Contents

Server

Server: Server Resource Access and Authentication

https://www.plesk.com/blog/various/what-is-server-management/

Access

The access to servers’ resources and their management must be provided only to authorized personnel.

Access requests should be requested in written form through e-mail. For every access request there should be at least given employees’ name, ID code, justification for access, duration of access privileges, server name and supervisor. Account sharing is prohibited and must be clearly stated to the requester.

Any access request must be reviewed and results documented.

Whenever possible 2FA must be enforced to provide enhanced security.

Dedicated administration accounts must be created on the server for every authorized employee.

Daily tasks must not be executed using an administrative account.

Monitoring and Logging

Implement monitoring and logging to log access logs to the server.

Access logs must contain at least user UID, session start timestamp. Any unauthorized access attempts, login timeouts must result in a fired alert from the monitoring software.

Authentication

Authentication must be done only using secure communication protocols (HTTPS, SSH) and utilizing only personalized accounts and credentials.

SSH Authentication

The SSH key must be created for the user by server administrator, the key should be secured using a strong password containing at least 12 characters, upper and lower case, numbers, and special characters.

HTTPS Authentication

2FA must be enforced for an additional layer of security whenever it is possible. Password for authentication must contain at least 12 characters, upper and lower case, numbers, and special characters.

Credentials and SSH keys encryption

Credentials and SSH keys can be sent via e-mail if they are encrypted using government provided personal ID code of employee using official software from https://www.id.ee/.

Credentials Storage

Any credentials that are stored on a file system should be encrypted using official software from https://www.id.ee/ and personal ID code of employee.

Decrypted container text documents must not be opened using Notepad++.

Server: External Devices and Removable Media

https://www.opswat.com/blog/removable-media

Device Control and Registration

Any external devices that are used on servers must be registered. Registration information must include device type, device serial number, its purpose.

BIOS security configuration

BIOS administrative access must be restricted by using a strong password containing at least 12 characters, upper and lower case, numbers, and special characters.

By default, BIOS configuration must prohibit booting from external devices, or the boot order must be configured so that external devices are in the lowest priority.

Interface Management

All unutilized physical interfaces must be disabled if possible.

Data Security

After data transfer to the removable media must be encrypted. It is prohibited to store sensitive data on removable media with the exception of encrypted offline backups.

Server: Managing Server Services and Functionality

https://www.cloudpanel.io/blog/what-is-server-management/#services-components

Required Services Identification

Only a minimal set of services must be installed. To determine the required set of services evaluation of server purpose must be done.

A list of essential services must be composed and relevant installation documentation reviewed. By default, operating systems provided repositories must be used when installing services. Package manager installation must be preferred over manual installation. Any manual installation must be documented with detailed actions taken.

The list of essential services must be added to the server's documentation before the installation.

Applications/Packages for Troubleshooting

Only trusted sources must be used for acquiring the software (e.g. providers' official page, official repositories).

Any additional installed software must be documented containing the software name, purpose of installation and origin of the software (e.g. link, repository, package name). In case of a package or compiled binary is downloaded as the installation file the checksum must be controlled. After troubleshooting the installed package and temporarily files must be removed.

Server: Server Implementation Plan

https://clickup.com/templates/scope-of-work/server-installation

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-2/plan-for-successful-system-implementations

Hardware Platform

Hardware platform specification must include the form factor of the server, suitable CPU, RAM requirements, storage requirements, network capability requirements(throughput). These specifications must be determined based on servers' purpose and anticipated users count.

Operating System and Applications

Lightweight GNU/Linux distributives must be used to save resources of the server. During OS choosing aspects like support and extensive community must be considered.

Based on servers purpose a minimal set of services and applications must be composed.

Physical Requirements Aspects

Based on hardware platform specifications determine the space requirements, heat dissipation requirements for the server.

Heat dissipation must also contain the calculated passively cooled components heat dissipation.

Power

Sufficient PSU must be chosen leaving an overhang of approximately 20% of maximum power consumption of the server.

For protection against brownouts and power spikes UPS must be placed between the server's power connection and the grid. UPS power output must be not lower than PSUs

Integration with Existing Network Management

A review of network topology must be done to integrate the new server. IP addresses, firewall rules, DNS records, integration with current logging and monitoring systems must be reviewed.

Backups

3-2-1-1-0 backup rule must be followed during planning of the backup planning. Backups must be not less than daily incremental backups daily and full backups weekly.

