Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

Quick Start: Cloud Infrastructure Benchmark

v1.0.0

10-08-2012

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the “SB Products”) as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products “as is” and “as available” without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member’s own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member’s membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document provides high level guidance for securing or evaluating virtual and cloud infrastructure. The recommendations expressed herein are not exhaustive. Instead, they intend to represent high value actions one may take toward securing or evaluating virtual and cloud infrastructure. Additionally, these recommendations intend to be provider, vendor, and product agnostic. Recommendations are placed in to four sections:

1. Common Recommendations
2. Virtual Infrastructure Recommendations
3. Cloud Infrastructure Recommendations
4. End User Work Load Recommendations

The above sections are defined in the Profiles section below. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for various roles, including security officers, virtual infrastructure administrators, cloud infrastructure administrators, cloud customers, cloud providers, and cloud auditors. Additionally, individuals and organizations that seek a starting point for the security controls to consider when adopting or building cloud infrastructure may find the recommendations in this document valuable.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Common Recommendations**

  Recommendations in this profile are applicable to all other profiles.

- **Virtual Infrastructure**

  This profile extends the "Common Recommendations" profile. Recommendations in this profile apply to virtual infrastructure components. They cover hosts, guests, network and virtual machine monitor.

- **Cloud Infrastructure**

  This profile extends the "Common Recommendations" profile. Recommendations in this profile apply to cloud infrastructure components and are not specific to any given cloud implementation.

- **End User Workloads**

  This profile extends the "Common Recommendations" profile. Recommendations in this profile apply to the end user workloads hosted by cloud infrastructure.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors
Pravin Goyal, *RHCE, HP-UX CSA, VCP, MBA, CISSP, GISP, CCSK, CloudU, CompTIA CE, VMware Inc.*
Michael A. Haines, *VMware, Inc.*
George Gerchow, *VMware, Inc.*

Contributor
Geoffrey Coulter, *VCE*
Mike Ellis, *vExpert, RoundTower Technologies*
Chris Farrow, *Compassion International*
Blake Frantz, *Center for Internet Security*
Wade Holmes, *VMware, Inc.*
Tom McAndrew, CISSP, CISA, CISM, QSA, *Coalfire Systems*
Mark Modisette, CISSP, CGEIT, PMP, ITIL, MCSE, *Security Executive*
Davi Ottenheimer, *K3DES*

Recommendations

1 Common Recommendations

Recommendations in this section are applicable to all profiles: Virtual Infrastructure, Cloud Infrastructure, and End User Work Loads.

1.1 Maintain Current Patch Levels

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure
- End User Workloads

Description:

Vulnerabilities are commonly discovered in hypervisors, operating systems, software, and hardware components. These vulnerabilities are often mitigated by vendor-provided software or firmware patches. It is recommended that patch levels for all IT components remain current.

Rationale:

By ensuring that all IT components maintain current patch levels, the risk associated with the vulnerabilities mitigated by those patches is reduced. If patch levels are not maintained, the risk of realizing negative impact to the confidentiality, integrity, and availability of IT components is increased.

Audit:

1. Verify the completeness of the IT asset inventory.
2. For each asset in the IT inventory, obtain or create a list of available, applicable vendor-provided patches.
3. For each asset in the IT inventory, obtain or create a list of installed vendor-provided patches.
4. Compare the list of available patches to the list of installed patches.
5. For each patch that is absent from the installed-patches-list, identify the root cause of the gap, make adjustments to patch management procedures, and implement the updated procedure.

Remediation:

1. Identify all IT components in the cloud environment for which the vendor releases security patches.
2. Follow your organization's patch management policy and procedures to apply these patches.

References:

1. Creating a Patch and Vulnerability Management Program - http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

1.2 Create and Enforce Account and Password Management Policies

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure
- End User Workloads

Description:

Account and Password Management Policies typically establish requirements for events that occur in an account's or password's life cycle. It is recommended that account management and password policies be created and enforced across all components.

Rationale:

The creation and enforcement of these policies is foundational to the efficacy of authentication and access control mechanisms. If account and password management policies are created and enforced then the probability of unauthorized access to assets may be reduced.

