control family name, the respective control total depicts the number of technical controls available for testing within each family.

This Key, using Harvey Balls (see: https://en.wikipedia.org/wiki/Harvey_Balls) describes the meaning of the “FedRAMP Moderate” column for each control in each table:

Supported	(Solid ‘●’)
Partially Supported	(Half ‘◐’)
Not Supported	(Empty ‘○’)
Does Not Apply	(blank ‘ ’)
Non-Technical Control	(as ‘Non-tech’)

Key for FedRAMP Moderate Controls

Access Control (AC)

The Access Control (AC) Control family is described as “Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.” Our assessment under this family pertains to the technical controls, which represent 42 of the 43 controls in this family.

Findings for AC

Table 5 - AC Controls Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Access Control (AC)	42
AC-1	Access Control Policy and Procedures	Non-tech
AC-2	Account Management	●
AC-2 (1)	Account Management Automated System Account Management	
AC-2 (2)	Account Management Removal of Temporary / Emergency Accounts	●
AC-2 (3)	Account Management Disable Inactive Accounts	◐
AC-2 (4)	Account Management Automated Audit Actions	●

AC-2 (5)	Account Management Inactivity Logout	●
AC-2 (7)	Account Management Role-Based Schemes	●
AC-2 (9)	Account Management Restrictions on Use of Shared Groups / Accounts	◐
AC-2 (10)	Account Management Shared / Group Account Credential Termination	●
AC-2 (12)	Account Management Account Monitoring / Atypical Usage	●
AC-3	Access Enforcement	◐
AC-4	Information Flow Enforcement	◐
AC-4 (21)	Information Flow Enforcement Physical / Logical Separation of Information Flows	●
AC-5	Separation of Duties	●
AC-6	Least Privilege	●
AC-6 (1)	Least Privilege Authorize Access to Security Functions	●
AC-6 (2)	Least Privilege Non-Privileged Access for Nonsecurity Functions	◐
AC-6 (5)	Least Privilege Privileged Accounts	●
AC-6 (9)	Least Privilege Auditing Use of Privileged Functions	●
AC-6 (10)	Least Privilege Prohibit Non-Privileged Users from Executing Privileged Functions	◐
AC-7	Unsuccessful Logon Attempts	●
AC-8	System Use Notification	◐
AC-10	Concurrent Session Control	●
AC-11	Session Lock	
AC-11 (1)	Session Lock Pattern-Hiding Displays	
AC-12	Session Termination	◐
AC-14	Permitted Actions Without Identification or Authentication	
AC-17	Remote Access	●
AC-17 (1)	Remote Access Automated Monitoring / Control	●
AC-17 (2)	Remote Access Protection of Confidentiality / Integrity Using Encryption	●
AC-17 (3)	Remote Access Managed Access Control Points	●
AC-17 (4)	Remote Access Privileged Commands / Access	◐
AC-17 (9)	Remote Access Disconnect / Disable Access	◐
AC-18	Wireless Access	
AC-18 (1)	Wireless Access Authentication and Encryption	
AC-19	Access Control For Mobile Devices	
AC-19 (5)	Access Control For Mobile Devices Full Device / Container-Based Encryption	
AC-20	Use of External Information Systems	
AC-20 (1)	Use of External Information Systems Limits on Authorized Use	
AC-20 (2)	Use of External Information Systems Portable Storage Devices	
AC-21	Information Sharing	◐
AC-22	Publicly Accessible Content	

Comments regarding the AC Family

During the assessment process, several noteworthy observations were obtained, particularly around the integration of the HyTrust CloudControl suite and the improvements to basic VMware vSphere management. For example, control AC-2(7), *Account Management | Role-Based Schemes* was supported for clean segregation of the CSP and tenant roles. A sample screenshot is below, which shows an attempt by a tenant to construct a Virtual Machine on a resource they did not have access to:

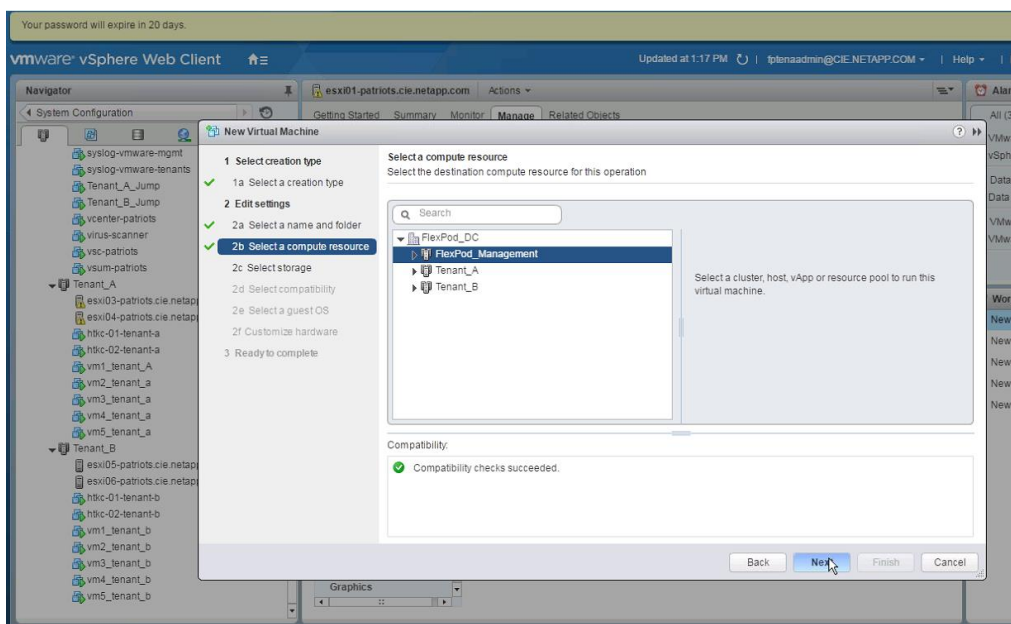


Figure 6 - Attempt by Tenant A to Create VM on Management Cluster...

This was followed up by a 'Permission denied...' dialogue when attempting to complete the creation.

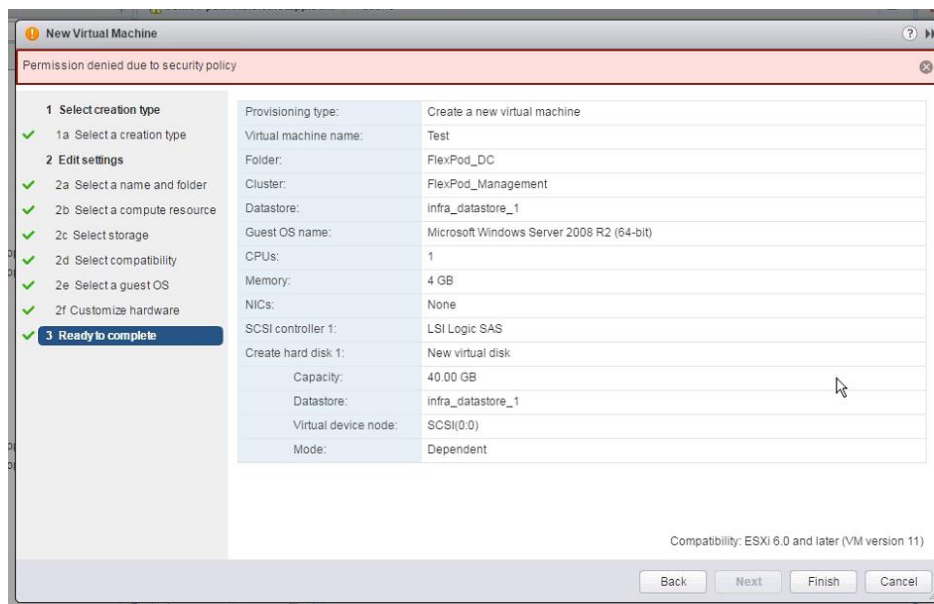


Figure 7 - ... and subsequent failure due to RBAC enforcement

Audit and Accountability (AU)

The Audit and Accountability (AU) Control family is described as “Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.” In this family, 17 technical controls are reviewed of the 19 total controls.