Documentation of Decisions

All decisions made during the planning must be documented with justifications.

Server: Logging and Monitoring

https://www.elastic.co/what-is/log-monitoring

https://www.blackduck.com/blog/logging-and-monitoring-best-practices.html

Logging and Monitoring Requirements

All servers, applications and network devices must be configured to log in with the required information according to the Logging and Monitoring Policy:

- System startups and booting
- Operating system and application logins and login attempts
- Attempts to exceed privileges
- Attempts to violate access lists or firewall rules
- Creation or modification of users, user groups, and their rights
- Security-related error messages
- Security mechanism warning messages

Monitoring rules for mentioned aspects must be configured and in case of any of the mentioned events are logged, an alert must be fired that sends a notification to the system administrator.

Log Data Storage

Storage of the Log files must be done on a dedicated storage server. All log files must be encrypted using a strong password and accessible only to the system administrator.

Log Review and Monitoring

Production environment logs must be reviewed weekly. During the review of the login attempts, unusual system behavior, changes in user permissions or groups, system errors must be checked.

Any anomalies must be documented and investigated immediately. In case of security breach detection employees should report the findings to the CEO and COO and inform local authorities.

Access Control and Authorization

Access to security logs must be restricted, access to log files can be granted for troubleshooting purposes only in case log files do not contain any sensitive data.

Server: UPS Integration with Servers

https://blog.enconnex.com/ups-buying-guide-how-to-choose-a-ups

https://upsbuyer.com/blog/post/understanding-integration-maintenance-ups-systems-business-owners/

https://www.dc-group.com/best-practices-in-ups-system-maintenance/

Choosing and Installing UPS unit

Total power demand on the unit must be calculated adding a safety margin of at least 20%. UPS unit should be made by a reputable manufacturer.

UPS must be installed in a suitable environment specified by the manufacturer in official documentation. Sufficient air flow in the installation area must be ensured.

Configuration and Testing

Configuration of the UPS unit if applicable must be made by using official manufacturer guides and documentation.

A simulated power failure test must be done after the installation of the UPS unit when the battery reaches full capacity.

Maintenance

Maintenance must be done referencing guides and documentation provided by the manufacturer.

All actions taken during the maintenance must be documented containing employees’ names, actions taken and reference to the official documentation and guides.

Server: Server Configuration

https://www.hostnoc.com/server-configuration/

Software

Server system and application software must be acquired only from official manufacturers websites, trusted repositories, verified third-party vendors. All acquired software must be documented including URLs, vendor names and version of software.

Document sources, including URLs and vendor names.

In case of installation from packaged source the packages must be compared to the provided hash from supplier.

Configuration According to Manufacturer Recommendations

Review of manufacturer documentation for the server must be done. After the review a checklist must be composed following the recommended setting if they do not compromise the company's security requirements. Following the checklist configure the server.

Baseline Configuration Documentation

Baseline Configuration of the server must be composed including default settings. Documentation must contain a list of installed software, installed software version, system settings, network configuration, security configuration (e.g. server firewall settings).

Installation and Configuration

All installations and configurations must be done without exposing the server to WAN. All installations and configurations must be done using installation manuals and official documentation. Any deviation from manuals and documentation must be documented.

Final review of servers' configuration must be done before putting into operation

Server: Server Network Configuration and Firewall Management

https://www.fortinet.com/resources/cyberglossary/firewall-configuration

Network Configuration

Server must be assigned with a static IP address in the network.

Basic firewall must be enabled.

Firewall Rule Management

Firewall configurations must be documented containing descriptive rule name, affected ports, purpose of the rule, date of creation, date of termination if applicable.

For configuring firewall rules required external or internal services must be identified and rules must be created for all traffic to and/or from the services.

Firewall must be configured in “Whitelist” mode.

Firewall rules must be reviewed after a server decommission or taking into operation.

Server: Server Operations Documentation

https://www.linkedin.com/advice/1/what-most-important-elements-include-server-py1tf#:~:text=Server%20documentation%20is%20the%20process,for%20troubleshooting%20and%20auditing%20purposes

https://www.techtarget.com/searchitoperations/tip/How-to-write-server-documentation

Action Documentation

Every action made on the production environment server must be documented containing commands executed, purpose of the action, actual outcome, employee name.

List of executed commands must be retrieved using the ‘history’ command with sensitive data omitted.

Documentation must be made so all changes are traceable when referring to it.