Audit:

1. Ensure that an inventory of all components requiring controlled access exists.
2. Ensure that access to all components is restricted in accordance with your organization's account and password management policies.

Remediation:

1. Create an inventory of all components and assets for which access must be restricted.
2. Implement access controls in accordance with your organization's account and password management policy.

1.3 Use a Central Directory for Authentication and Authorization

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure

- End User Workloads

Description:

Many operating systems and software stacks can be configured to authenticate and authorize requests using a centralized directory server. It is recommended that all components be configured in this manner.

Rationale:

Leveraging a central directory for authentication and authorization requests will help minimize the risk associated with inappropriately provisioned and deprovisioned accounts. If a central directory is not used, the opportunity for error when creating a new or decommissioning an old account increases. These errors may lead to unauthorized access.

Audit:

1. Ensure that an inventory of all components / systems in the cloud environment that can be integrated with a central directory for facilitating authentication and authorization exists.
2. Check details of authentication and authorization requirements and organization's account management policy.
3. Ensure that a central directory is configured with all the account details and attributes.
4. Ensure that all the components / systems use the central directory for authenticating and authorizing any user.

Remediation:

1. Create an inventory of all the components / systems in the cloud environment that can be integrated with a central directory for facilitating authentication and authorization.
2. Identify authentication and authorization requirements based on your environment and organization's account management policy.
3. Configure the central directory with all the account details and attributes.
4. Configure all the components / systems to use the central directory for authenticating and authorizing any user.

1.4 Configure Firewalls to Restrict Access

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure
- End User Workloads

Description:

A firewall provides the ability to restrict access to network resources in accordance with a security policy. It is recommended that firewalls be placed between networked components and be configured to reflect least privilege.

Rationale:

Limiting communication between networked components reduces the attack surface of those components. Additionally, the impact of a compromised or misused component may be minimized if the firewall is configured to restrict ingress and egress traffic.

Audit:

1. Ensure that an inventory of all the components / systems in the cloud environment that can be firewall protected exists.
2. Check details of firewall configuration requirements and organization's firewall configuration management policy.
3. Ensure that the firewall is configured on all the components based on the requirements.

Remediation:

1. Create an inventory of all the components / systems in the cloud environment that can be firewall protected.
2. Identify firewall configuration requirements based on your environment and organization's firewall configuration management policy.
3. Configure the firewall on all the components based on the requirements.

1.5 Use TLS/SSL where Possible

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure
- End User Workloads

Description:

The Transport Layer Security (TLS) / Secure Socket Layer (SSL) protocols provide confidentiality, integrity, and authenticity guarantees to data transmitted using them. It is recommended that TLS/SSL be used to protect data in transit where possible.

Rationale:

Leveraging TLS/SSL to protect all communication in a cloud infrastructure will decrease opportunity to compromise the confidentiality and integrity of data in transit. If TLS/SSL is not used, the authenticity of client/server end-points cannot be guaranteed nor the confidentiality of credentials or other information traversing the network be assured.

Audit:

1. Ensure an inventory of all network-accessible services present in the cloud environment that depend on peer-authenticity, data confidentiality, and/or data integrity exists.
2. Ensure that all such services are protected by TLS/SSL.

Remediation:

1. Create an inventory of all network-accessible services present in the cloud environment that depend on peer-authenticity, data confidentiality, and/or data integrity.
2. Implement or enable TLS/SSL for all such services.

References:

1. TLS Charter - http://datatracker.ietf.org/wg/tls/charter/

1.6 Do Not Use Default Self-Signed Certificates

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure
- End User Workloads

Description:

The security guarantees provided by TLS/SSL are heavily dependent on certificates. Certificates are a chain of trust, where each certificate is signed (trusted) by a higher, more credible certificate. At the top of the chain of trust are the root certificates, owned by a certificate authority (CA). Self-signed certificates are not signed by a certificate authority. It is recommended that all default self-signed certificates be replaced by certificates that are signed by a trusted CA.