Findings for AU

Our test environment did not contain a Security Information and Event Management (SIEM) platform, which would be a traditional component in a true CSP and workload environment; so, at best, partial support for a FedRAMP control would be the greatest possible outcome. We were able to view syslog information through a built-in system logging server, which was integrated with the management, infrastructure, VMware, and HyTrust elements. We observed those logs to determine capabilities in this control family.

Table 6 - AU Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Audit and Accountability (AU)	17
AU-1	Audit and Accountability Policy and Procedures	Non-tech
AU-2	Audit Events	●
AU-2 (3)	Audit Events Reviews and Updates	●
AU-3	Content of Audit Records	●
AU-3 (1)	Content of Audit Records Additional Audit Information	●
AU-4	Audit Storage Capacity	
AU-5	Response to Audit Processing Failures	
AU-6	Audit Review, Analysis, and Reporting	
AU-6 (1)	Audit Review, Analysis, and Reporting Process Integration	
AU-6 (3)	Audit Review, Analysis, and Reporting Correlate Audit Repositories	
AU-7	Audit Reduction and Report Generation	●
AU-7 (1)	Audit Reduction and Report Generation Automatic Processing	●
AU-8	Time Stamps	●
AU-8 (1)	Time Stamps Synchronization with Authoritative Time Source	●
AU-9	Protection of Audit Information	●
AU-9 (2)	Protection of Audit Information Audit Backup on Separate Physical Systems / Components	
AU-9 (4)	Protection of Audit Information Access by Subset of Privileged Users	●
AU-11	Audit Record Retention	Non-tech
AU-12	Audit Generation	●

Noteworthy Comments on the AU Control Family

As mentioned, absence of a SIEM system removes review, analysis, and reporting functionality from the environment and, as a result, controls for AU-6 were not evaluated. No set-aside mechanisms were

constructed in the lab instance for audit storage, as a discrete resource and for automatic detection of audit failures, and resulted in AU-4 and AU-5 being reviewed as Does Not Apply.

In our test data collection, we relied on audit logs for confirmation of many of the other controls. For example, a HyTrust created Cloud VM Set for Tenant A, in this environment, generated the following HyTrust event, which was evident through this console view of this filtered event:



Figure 8 - Screenshot of HyTrust Audit Log Event

The HyTrust log below contained more complete and generic information, with appropriate user access tracking:

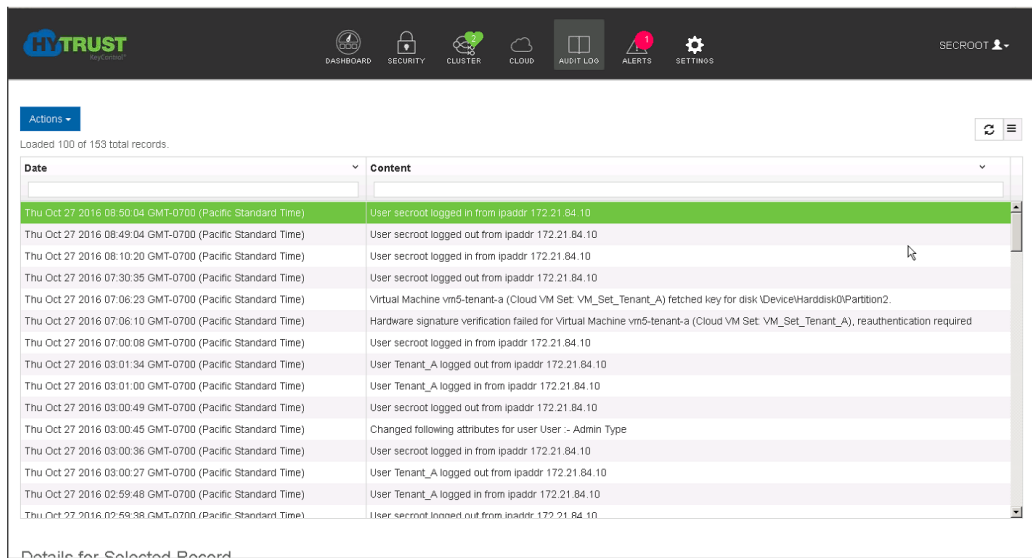
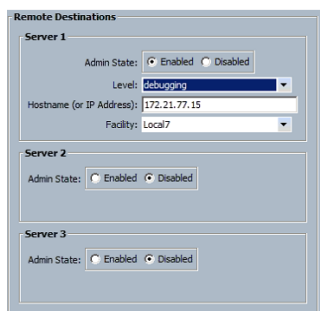


Figure 9 - Additional Audit Log Example of User Activity

Lastly, representative of the complete logging potential for the CSP is shown in this final example of the Cisco UCS Systems Manager integration into the logging process, shown in the two screen captures:



This screen shows the management tuning for logging that is available for Cisco UCS:

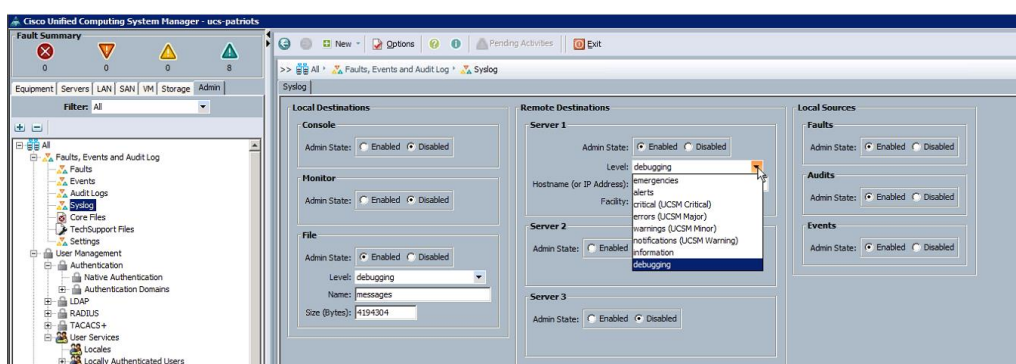


Figure 10 - Cisco UCS Logging Configuration Examples

Although lacking complete SIEM functionality, the Syslog VM, running Syslog Watcher, did support some rudimentary trending and analytical functions, which facilitated local analysis and remote support for the logging process and HyTrust's Audit Logging.

Received	Source IP	Source Name	Facility	Severity	Timestamp	Tag	Origin	Message
10/27/2016 8:11:17.114 AM	172.21.77.50	htcc-primary-patriots	local 5	Notice	Oct 27 15:11:11		htcc-prima...	HA Sync finished
10/27/2016 8:01:18.289 AM	172.21.77.50	htcc-primary-patriots	local 5	Notice	Oct 27 15:01:12		htcc-prima...	HA Sync finished
10/27/2016 7:51:19.791 AM	172.21.77.50	htcc-primary-patriots	local 5	Notice	Oct 27 14:51:14		htcc-prima...	HA Sync finished
10/27/2016 7:41:20.233 AM	172.21.77.50	htcc-primary-patriots	local 5	Notice	Oct 27 14:41:14		htcc-prima...	HA Sync finished
10/27/2016 7:31:18.553 AM	172.21.77.50	htcc-primary-patriots	local 5	Notice	Oct 27 14:31:13		htcc-prima...	HA Sync finished
10/27/2016 7:21:19.540 AM	172.21.77.50	htcc-primary-patriots	local 5	Notice	Oct 27 14:21:14		htcc-prima...	HA Sync finished

Figure 11 - Syslog Watcher Console Example for AU Control Family Support






Security Assessment and Authorization (CA)

The description of the Security Assessment and Authorization (CA) control family is “Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.” Comprising a total of 15 controls, CA has 8 technical controls amenable to the assessment for compliance.