Server: Server Accident Readiness, Backup and Recovery

https://www.ibm.com/think/topics/backup-disaster-recovery#:~:text=Backup%20and%20disaster%20recovery%20involves,corruption%2C%20cyberattack%20or%20natural%20disaster

https://www.ready.gov/business/emergency-plans/recovery-plan

https://www.liquidweb.com/blog/server-disaster-recovery/

Backup Schedule

The backup schedule must be determined by the server’s purpose and its environment (e.g. production, development)

Full backups in production must be done at least once per week.

Incremental backups in production must be made at least daily.

For other environments a backup schedule must be configured based on necessity and stability of the system.

Encryption of Backups

All backups must be encrypted using strong password.

Recovery Plan

Recovery Plan must be composed for every server that is being backed up.

Recovery Plan must contain at least:

- Introduction
- Recovery Team
- Pre-Recovery Checklist
- Recovery Procedures
- Backup Validation Procedure
- Communication Plan in case of production environments
- Post-Recovery Review

Backup Validation

Backups must be validated after their creation by simulation server restoration from backups.

Results of backup validation and issues during it must be documented.

Server: Server Monitoring

https://thectoclub.com/test-management/server-performance-monitoring/#:~:text=Server%20monitoring%20is%20the%20process,%2C%20firewalls%2C%20and%20so%20on

Monitoring Planning

Before implementing monitoring appropriate monitoring tools, metrics collection tools must be determined.

Every server must be monitored.

Data observability and alerting

Configure metrics visualization which must contain at least:

- CPU usage
- RAM usage
- Disc space usage
- I/O operations
- Network Usage
- System uptime and boot time

- Load average
- Process counts
- List of key services running
- Status of each service

Alert rules for every metric must be configured and notification mechanisms provided to alert systema administrators.

Server: Regular Security Checks

https://www.getastra.com/blog/security-audit/server-security-audit/

https://phoenixnap.com/kb/server-security

Security check prerequisite

Before security check list of servers within company must be reviewed. Server from the list must be categorized as internal or public exposed. Automated auditing tools are preferred for security checks.

Basic Security Testing Checklist

- Review that all user accounts comply with their roles and password policies
    - Document:
        - User ID
        - User permissions and groups
        - Compliance with password policies
- Identify and review accounts that have not been used for a period
    - Document:
        - User ID
        - User permissions and groups
        - Last user activity
- Based on account reviewed take appropriate actions
    - Document:
        - User ID
        - User permissions and groups
        - Suspended, deleted accounts
- Review system services that are currently running on each server
    - Document:
        - Service name
        - Service purpose
- Review public-exposed servers network configuration
    - Document:
        - Ports, listening addresses
        - Service that utilizes specific port

- Scan public-exposed servers ports
    - Document:
        - Scan results
- Review if all monitoring and alerting systems are operational
    - Document:
        - Monitoring and/or Alerting system name
        - Monitoring and/or Alerting status

Results of the checks must be always documented, even if non-compliances are not found.

Non-compliances found during security checks must receive security risk classification (e.g. high, low).

Remediation Actions

Each vulnerability or non-compliance must be fixed immediately after security checks are completed. Remediation actions that have been taken to fix the vulnerability must be documented containing actions to fix the vulnerability, justification, employees name and date. After fixing the vulnerability server configuration documentation must be updated.

Server: Server Decommissioning

https://www.dataknox.io/server-management/server-decommissioning

https://serverlift.com/blog/how-to-decommission-a-data-center-server/

Notification

Before the servers decommissioning process starts a formal notification must be sent to relevant users and stakeholders. Notification must contain reasons for decommissioning, date of decommissioning and any potential downtime that may occur because of decommissioning.

Preparation for Decommissioning

All critical data must be identified on the server, which includes logs if the log persistence is required by the SLA. All critical data must be documented containing the type of data, timestamp.

A full backup of the identified critical data must be done before the decommissioning. Backup integrity and availability must be checked immediately after the backups are done.

If applicable relevant services for servers' purpose must be identified, documented, and migrated to the new server.

Decommissioning Process

Server must be decommissioned only if the new environment is ready and operational.

The new environment must be tested before decommissioning and approved for operational use by system administrators.

Shutdown of old environment must be done outside peak users time frame to minimize downtime.

Servers service and applications must be shutdown before decommissioning. Finally, a full backup of the server must be done to provide restoring point in case of the new environment failing.

For physical servers all cables and attached devices must be removed before removing the server from its location.