Using self-signed certificates is a good start for securing your servers by setting up temporary SSL mechanism in development and test environments. However, this practice is not recommended for a production environment where security is a prime requirement. You must use certificates from a trusted certificate authority (CA). Certificates use a chain of trust, where each certificate in the chain is signed (trusted) by a higher, more credible certificate. At the top of the chain of trust are the root certificates, issued by a CA.

Rationale:

Leveraging certificates that are signed by a trusted CA will reduce opportunity for a successful man-in-the-middle attack.

Audit:

1. Ensure an inventory of all TLS/SSL enabled components exists.
2. Check the details of the digital certificate management procedure followed by the organization.
3. Ensure that the certificates used by these components are in line with certificate management procedures.

Remediation:

1. Create an inventory of all TLS/SSL enabled components.
2. Follow your organization's digital certificate management policy to replace all default self-signed certificates with certificates issued from trusted CAs only.

1.7 Configure Centralized Remote Logging

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure
- End User Workloads

Description:

Operating systems and other software components can commonly be configured to send logs to a remote server. It is recommended that all components be configured in this manner.

Rationale:

Centralizing log collection will help improve the organization's ability to identify, correlate, detect, and potentially minimize the impact of security events.

Audit:

1. Ensure that all the components / systems in the cloud environment that can be configured to log to a central log server have been identified.
2. Ensure that a central log server is properly configured and is operational based on organization's log management policy.
3. Ensure that all the components / systems are sending logs to the centralized log server.

Remediation:

1. Identify all the components / systems in the cloud environment that can be configured to log to a central location.
2. Configure a central log server based on your organization's log management policy.
3. Configure components / systems send logs to the central log server.

1.8 Maintain Time Synchronization Services

Profile Applicability:

- Virtual Infrastructure
- Cloud Infrastructure
- End User Workloads

Description:

Networked devices typically contain a clock that maintains the current time and date. These clocks are often susceptible to clock skew. Over time, this skew can grow, causing the device's clock to no longer represent the correct time and date. To account for this, devices can typically be configured to pull time information from an authoritative time server and adjust their internal clocks accordingly. It is recommended that all components be configured to synchronize their clocks with a secured, central time server.

Rationale:

Ensuring that all components have synchronized clocks will increase the organization's ability to accurately interpret log and event data that is enriched with a time stamp. Additionally, time synchronization will decrease the probability of a service outage caused by a security control that depends on synchronized clocks, such as Kerberos.

Audit:

1. Ensure that all the components / systems have been identified which require a secure time synchronization service.
2. Check details of clock synchronization procedures followed to ensure secure time synchronization.
3. Ensure that all the components / systems have time synchronization set and time synchronization is operational.

Remediation:

1. Identify all components / systems that require time synchronization services.
2. Deploy a secure, centralized time server in accordance with your organization's policies.
3. Configure all components to synchronize their clocks with the central time server.

References:

1. Network Time Protocol - http://www.ntp.org/

2 Virtual Infrastructure Recommendations

Recommendations in this section are applicable to virtual infrastructure components.

2.1 Review and Minimize Hypervisor Attack Surface

Profile Applicability:

- Virtual Infrastructure

Description:

A hypervisor provides virtual hardware resources to the guest operating systems it hosts and manages the execution of those guest operating systems. It is recommended that the attack surface of the given hypervisor be reviewed and minimized.

Rationale:

Reviewing and minimizing the attack surface of the hypervisor will reduce the probability of the hypervisor and its guests becoming compromised. If the hypervisor becomes compromised, the risk associated with the confidentiality, integrity, and availability of processes and data hosted by the hypervisor increases.

Audit:

1. Ensure that an inventory of hypervisors exists.
2. Ensure that a threat model for the hypervisors exists.
3. Ensure that security features provided by the hypervisor are enabled.
4. Ensure that dynamic root of trust measurement is enabled.

Remediation:

1. Create an inventory of all hypervisors in the environment.
2. Create an inventory of mechanisms by which the hypervisor may receive/process data/requests.
3. Reduce and restrict the aforementioned mechanisms, starting with those that receive/process data/requests from untrusted origins.
4. Enable security features provided by the hypervisor.
5. Consider implementing dynamic root of trust measurement.