Findings for CA

Non-technical assessment is the domain of CA-1, CA-2(1), CA-2(3), CA-3, CA-7(1), CA-8(1), and CA-9 and is not reviewed on our FlexPod Datacenter test instance.

Table 7 - CA Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Security Assessment and Authorization (CA)	8
CA-1	Security Assessment and Authorization Policies and Procedures	Non-tech
CA-2	Security Assessments	
CA-2 (1)	Security Assessments Independent Assessors	Non-tech
CA-2 (2)	Security Assessments Specialized Assessments	
CA-2 (3)	Security Assessments External Organizations	Non-tech
CA-3	System Interconnections	Non-tech
CA-3 (3)	System Interconnections Unclassified Non-National Security System Connections	
CA-3 (5)	System Interconnections Restrictions on External Network Connections	
CA-5	Plan of Action and Milestones	
CA-6	Security Authorization	
CA-7	Continuous Monitoring	
CA-7 (1)	Continuous Monitoring Independent Assessment	Non-tech
CA-8	Penetration Testing	
CA-8 (1)	Penetration Testing Independent Penetration Agent or Team	Non-tech
CA-9	Internal System Connections	Non-tech

CA Family Comments

Controls under the Security Assessment family category (CA-2 and CA-2(2)) were addressed partially only because of the absence of an actual workload operating on the lab instance. It should be noted that the tools provided by HyTrust CloudControl support both the Security Assessment roles, under the RBAC definitions, and tools for some aspects of Specialized Assessments. A comprehensive assessment suite is out of scope for the tool, however.

Configuration Management (CM)

The Configuration Management (CM) control family is described as “Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.” 25 of the 26 required FedRAMP “moderate” controls are technical and, as such, are subject to our assessment.

CM Findings

Except for CM-1, the Policy and Procedure control, the remaining controls deal with environment and configuration baselines, change control mechanisms, configurations, inventories, software usage control for systems, and user-installation. As with previous control families, the absence of an actual Agency application in Tenant A/B removes several controls from being open to assessment. Those controls are noted by a blank.

Table 8 - CM Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Configuration Management (CM)	25
CM-1	Configuration Management Policy and Procedures	Non-tech
CM-2	Baseline Configuration	●
CM-2 (1)	Baseline Configuration Reviews and Updates	◐
CM-2 (2)	Baseline Configuration Automation Support for Accuracy / Currency	●
CM-2 (3)	Baseline Configuration Retention of Previous Configurations	◐
CM-2 (7)	Baseline Configuration Configure Systems, Components, or Devices for High-Risk Areas	◐
CM-3	Configuration Change Control	●
CM-4	Security Impact Analysis	
CM-5	Access Restrictions for Change	●
CM-5 (1)	Access Restrictions for Change Automated Access Enforcement / Auditing	●
CM-5 (3)	Access Restrictions for Change Signed Components	
CM-5 (5)	Access Restrictions for Change Limit Production / Operational Privileges	●
CM-6	Configuration Settings	●
CM-6 (1)	Configuration Settings Automated Central Management / Application / Verification	●
CM-7	Least Functionality	
CM-7 (1)	Least Functionality Periodic Review	
CM-7 (2)	Least Functionality Prevent Program Execution	◐
CM-7 (5)	Least Functionality Authorized Software / Whitelisting	
CM-8	Information System Component Inventory	●
CM-8 (1)	Information System Component Inventory Updates During Installations / Removals	●
CM-8 (3)	Information System Component Inventory Automated Unauthorized Component Detection	●

CM-8 (5)	Information System Component Inventory No Duplicate Accounting of Components	●
CM-9	Configuration Management Plan	
CM-10	Software Usage Restrictions	
CM-10 (1)	Software Usage Restrictions Open Source Software	
CM-11	User-Installed Software	◐

Comments on the CM Family Findings

The lab test instance had several observed occurrences of CM-2 *Baseline Configuration* control application, including hypervisor hardening and Virtual Machine images created from “reference grade” system installation masters.

Configuration change management and control was reviewed in several areas with examples of platform configuration management, policy-based Virtual Machine management, and other examples here:

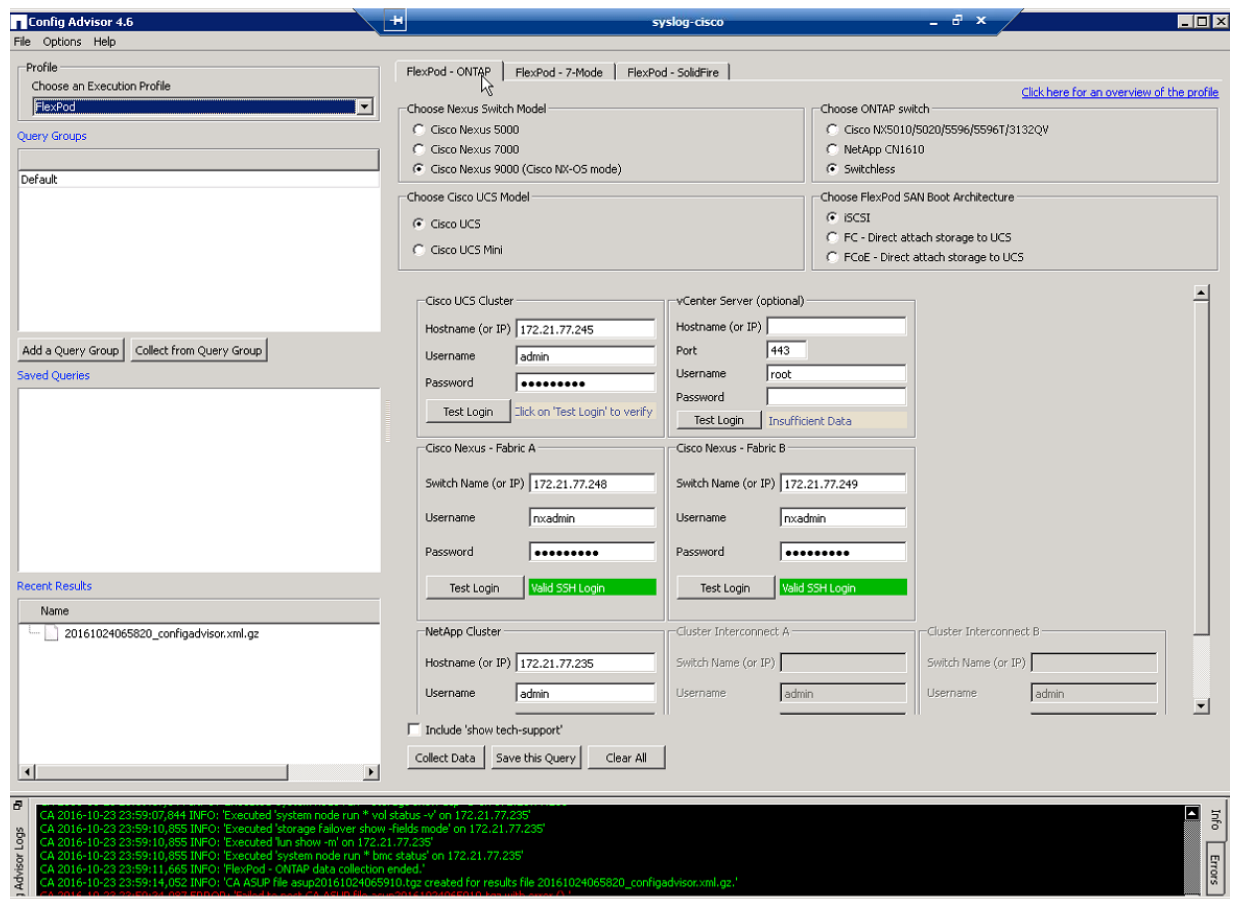


Figure 12 - NetApp Config Advisor for Networking, UCS and Storage Control

The powerful Config Advisor tool was also capable of determining out-of-compliance configurations that varied from desired baselines, suggesting recommended remediation actions, and performing ad-hoc or automated compliance checks for the entire FlexPod Datacenter.

Config Advisor 4.5 (FlexPod Results) - ASFEndToEnd.xml.gz

Infrastructure	Components	Running Firmware	Recommended Firmware
Hypervisor	Host OS	✓ VMware ESXi 6.0.0	VMware ESXi 6.0
Compute	Cisco UCS HBA enic Firmware	✓ 2.1.2.38	2.1.2.71
	Cisco UCS HBA fnic Firmware	✗ 1.5.0.45-3vmw	1.6.0.24
	Cisco UCS Manager	✗ 2.2(6)	2.2(5)
Network	Cisco NX-OS	✓ 7.1(1)N1(1)	7.2(1)N1(1)
Storage	NetApp Clustered Data ONTAP	✓ 8.3.1P1	8.3.1

As per NetApp Interoperability Matrix Tool, running configuration is not supported. Refer 'Recommended Firmware' column for the supported firmware matrix.

Configuration Check Profile : FlexPod - End-to-End FCoE

Filters: All Devices Only Selected Devices Dashboard Failures

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
High	FlexPod FC Zoning Storage Check	SP-ASF01 (Cluster)	Ensures that FC zones are configured correctly.	Storage Virtual Machine 'ASF-SVM01' LUN 'ESXUNCLPROD01' is mapped to groups [CLUSTER_vmware_PRODUCION_ig, Commvault_windows_MA_ig], multiple groups are mapped to same boot LUN.	
High	FlexPod FC Zoning Storage Check	SP-ASF01 (Cluster)	Ensures that FC zones are configured correctly.	Storage Virtual Machine 'ASF-SVM01' LUN 'ESXUNCLPROD02' is mapped to groups [CLUSTER_vmware_PRODUCION_ig, Commvault_windows_MA_ig], multiple groups are mapped to same boot LUN.	

Figure 13 - FlexPod Datacenter Firmware Compliance Check Report

Policy-based enforcement of trusted CM-7(2), *Least Functionality | Prevent Program Execution* was exhibited in this example of using Trusted Publisher AD settings in the test instance:

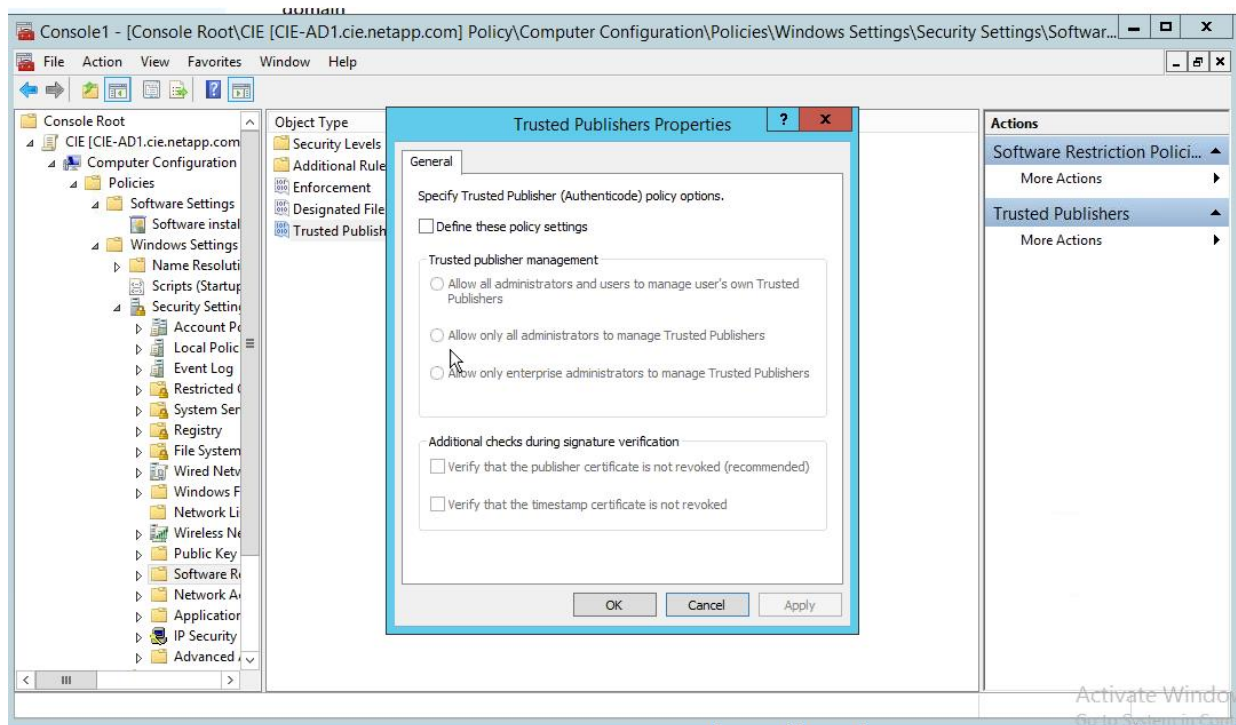


Figure 14 - User of Trusted Publisher Policy Enforcement


Contingency Planning (CP)

FedRAMP's Contingency Planning (CP) control family, described as "Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations", has a total of 15 of the 24 required FedRAMP "moderate" controls, all of which are technical.

CP Findings

Because of the absence of actual planning for contingency sites, alternate locations for storage and processing, existing telecom services and backup subsystems, only the availability of managed VMware VM snapshots could be verified for this control family.

Table 9 - CP Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Contingency Planning (CP)	15
CP-1	Contingency Planning Policy and Procedures	Non-tech
CP-2	Contingency Plan	
CP-2 (1)	Contingency Plan Coordinate With Related Plans	Non-tech
CP-2 (2)	Contingency Plan Capacity Planning	Non-tech
CP-2 (3)	Contingency Plan Resume Essential Missions / Business Functions	
CP-2 (8)	Contingency Plan Identify Critical Assets	
CP-3	Contingency Training	
CP-4	Contingency Plan Testing	
CP-4 (1)	Contingency Plan Testing Coordinate with Related Plans	Non-tech
CP-6	Alternate Storage Site	
CP-6 (1)	Alternate Storage Site Separation from Primary Site	
CP-6 (3)	Alternate Storage Site Accessibility	Non-tech
CP-7	Alternate Processing Site	
CP-7 (1)	Alternate Processing Site Separation from Primary Site	Non-tech
CP-7 (2)	Alternate Processing Site Accessibility	Non-tech
CP-7 (3)	Alternate Processing Site Priority of Service	Non-tech
CP-8	Telecommunications Services	
CP-8 (1)	Telecommunications Services Priority of Service Provisions	
CP-8 (2)	Telecommunications Services Single Points of Failure	
CP-9	Information System Backup	
CP-9 (1)	Information System Backup Testing for Reliability / Integrity	
CP-9 (3)	Information System Backup Separate Storage for Critical Information	Non-tech
CP-10	Information System Recovery and Reconstitution	
CP-10 (2)	Information System Recovery and Reconstitution Transaction Recovery	

Comments regarding the CP Control Family

Although the particular lab instance reviewed had the limitation of a single location, FlexPod MetroCluster solutions, which address additional disaster recovery and business continuity requirements referenced by controls CP-6, CP-6(1), CP-6(3), CP-7, CP-7(1), CP-7(2) and CP-7(3), may be constructed using guidance found at these locations: (design) <http://www.netapp.com/us/media/nva-0030-design.pdf> and (deployment) <http://www.netapp.com/us/media/nva-0030-deploy.pdf>.