References:

1. Trusted Platforms - http://download.intel.com/technology/efi/SF09_EFIS001_UEFI_PI_TCG_White_Paper.pdf
2. CIS Hypervisor Benchmarks - http://benchmarks.cisecurity.org/browse/benchmarks/servers/virtualization

2.2 Review and Minimize Virtual Machine Manager Attack Surface

Profile Applicability:

- Virtual Infrastructure

Description:

Hypervisors can be managed through Virtual Machine Manager (VMM) applications. It is recommended that the attack surface of VMM applications be reviewed and minimized.

Rationale:

Reviewing and minimizing the attack surface of the VMM applications will reduce the probability of the VMM, hypervisor, and guest becoming compromised. If the VMM becomes compromised, the risk associated with the confidentiality, integrity, and availability of processes and data hosted by the hypervisors under its management increases.

Audit:

1. Ensure that an inventory of all VMM applications exists.
2. Ensure that an inventory of mechanisms by which the VMM may receive/process data/requests exists.
3. Ensure a threat model for each VMM exists.
4. Ensure security features provided by the VMM application are enabled.
5. Ensure the operating system that the VMM application is installed on has been secured in accordance with your organization's security requirements.

Remediation:

1. Create an inventory of all VMM applications.
2. Create an inventory of mechanisms by which the VMM may receive/process data/requests.
3. Reduce and restrict the aforementioned mechanisms, starting with those that receive/process data/requests from untrusted origins.
4. Enable security features provided by the VMM application.
5. Secure the operating system that the VMM application is installed on in accordance with your organization's security requirements.

References:

1. CIS OS Benchmarks - http://benchmarks.cisecurity.org/browse/benchmarks/os

2.3 Use Templates to Deploy Virtual Machines

Profile Applicability:

- Virtual Infrastructure

Description:

A virtual machine template is a standardized group of hardware and software settings that can be used to create new virtual machines from. Templates allow an organization to bake its security requirements in to all virtual machines create it from it. It is recommended that standardized virtual machines templates be used to create virtual machines.

Rationale:

Developing and leveraging standardized virtual machine templates will increase the probability that virtual machines in the environment are compliant with the organization's security requirements. If templates are not used, security controls may be inconsistently applied to virtual machines.

Audit:

1. Ensure an inventory of server and workstation roles exists.
2. Ensure that standardized virtual machine templates exist for each role.
3. Ensure that existing virtual machines were created using approved templates only.

Remediation:

1. Create an inventory of server and workstation roles used in the organization. i.e. web server, file server, etc.
2. For each role, create a virtual machine template that is configured in compliance with the organization's security requirements.
3. Use only approved virtual machine templates to create virtual machines.

References:

1. Oracle VM Templates - http://www.oracle.com/technetwork/server-storage/vm/templates-101937.html
2. Deploy a Virtual Machine from a Template in the vSphere Client - http://pubs.vmware.com/vsphere-50/topic/com.vmware.vsphere.vm_admin.doc_50/GUID-9062F225-E01B-42BA-8AFB-8EA4069068FE.html
3. About Virtual Machine Templates - http://technet.microsoft.com/en-us/library/bb740838.aspx

2.4 Disconnect unauthorized devices from Virtual Machines

Profile Applicability:

- Virtual Infrastructure

Description:

A hypervisor may make devices, such as USB ports or network interfaces, available to its guest operating systems. It is recommended that all devices not required by the virtual machine be disabled or disconnected from the virtual machine.

Rationale:

In a physical environment, adding devices to machines have to follow a typical hardware procurement cycle with multiple levels of approvals and people involved in it. But, in a virtual environment, adding devices to virtual machines can be trivial without following the typical procurement path. This can lead to loss of control over the devices that are used by virtual machines and device features can be used as a point of attack. Hence, the device usage should be restricted on all the virtual machines.

Audit:

1. Ensure that an inventory of virtual machines exists.
2. Ensure that an inventory of devices required by each virtual machine exists.
3. Ensure that an inventory of devices currently in use by virtual machines exists.
4. Ensure that all devices currently in use by a virtual machine are in the required-devices list.
5. Ensure that all devices currently in use by a virtual machine are in the approved-devices list.

Remediation:

1. Create an inventory of all virtual machines
2. Create an inventory of all devices required by each virtual machine.
3. Create an inventory of all devices used by each virtual machine.
4. Identify the devices that are approved to be used in virtual machines based on your organization's asset management policy.
5. Disable, disconnect and remove the unapproved devices for all the virtual machines.

2.5 Disable MAC Address Changes and Promiscuous Node on Guests

Profile Applicability:

- Virtual Infrastructure

Description:

Many operating systems allow the administrator to customize the hardware address associated with a given network interfaces. Additionally, many operating systems allow administrators to place network interfaces in to promiscuous mode, which causes the interface to accept packets that are not destined to an address assigned to the interface itself. It is recommended that MAC address modifications and promiscuous mode be prevented by the virtual infrastructure.

Rationale:

If the virtual infrastructure allows a guest to transmit forged MAC addresses then the guest's ability to defeat access control mechanisms may be increased. Additionally, if a guest is permitted to observe network traffic that is intended for other network devices then the confidentiality of transmitted information may be at increased risk.

Audit:

1. Ensure that an inventory of all virtual networks exists.
2. Review the organization's network management policy.
3. Ensure that all the virtual networks are configured to reject spoofed traffic and promiscuous mode configuration.

Remediation:

1. Create an inventory of all virtual networks
2. Configure all the virtual networks to reject spoofed traffic and promiscuous mode configuration based on your organization's network management policy.

2.6 Ensure Network Isolation through VLANs

Profile Applicability:

- Virtual Infrastructure

Description:

Virtual LANs (VLAN) allow for the segmentation of networks into distinct broadcast domains. It is recommended to segment network traffic using VLANs.

Rationale:

Isolating network traffic in to VLANs may decrease a malicious guest's visibility and accessibility to other devices in the network. Additionally, VLANs restrict broadcast domain and therefore limit the opportunity for information leaks via network broadcast.

Audit:

1. Ensure an inventory of all network traffic types and zones of trust exist.
2. Check details of organization's network management policy.
3. Ensure that respective network traffic is isolated through VLANs.

Remediation:

1. Create an inventory of all the network traffic types and trust levels in your environment.
2. Create a VLAN for each distinct traffic type or trust zone in alignment with your organization's network management policy.

References:

1. RFC 5517 - http://tools.ietf.org/html/rfc5517
2. VLAN Security White Paper - http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

2.7 Port Groups Should not be Configured to Reserved VLANs

Profile Applicability:

- Virtual Infrastructure

Description:

Hypervisors do not use the concept of native VLAN. Frames with a VLAN specified in the port group will have a tag, but frames with a VLAN not specified in the port group are not tagged and therefore will end up as belonging to native VLAN of the physical switch. Additionally, certain physical switches reserve certain VLAN IDs for internal purposes and often disallow traffic configured to these values. For example, Cisco Catalyst switches typically reserve VLANs 1001–1024 and 4094, while Nexus switches typically reserve 3968–4047 and 4094. It is recommended that VLANs not be configured with the same VLAN IDs that are used by the physical switches or VLAN IDs that are reserved.

Rationale:

Leveraging reserved VLAN IDs may result in network traffic being routed in an unexpected manner, which may impact the confidentiality of network traffic or the availability of services that depend on the virtual network.

Audit:

1. Ensure that VLAN IDs requirements were identified.
2. Ensure that reserved VLAN IDs were identified.
3. Ensure that native VLAN IDs were identified.
4. Ensure that VLAN IDs were configured based on organization's network management policy.

Remediation:

1. Identify the VLAN IDs requirements in your organization.
2. Identify the reserved VLAN IDs by checking physical switch documentation.
3. Identify native VLAN IDs.
4. Configure VLAN IDs based on your organization's network management policy.

3 Cloud Infrastructure Recommendations

Recommendations in this section are applicable to cloud infrastructure components.