Identification and Authentication (IA)

The Identification and Authentication (IA) control family has 26 technical controls and one policy and procedure and is described as “Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.”

Findings for IA

Focus on multifactor authentication as an identification safeguard is stressed in conjunction with technology-based methods to determine and confirm acceptable connection methods. Other controls that would implement Identification and Authentication for the Agency application workload were not present nor observed. As in previous sections, those were denoted by a blank.

Table 10 - IA Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Identification and Authentication (IA)	26
IA-1	Identification and Authentication Policy and Procedures	Non-tech
IA-2	Identification and Authentication (Organizational Users)	●
IA-2 (1)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts	●
IA-2 (2)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts	●
IA-2 (3)	Identification and Authentication (Organizational Users) Local Access to Privileged Accounts	●
IA-2 (5)	Identification and Authentication (Organizational Users) Group Authentication	
IA-2 (8)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts - Replay Resistant	●
IA-2 (11)	Identification and Authentication (Organizational Users) Remote Access - Separate Device	●
IA-2 (12)	Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	
IA-3	Device Identification and Authentication	●
IA-4	Identifier Management	●
IA-4 (4)	Identifier Management Identify User Status	●
IA-5	Authenticator Management	●
IA-5 (1)	Authenticator Management Password-Based Authentication	●

IA-5 (2)	Authenticator Management PKI-Based Authentication	
IA-5 (3)	Authenticator Management In-Person or Trusted Third-Party Registration	
IA-5 (4)	Authenticator Management Automated Support for Password Strength Determination	
IA-5 (6)	Authenticator Management Protection of Authenticators	
IA-5 (7)	Authenticator Management No Embedded Unencrypted Static Authenticators	
IA-5 (11)	Authenticator Management Hardware Token-Based Authentication	
IA-6	Authenticator Feedback	●
IA-7	Cryptographic Module Authentication	●
IA-8	Identification and Authentication (Non-Organizational Users)	◐
IA-8 (1)	Identification and Authentication (Non-Organizational Users) Acceptance of PIV Credentials from Other Agencies	
IA-8 (2)	Identification and Authentication (Non-Organizational Users) Acceptance of Third-Party Credentials	
IA-8 (3)	Identification and Authentication (Non-Organizational Users) Use of FICAM-Approved Products	
IA-8 (4)	Identification and Authentication (Non-Organizational Users) Use of FICAM-Issued Profiles	

Comments regarding the IA Control Family

Although multi-factor authentication was feasible, the integration of the second factor via RSA Key or other technologies was not observed in the lab FlexPod under review. We did consider the integration to be trivial and comprehensive enough to warrant a partially supported for controls IA-2(1), IA-2(2) and IA-2(3). Missing elements to access PKI support via the Internet were causal in the partial integration.

An example of centralized control by HyTrust CloudControl of the Authentication Policy settings is shown here:

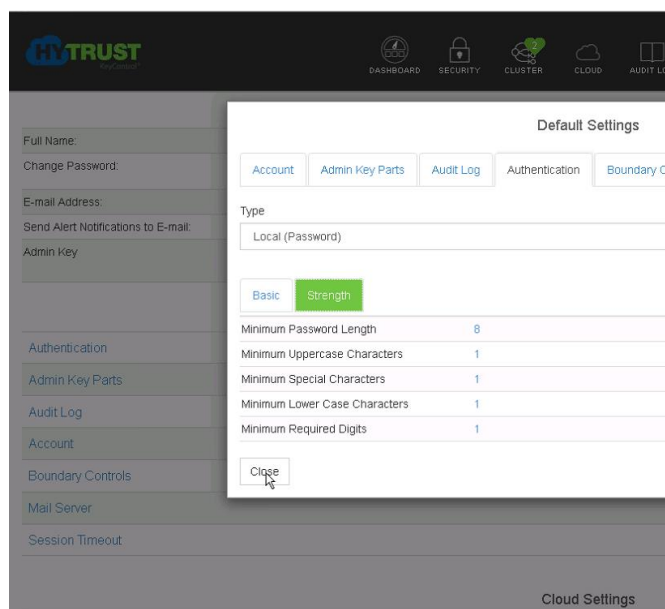


Figure 15 - HyTrust CloudControl Password Policy Configuration

The accompanying vCenter Single Sign-on (SSO) integration with the Microsoft AD control mechanism is depicted in this screen:

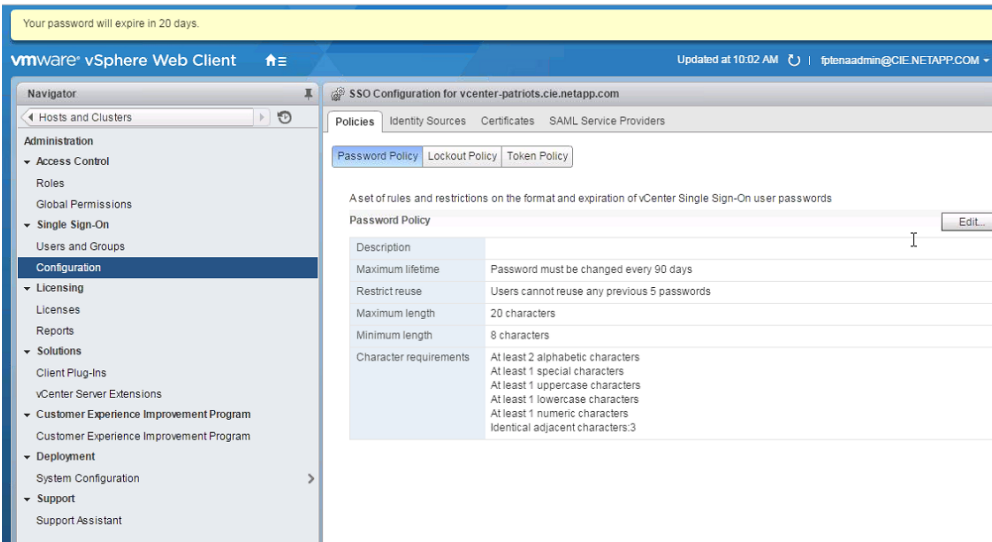


Figure 16 - VMware vCenter SSO Configuration with Password Policy settings

Media Protection (MP)

The Media Protection (MP) control family is defined by the statement “Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.” Our examination of the 9 technical controls was limited due to our use of the FAS storage subsystem in our lab review.