3.1 Secure Access to Cloud Application Programming Interfaces (API)

Profile Applicability:

- Cloud Infrastructure

Description:

Cloud-based services and applications often expose APIs that allow one to pragmatically interact with and manage aspects of the service or application. It is recommended that these API be fortified by the service provider and access to API keys be restricted by the consumer.

Rationale:

Performing a security review and fortifying the cloud API will help ensure that the API cannot be abused. Additionally, restricting access to API keys will reduce opportunity for unauthorized access to the cloud service or application. If accessibility to API keys is not restricted, unauthorized actors may abuse the API to negatively impact the service or information processed by it.

Audit:

1. Ensure than an inventory of cloud APIs exists.
2. Ensure a security review of the API and code bases that implement it exist.
3. Ensure an inventory of the organization's security requirements exists.
4. Ensure an inventory of security guarantees provided by the application/service exists.
5. Ensure controls are in place that enforces the aforementioned security requirements and guarantees.

Remediation:

1. Create an inventory of APIs provided by the cloud application/service and an inventory of API implementations.
2. Perform a security review of all APIs provided by the cloud application or service (provider).
3. Perform a security review of all code bases that implement the API (consumer).
4. Implement controls to align the API and implementations of it with the organization's security requirements and the application/service's security guarantees.

References:

1. Protect the API Keys to your Cloud Kingdom - https://blog.cloudsecurityalliance.org/2011/04/18/protect-the-api-keys-to-your-cloud-kingdom/

3.2 Encrypt Data at Rest

Profile Applicability:

- Cloud Infrastructure

Description:

Providing security for sensitive data in the cloud is a complex and critical task for any organization. Further, privacy concerns continue to generate regulations that hold data owners accountable for breaches and misuse. One method used to provide protection from the risks associated with deploying sensitive information into the cloud is encryption. It is recommended that all sensitive information be encrypted at rest.

Rationale:

Applying strong and proven encryption algorithms, such as the Advanced Encryption Standard (AES), to cloud deployments helps protect data by making it indecipherable to anyone who does not have access to the encryption key.

Audit:

1. Ensure an inventory of all sensitive information types present in the cloud infrastructure exists.
2. Ensure an inventory of all applications and processes that operate on this information exists.
3. Ensure that all storage locations used by these processes to store the sensitive information are identified.
4. Ensure the sensitive information at these locations is encrypted with a proven algorithm.

Remediation:

1. Create an inventory of all sensitive information types present in the cloud infrastructure.
2. Create an inventory of all applications and processes that operate on this information.
3. Identify the persistent and temporary locations these processes store the sensitive information.
4. Encrypt the sensitive information at these locations with a proven encryption algorithm, such as AES.

3.3 Establish Appropriate Resource Isolation

Profile Applicability:

- Cloud Infrastructure

Description:

One of the key aspects of cloud computing is the shared infrastructure and resources, such as CPU, memory, disk, and network, that comprise the physical topology. A key challenge of this is identifying and providing resource isolation in the traffic of one end tenant from another.

Rationale:

A Cloud platform consists of a physical infrastructure, including hosts, networks components, and storage. On top of this is a virtualized environment that implements virtual resources including data stores, port groups, and resource pools. Cloud applications abstracts Storage Resource Groups (SRG), Networks, and Compute Resource Groups (CRGs).

Providing the separation between the resource abstractions may help to reduce the resource management issues. More importantly, it allows for common layering to handle both small internal enterprise scenarios and large-scale service providers.

Audit:

1. Ensure that all resource isolation requirements were identified.
2. Check details of organization's commitments.
3. Ensure that resources are segregated and assigned based on organization's commitments.
4. Ensure resource availability to back specific cloud resources.
5. Ensure underlying resources are managed effectively.

Remediation:

1. Identify all resource isolation requirements.
2. Segregate and assign resources based on your organization's commitments.
3. Provide resources to back specific cloud resources.
4. Manage the underlying resources.

3.4 Evaluate Denial of Service Scenarios and Mitigations

Profile Applicability:

- Cloud Infrastructure

Description:

A denial of service (DoS) may be given rise by malicious intent or unforeseen resource consumption in the cloud infrastructure. It is recommended that denial of service scenarios and mitigations be evaluated.