MP Findings

Table 11 - MP Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Media Protection (MP)	9
MP-1	Media Protection Policy and Procedures	Non-tech
MP-2	Media Access	●
MP-3	Media Marking	◐
MP-4	Media Storage	◐
MP-5	Media Transport	●
MP-5 (4)	Media Transport Cryptographic Protection	●
MP-6	Media Sanitization	◐
MP-6 (2)	Media Sanitization Equipment Testing	
MP-7	Media Use	●

MP-7 (1)	Media Use Prohibit Use without Owner	●
----------	--	---

Comments on MP Control Findings

Media Access control is an intrinsic function of the NetApp FAS storage subsystem, which requires subscription to NAS volumes for the CSP and Tenant A/B workloads.

Rudimentary electronic marking of media is performed via the VMware storage assignment and rights management, which may be configured to coordinate access to the FAS data stores and would facilitate appropriate allocation of intended storage to the intended workload.

Media storage MP-4 and transport MP-5/MP-5(4) controls are present by nature in the FlexPod itself, which can support encrypted media at the hard disk drive (HDD) level and via secure CSP key management techniques that render media unreadable should it be remove and examined.

Transport and sanitization of media were not objectives of the test FlexPod instance, but were confirmed for the particular action of FAS storage HDD removal.

Risk Assessment (RA)

“Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information” defines the Risk Assessment (RA) control family. 8 technical controls were available for evaluation of the 10 total controls.

RA Findings

Only one control was available for assessment, RA-5(5), which was addressed by the NetApp FAS Virus Scanning pool, which may perform AV scans on the NFS/NAS volumes, when VMware workloads used for tenant data storage are deployed.

Table 12 - RA Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	Risk Assessment (RA)	9
RA-1	Risk Assessment Policy and Procedures	Non-tech
RA-2	Security Categorization	Non-tech
RA-3	Risk Assessment	
RA-5	Vulnerability Scanning	
RA-5 (1)	Vulnerability Scanning Update Tool Capability	
RA-5 (2)	Vulnerability Scanning Update by Frequency / Prior to New Scan / When Identified	
RA-5 (3)	Vulnerability Scanning Breadth / Depth of Coverage	
RA-5 (5)	Vulnerability Scanning Privileged Access	●
RA-5 (6)	Vulnerability Scanning Automated Trend Analyses	
RA-5 (8)	Vulnerability Scanning Review Historic Audit Logs	

Noteworthy Comments Regarding RA Controls

An example of NetApp AV support is shown in the following two screens.

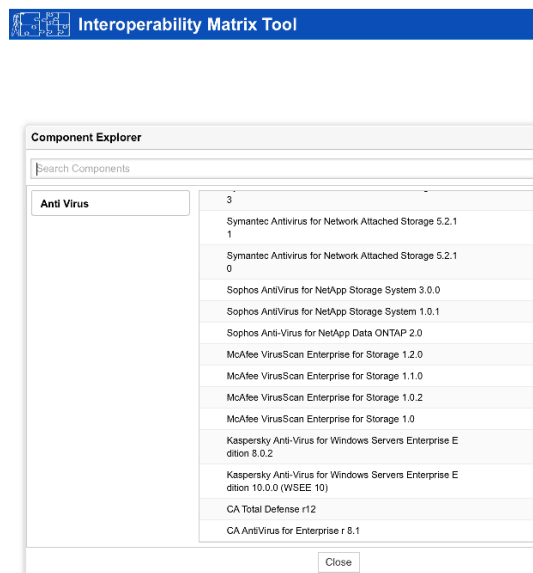


Figure 17 - FAS Configuration for AV Integration Example

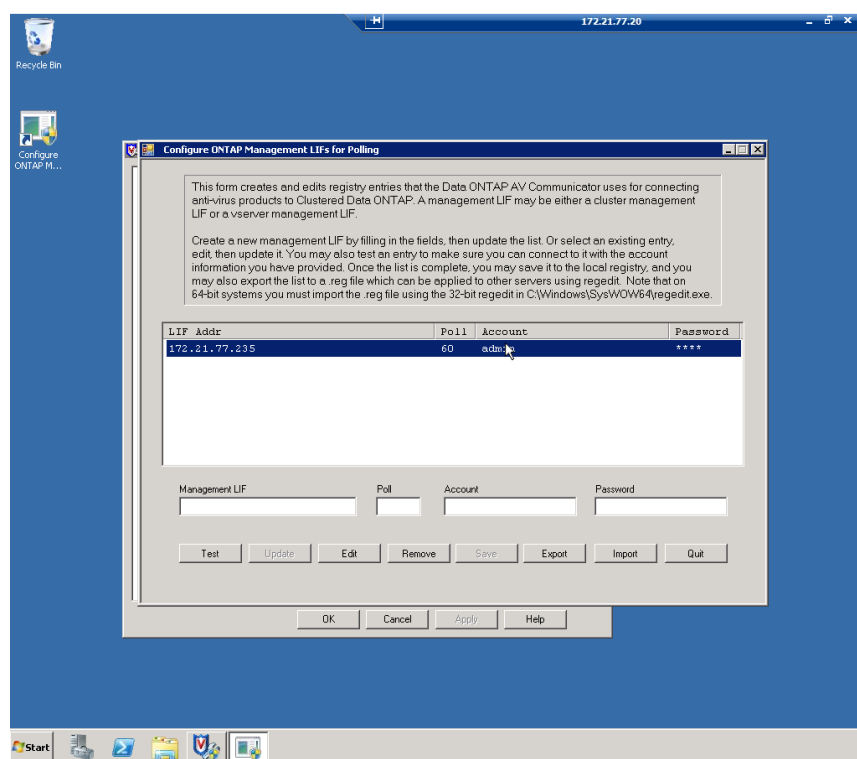


Figure 18 - ONTAP Management Configuration to Enable Polling for AV Integration

System and Services Acquisition (SA)

Defined in the NIST guidance as “Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization”, the System and Services Acquisition (SA) control family is comprised of 22 controls, of which 19 were available for technical assessment.

SA Findings

Table 13 - SA Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	System and Services Acquisition (SA)	19
SA-1	System and Services Acquisition Policy and Procedures	Non-tech
SA-2	Allocation of Resources	●
SA-3	System Development Life Cycle	●
SA-4	Acquisition Process	●
SA-4 (1)	Acquisition Process Functional Properties of Security Controls	
SA-4 (2)	Acquisition Process Design / Implementation Information for Security Controls	
SA-4 (8)	Acquisition Process Continuous Monitoring Plan	
SA-4 (9)	Acquisition Process Functions / Ports / Protocols / Services in Use	Non-tech
SA-4 (10)	Acquisition Process Use of Approved PIV Products	
SA-5	Information System Documentation	●
SA-8	Security Engineering Principles	●
SA-9	External Information System Services	
SA-9 (1)	External Information Systems Risk Assessments / Organizational Approvals	
SA-9 (2)	External Information Systems Identification of Functions / Ports / Protocols / Services	Non-tech
SA-9 (4)	External Information Systems Consistent Interests of Consumers and Providers	
SA-9 (5)	External Information Systems Processing, Storage, and Service Location	
SA-10	Developer Configuration Management	●
SA-10 (1)	Developer Configuration Management Software / Firmware Integrity Verification	●
SA-11	Developer Security Testing and Evaluation	●
SA-11 (1)	Developer Security Testing and Evaluation Static Code Analysis	●
SA-11 (2)	Developer Security Testing and Evaluation Threat and Vulnerability Analyses	●
SA-11 (8)	Developer Security Testing and Evaluation Dynamic Code Analysis	●

Comments on SA Family Controls

Consisting only of a CSP platform and devoid of any actual Agency workload, we may only observe and comment on the Infrastructure as a Service (IaaS) environment and HyTrust application base. This

evaluation was based on RFI materials observed in the supporting documentation from Cisco, NetApp, VMware, Microsoft, RedHat, and HyTrust. Sections SA-10, *Developer Configuration Management* and SA-11, *Developer Security Testing and Evaluation* also focus on the platforms to support Virtual Machines, storage, and network integration.

System and Communications Protection (SC)

The System and Communications Protection (SC) control family is defined as “Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.” FedRAMP “moderate” controls total 32, with 31 requiring technical validation.

SC Findings

This control family is comprehensive and highly important with firewall deployment, logical partitioning, shared resource rules, denial of service protections, availability, data transmission, cryptographic key management, cryptographic protection, mobile, voice, PKI, DNS, data protection, etc. As in previous sections, a blank indicates non-testing due to the particulars of our lab test-bed.

Table 14 - SC Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	System and Communications Protection (SC)	31
SC-1	System and Communications Protection Policy and Procedures	Non-tech
SC-2	Application Partitioning	●
SC-4	Information in Shared Resources	◐
SC-5	Denial of Service Protection	◐
SC-6	Resource Availability	◐
SC-7	Boundary Protection	
SC-7 (3)	Boundary Protection Access Points	
SC-7 (4)	Boundary Protection External Telecommunications Services	
SC-7 (5)	Boundary Protection Deny by Default / Allow by Exception	
SC-7 (7)	Boundary Protection Prevent Split Tunneling for Remote Devices	
SC-7 (8)	Boundary Protection Route Traffic to Authenticated Proxy Servers	
SC-7 (12)	Boundary Protection Host-Based Protection	
SC-7 (13)	Boundary Protection Isolation of Security Tools / Mechanisms / Support Components	
SC-7 (18)	Boundary Protection Fail Secure	
SC-8	Transmission Confidentiality and Integrity	
SC-8 (1)	Transmission Confidentiality and Integrity Cryptographic or Alternate Physical Protection	
SC-10	Network Disconnect	◐

SC-12	Cryptographic Key Establishment and Management	
SC-12 (2)	Cryptographic Key Establishment and Management Symmetric Keys	
SC-12 (3)	Cryptographic Key Establishment and Management Asymmetric Keys	
SC-13	Cryptographic Protection	
SC-15	Collaborative Computing Devices	
SC-17	Public Key Infrastructure Certificates	
SC-18	Mobile Code	
SC-19	Voice Over Internet Protocol	
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	●
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	●
SC-22	Architecture and Provisioning for Name / Address Resolution Service	◐
SC-23	Session Authenticity	●
SC-28	Protection of Information at Rest	●
SC-28 (1)	Protection of Information at Rest Cryptographic Protection	◐
SC-39	Process Isolation	●

Comments Regarding the SC Controls Reviewed

The absence of an Internet or private connection in this test environment and the absence of firewalls, HTTPS load-balancers, and other access infrastructure eliminated a large number of controls from our review.

VMware vSphere hypervisors via their architecture (VMware clusters separating the CSP, Tenant A and Tenant B workloads), operated in conjunction with the HyTrust Cloud Control policy management suite to create and enforce an “industrial strength” technical base for FedRAMP “moderate” compliance.

Rigorous application of VLAN allocation for the network layer further re-enforced the partitioning of resources.

The Cisco UCS solution supports fine-grained policy control specifically for multi-tenant requirements and systems isolation for components (e.g. UCS VIC PCIe virtualization), which may be leveraged to further enhance compliance in the SC controls family.

System and Information Integrity (SI)

Defined as “Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response”, the System and Information Integrity (SI) control family is comprised of 28 total controls. 27 controls were available for technical assessment in our scenario.

SI Findings

As in the AU family, absence of a SIEM system eliminated rich Information System Monitoring control compliance. In an actual CSP with an actual tenant workload, there would be a code base to protect. This would be in addition to the intrinsic support for MD5-based boot-time component validation provided by VMware vSphere.

Table 15 - SI Control Family Findings

CONTROL ID	CONTROL NAME	FEDRAMP MODERATE
	System and Information Integrity (SI)	27
SI-1	System and Information Integrity Policy and Procedures	Non-tech
SI-2	Flaw Remediation	
SI-2 (2)	Flaw Remediation Automated Flaw Remediation Status	
SI-2 (3)	Flaw Remediation Time to Remediate Flaws / Benchmarks for Corrective Actions	
SI-3	Malicious Code Protection	●
SI-3 (1)	Malicious Code Protection Central Management	
SI-3 (2)	Malicious Code Protection Automatic Updates	
SI-3 (7)	Malicious Code Protection Nonsignature-Based Detection	
SI-4	Information System Monitoring	●
SI-4 (1)	Information System Monitoring System-Wide Intrusion Detection System	
SI-4 (2)	Information System Monitoring Automated Tools for Real-Time Analysis	
SI-4 (4)	Information System Monitoring Inbound and Outbound Communications Traffic	
SI-4 (5)	Information System Monitoring System-Generated Alerts	●
SI-4 (14)	Information System Monitoring Wireless Intrusion Detection	
SI-4 (16)	Information System Monitoring Correlate Monitoring Information	
SI-4 (23)	Information System Monitoring Host-Based Devices	
SI-5	Security Alerts, Advisories, and Directives	
SI-6	Security Function Verification	
SI-7	Software, Firmware, and Information Integrity	●
SI-7 (1)	Software, Firmware, and Information Integrity Integrity Checks	●
SI-7 (7)	Software, Firmware, and Information Integrity Integration of Detection and Response	●
SI-8	Spam Protection	

SI-8 (1)	Spam Protection Central Management	
SI-8 (2)	Spam Protection Automatic Updates	
SI-10	Information Input Validation	◐
SI-11	Error Handling	◐
SI-12	Information Handling and Retention	
SI-16	Memory Protection	◐

Comments on SI Family Controls

SI-3, SI-4, SI-7, SI-7(1), and SI-7(7) compliance is partially owed to the intrinsic support in VMware for code protection, monitoring, and integrity checking. Actual Agency workloads would have their own systems with integrated services supporting the complex applications being hosted.

SI-7(7) control delivery via HyTrust DataControl added extreme image detection and protection benefits through the use of encrypted VMware virtual machine images, which cannot be executed, unless authorizing keys are supplied to decrypt the image. An example of that support is shown in the following screen captures.

Name	Status	IP Address	Cert Expires	VM Set	Updated Agent	Folders	Disks
vm1-tenant-a	Online	172.21.84.60	10/07/2017	VM_Set_Tenant_A		0	1
vm2-tenant-a	Online	172.21.84.61	10/07/2017	VM_Set_Tenant_A		0	1
vm3-tenant-a	Online	172.21.84.62	10/07/2017	VM_Set_Tenant_A		0	1
vm4-tenant-a	Online	172.21.84.63	10/07/2017	VM_Set_Tenant_A		0	1
vm5-tenant-a	Online	172.21.84.64	10/07/2017	VM_Set_Tenant_A		0	1

IP Address:	172.21.84.60
Description:	Empty
Certificate Valid Until:	10/07/2017
Heartbeat:	5 minutes
Grace Period:	1 days
Status:	Online
OS:	Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1 (build 7601) 64-bit

Figure 19 - HyTrust DataControl Protected VM Example for Tenant A

The **vm1-tenant-a** VM above has an AES-512 encrypted machine image and requires the appropriate policy-managed key to load, boot and operate the virtual machine.