Rationale:

Proactively considering scenarios that may lead to a denial of service and implementing mitigations may decrease the probability and impact of such an event, thereby increasing service availability.

Audit:

1. Ensure that the possible actions in the cloud environment that might lead to a DoS are identified.
2. Ensure that cloud application features that can aid in limiting such actions were identified.
3. Check details of organization's cloud management policy.
4. Ensure that such limiting options for cloud application are configured.

Remediation:

1. Identify the possible actions in the cloud environment that might lead to a DoS.
2. Identify cloud application features that can aid in limiting such actions.
3. Configure such limiting options for your cloud application based on your organization's cloud management policy.

3.5 Do Not Use or Set Guest Customization Passwords

Profile Applicability:

- Cloud Infrastructure

Description:

Guest customization typically allows an administrator to customize various options in the guest, such as the IP addresses, host name, or to join an Active Directory domain. It is recommended that guest customization passwords not be used.

Rationale:

Setting a guest customization password may increase the possibility of exposing credentials during guest customization steps.

Audit:

1. Ensure that guest customization requirements were identified.
2. Check details of organization's guest customization policy.
3. Ensure that guest customization parameters were set as appropriate.
4. Ensure that no passwords were used that might be exposed during guest customization.

Remediation:

1. Identify guest customization requirements.

2. Follow your organization's guest customization policy and set customization parameters as appropriate.

3.6 Evaluate Cloud Architecture Dependencies

Profile Applicability:

- Cloud Infrastructure

Description:

Cloud infrastructures are typically dependent on the tight integration of various hardware and software components. It is recommended that interdependencies within the architecture be evaluated and documented.

Rationale:

Evaluating and documenting interdependencies within cloud infrastructure components will reduce the probability of service level degradation or outage resulting from a change.

Audit:

1. Ensure that all hardware and software components in the cloud environment were identified.
2. Ensure that all dependencies of these components were recursively identified.
3. Ensure that such dependencies are documented in accordance with your organization's cloud management policy.

Remediation:

1. Identify all the hardware and software components in the cloud environment.
2. Recursively identify the software and hardware dependencies of the components.
3. Document the dependencies in accordance with your organization's cloud management policy.

3.7 Align Infrastructure Security Controls with Tenant Requirements

Profile Applicability:

- Cloud Infrastructure

Description:

Cloud infrastructure often serves multiple tenants with distinct security profiles and requirements. It is recommended that security controls provided by the cloud infrastructure to the tenant be evaluated against each tenant's security requirements.

Rationale:

By aligning the security controls provided by the cloud infrastructure with the security requirements of each tenant, each tenant will be able to operate in a manner that is consistent with their statutory, regulatory, and compliance obligations.

Audit:

1. Ensure that an inventory of each tenant's security requirements exists.
2. Ensure that an inventory of security controls provided by the cloud infrastructure exists.
3. Ensure that security controls for each tenant are configured in alignment with tenant requirements.

Remediation:

1. Create an inventory of the security requirement of each tenant.
2. Create an inventory of the security controls provided by the cloud infrastructure.
3. Identify tenant security requirements that cannot be satisfied by existing infrastructure controls.
4. Configure infrastructure controls to align with each tenant's requirements, where possible.
5. Coordinate with tenants to develop a plan to meet any unmet requirements.

References:

1. Deploying Secure Multi-Tenancy into Virtualized Data Centers - http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/securecldeployg.html

4 End User Workload Recommendations

Recommendations in this section are applicable to end user workloads, such as virtual desktops, that are hosted by the cloud infrastructure.

4.1 Segment and Restrict User and Server Workload Communication

Profile Applicability:

- End User Workloads

Description:

In this context of this section, two types of workloads may exist in a cloud delivery environment:

1. Server Workload – These workloads are comprised of file, print, web, database, and other server types that process requests made by various types of clients.
2. End User Workload – These workloads are comprised of desktops, laptops, PDAs, thin-clients, and other devices that are operated directly by the end user.

It is recommended that end user and server workload network traffic be segmented and that inter-network communication is restricted to reflect least privilege.

Rationale:

Segmenting and restricting user and server workload networks will reduce the probability of a compromised or misused workstation or server impacting other assets. If server and user communication is not segmented and restricted, the rate at which malware or other intrusions propagate throughout the fleet of workstations and servers may be higher than if communication is restricted. A higher threat propagation rate typically corresponds with a greater impact and reduced ability to contain the threat.

Audit:

1. Ensure an inventory of end user and server workloads exists.
2. Ensure an inventory of network interfaces present on end user and server workloads exists.
3. On each interface, ensure that an access control mechanism is preventing inter-asset communication for traffic types that are required for operations.

Remediation:

1. Create an inventory of end user and server workloads.
2. Create an inventory of each network interface on each user and server workload.
3. Implement an access control mechanisms that restricts communication via those interfaces to reflect least privilege.

4.2 Restrict User-to-User Workload Communication

Profile Applicability:

- End User Workloads

Description:

Given the rise of centralized services, such as file sharing and printing, the need for a given user's workstation to directly communicate with another user's workstation is greatly reduced. Therefore, it is recommended that user-to-user network communication be restricted.

Rationale:

Restricting user-to-user communication will reduce the probability of a compromised or misused workstation impacting other workstations. If user-to-user communication is not restricted, the rate at which malware or other intrusions propagate throughout the fleet of workstations may be higher than if communication is restricted. A higher threat propagation rate typically corresponds with a greater impact and reduced ability to contain the threat.

Audit:

1. Ensure an inventory of end user workloads exists.
2. Ensure an inventory of network interfaces present on end user workloads exists.
3. On each interface, ensure that an access control mechanism is preventing inter-workstation communication.

Remediation:

1. Create an inventory of end user workloads.
2. Create an inventory of each network interface on each user workload.
3. Implement an access control mechanisms that prevents inter-workstation communication via those interfaces.

4.3 Deploy Anti-Malware Solution to End User Workloads

Profile Applicability:

- End User Workloads

Description:

Anti-malware solutions are commonly applied to physical IT components to minimize the risk associated with viruses and exploits for known vulnerabilities. It is recommended that anti-malware solutions be deployed to protect end user workloads hosted in cloud infrastructure.

Rationale:

Deploying an anti-malware solution for end user workloads will decrease the probability of a those workloads being negatively impacted by viruses or known attack patterns. If an anti-malware solution is not deployed to protect end user workloads, the risk of a malware infection is increased.

Note: Resource-intensive tasks such as virus scanning can have a significant impact on performance, necessitating additional server hardware and resulting in lower consolidation ratios for virtual desktop deployments. Consider offloading portions of the anti-malware solution's processing from individual end user workloads to dedicated servers or devices.

Audit:

1. Ensure an inventory of end user workloads exists.

2. Ensure that an anti-malware solution is installed on each end user workload component.
3. Ensure that the anti-malware solution is configured in alignment with your organization's policies.

Remediation:

1. Create an inventory of end user workloads.
2. Install an anti-malware solution on each end user workload component.
3. Configure the anti-malware solution to align with your organization's policies.

4.4 Audit Privileged Access to End User Workloads

Profile Applicability:

- End User Workloads

Description:

Generally, administrative accounts possess great privilege. The reach of this privilege is compounded for administrators of cloud infrastructure. To help manage the risk associated with privileged accounts, organizations may choose to establish auditing mechanisms that issue notifications when a given privilege is exercised. It is recommended that privileged access to end user workloads be audited.

Rationale:

By auditing privileged access to end user workloads, the organization's ability to detect a compromised or abused privileged account is increased. If privileged access is not audited, the impact of a compromised or abused privileged account may increase.

Audit:

1. Ensure an inventory of end user workloads exists.
2. Ensure an inventory of privileged accounts exists.
3. Ensure audit mechanisms are enabled and that notifications are sent when privileged access to end user workloads occurs.

Remediation:

1. Create an inventory of end user workloads.
2. Create an inventory of privileged accounts that have access to those workloads.
3. Implement audit mechanisms that send notifications when privileged access to user workloads occurs.

Appendix: Change History

Date	Version	Changes for this version
2012-10-08	1.0.0	Initial Public Release