Name	Encrypted Disk	Cipher	Key Expiration	On Expiration	Size	Mapped Device	Last Rekey	Next Rekey	State
DeviceHarddisk	C:	AES-XTS-512	Never	No Use	40498 MB	C:	10/07/2016	NA	Active

Figure 20 - VM Disk using HyTrust DataControl from Tenant A (above)

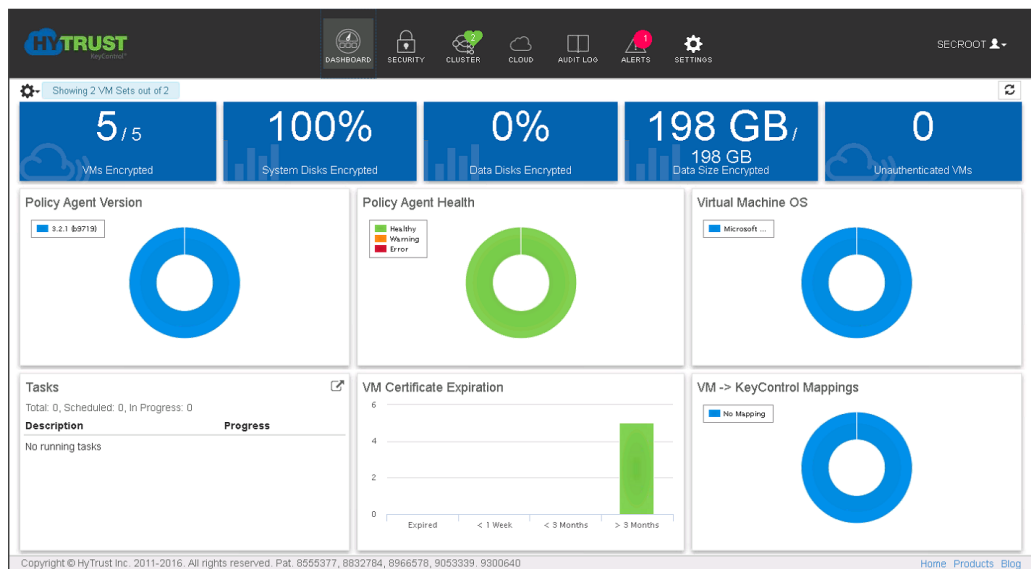


Figure 21 - HyTrust Dashboard

Other Observations (Other)

All configuration, control and operation of this lab test instance was performed by the supporting technical architect from NetApp, who had administrative access to the resources through their corporate networks and secure VPN used to access the RTP lab from afar.

Jump stations – which are workstations built into the lab and test infrastructure and secured by corporate firewalls and the network access rules restricting access to/from those devices – were used exclusively to access both CSP and tenant workloads in their respective clusters. This use of restricted administrative workstations is both a best practice and a likely model to be used in actual production FedRAMP CSP and Agencies.

Our data was collected during a number of WebEx sessions with the NetApp technical architects, who “drove” the test environment, by a combination of RDP, VNC, and SSH console sessions. We performed screen captures of critical information to support and substantiate our findings. This approach differs from an actual audit, which would rely entirely on RFI materials provided by the CSP and/or Agency in conjunction with interviews and penetration testing activities.

SUMMARY OF THE SIMULATED AUDIT FINDINGS

One hundred seventeen (117) controls in the test instance were found to either Support or Partially Support the FedRAMP “moderate” baseline requirements. This represented approximately 42% (117 of 282) of the technical controls require for “moderate” FedRAMP compliance.

The following comments pertain to our summary of findings:

- Fifty-four (54) technical controls were unexamined in the six control families (Awareness and Training (AT), Incident Response (IR), Maintenance (MA), Physical and Environmental Protection (PE), Planning (PL), and Personnel Security (PS)) that were not evaluated.
- Internet access would involve Firewalls, IDS/IPS, DLP, and Load Balancers and would open up a host of additional control opportunities.
- The lab validation instance was devoid of actual applications and of services that would be present in the remaining infrastructure of a real CSP – two elements that would bring many of the 165 remaining technical controls into action. For example: wireless, portable storage and mobile devices are addressed by 7 controls, which would be in force should the Agency application use those services.
- The actual Agency tenant workload – a defined application occupying the “placeholder” 3 tier architecture within a true CSP FedRAMP delivery – is another missing component of our laboratory FlexPod Datacenter test environment. A real application seeking an ATO would fill this void.
- The VMware vSphere is a desirable hypervisor, orchestration, and management platform with widespread acceptance in the federal information technology arena. Although not a requirement, we have observed that CSPs and existing Agencies expect VMware equivalent functionality in their cloud deployments. The FlexPod is capable of supporting a wide variety of hypervisors, should they be specifically required.
- The tested FlexPod Datacenter instance was devoid of a minor “daughter card” on the Cisco UCS motherboards to enable TXT/TPM support on the Intel Xeon V3 CPUs. Geolocation service, potentially desirable to prevent hijacking of VMware virtual machines, could easily be enabled with the inclusion of this feature.

COALFIRE OPINION

The US Federal Risk and Authorization Management Program (FedRAMP) was created to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA), and to promote an accelerated adoption of secure cloud solutions by federal agencies.

The FlexPod® Datacenter and other converged infrastructure solutions, which package and codify the integration of compute, network, and storage elements, create a uniform and reliable base for implementation of Cloud Service Provider services to host Agency applications.

The author's opinion is based on the results of the testing performed on the Fall 2016 RTP North Carolina laboratory test instance of FlexPod Datacenter with VMware vSphere 6.0, HyTrust CloudControl and DataControl, as documented, configured, and reviewed for a NIST SP800-53r4-inspired FedRAMP 2.1 "moderate" baseline. In our opinion, the solution **is effective** in providing significant and substantial support for the objectives and requirements of both CSPs and federal agencies in pursuit of a FedRAMP "Ready" product.

Our opinion is dependent on a number of underlying presumptions, which are enumerated here:

- Adherence to vendor best practices
- Hardening of configurations
- Presence of an actual (not hypothetical) workload
- Certain underlying CSP services being present
- Alignment of technical controls with actual CSP/Agency missions, roles, responsibilities, policies, procedures, baselines, mandates, etc.
- Physical and organizational controls
- Presence of IT staff at the CSP and the Agency
- Federal agency users subscribing to actual applications and services

A COMMENT REGARDING REGULATORY COMPLIANCE

Coalfire disclaims generic suitability of any product to cause a customer using that product to achieve regulatory compliance. ***Customers attain compliance through a Governance, Risk Management, and Compliance (GRC) program, not via the use of a specific product. This is true for FedRAMP CSPs and federal agencies, as well as for customers targeting compliance with other regulations.***

ABOUT THE AUTHORS AND CONTRIBUTORS

Chris Krueger | Author | Principal, Cloud and Virtualization, Coalfire Labs, Coalfire Systems
As Principal, Mr. Krueger contributes as an author and thought leader on information security and regulatory compliance topics for Coalfire's clientele in the "new and emerging" technical areas.

Jason Macallister | Reviewer | Senior Consultant, Coalfire Labs, Coalfire Systems
Mr. Macallister consults on information security and regulatory compliance topics as they relate to advanced infrastructure, emerging technology, and VMware products.

James DeCaires | NetApp Project Sponsor | Sr. Product Manager, NetApp
Mr. DeCaires is a FlexPod Product Manager with responsibility for messaging.

Arvind Ramakrishnan | Technical Lead | Solutions Architect, NetApp
Mr. Ramakrishnan is an Architect focused on developing and validating converged infrastructure solutions.

Published January 2017.

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com

Copyright © 2014-2017 Coalfire Systems, Inc. All Rights Reserved. Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

WP_NetApp FlexPod Datacenter Validated Architecture with VMware for FedRAMP 2.1 v1.0