Network diagrams, inventory lists and relevant documentation must be updated to reflect the server decommissioning.

Server: Server Data Storage Encryption

https://cloudian.com/guides/data-protection/data-encryption-the-ultimate-guide

https://www.newsoftwares.net/blog/encrypting-data-to-a-server-a-comprehensive-guide

Initial Preparation

All data storage devices including removable media must be identified and added to the inventory list. Inventory list must contain at least name of the device, serial number, type and capacity.

TPM must be enabled along with Secure Boot in BIOS configuration.

Configuring Data Storage Encryption

While choosing encryption software full-disc encryption capability must be supported by the software.

Software providers’ official documentation and guides must be used during encryption.

For data arrays in virtualized solutions if applicable built-in encryption must be used.

All actions taken during encryption must be documented omitting sensitive information.

Encryption Key Management

Each storage device must be encrypted using different encryption keys. It is prohibited to reuse encryption keys. Only strong algorithms must be utilized for encryption key creation.

Encryption keys must be stored securely and encrypted. It is allowed to store encryption keys in encrypted ID containers.

Encryption key access must be granted only to authorized personnel.

Documentation

Each encryption key must be documented containing key name, type of key, and related data storage device.

Server: Server Operation Documentation Management

Preparation of Server Operation Documentation

Servers type and purpose must be identified before composing documentation.

Local legislation and company policies must be reviewed before composing documentation and check list must be composed to comply.

Restriction of Access

Access to the documentation must be restricted and granted only to authorized personnel.

Employees who require access to the documentation must submit a written request that must contain employee name, role, reason for access and access duration period if applicable. Requests must be reviewed and approved by the system administrator and security specialist.

Versioning and Updating Documentation

Documentation must be versioned; versioning must allow tracking changes and review older versions.

GitLab or Confluence are allowed as versioning solutions.

Review and Update

Documentation must be reviewed annually, and any changes made to the documentation must be complimented with descriptive comments.

Server: Server Boot Security

https://medium.com/@lfoster49203/how-to-implement-and-configure-secure-boot-to-prevent-unauthorized-code-execution-44b2a286850d

Boot Settings Access

Boot settings must be protected with a strong password. Only authorized personnel must have access to Boot Settings.

Firmware Configuration Interface Access

Firmware Configuration Interface must be protected with a strong password. Only authorized personnel must have access to Firmware Configuration Interface.

Secure Boot Support

Operation systems that are used on the server must support Secure Boot.

Secure Boot must be always enabled, with an exception during Operating System installation.

Signing Bootloader and System Kernel

The bootloader and kernel must be signed with a trusted key. Key can be a self-generated certificate.

After signing bootloader and kernel the signature must be validated immediately.

Stored signing keys must be encrypted.

All unused, unnecessary signing keys must be removed from the server.

Server: Encapsulating Security Critical Software and OS Components

Identify Security-Critical Components

An inventory list of all applications and components that handle authentication tokens, certificates, encryption keys, and user credentials must be done.

Documentation based on list must be composed that include name of the component, type of data handled.

Isolated Execution Environments

All the identified components must be isolated using virtualization or containerization.

Containers made for isolation of security critical components must run with restricted privileges.

Base image for containerization must not contain critical and high CVE-s layers.

Components that process untrusted data (e.g. user input) must be containerized.

Linux and Unix Servers

Linux and Unix Servers: Identification Assignment

https://labex.io/tutorials/linux-how-to-handle-linux-user-id-assignment-420754

https://www.freecodecamp.org/news/how-to-manage-users-in-linux/

User and Group Identification Assignment

User and group names must be descriptive and unique.

During user creation UID of the user must be consistent across all servers and environments. Created user or group must be documented.

Documentation must contain Created user UID, user groups, date of creation, commands disabled if applicable.

Linux and Unix Servers: Removable Media Automounting Disabling

Disabling Automount

The service responsible for automounting removable media must be identified.

Before disabling the service impact on the system must be identified.

Service must be always disabled.

After disabling the service automounting must be tested using the companies registered removable media.

Linux and Unix Servers: Application Security

https://www.techtarget.com/searchdatacenter/tip/Compare-two-Linux-security-modules-SELinux-vs-AppArmor

https://tuxcare.com/blog/leveraging-selinux-and-apparmor-for-optimal-linux-security/

Enabling Crucial Services

ASLR, DEP/NX, SELinux, AppArmor must be installed on the server.

ASLR must be configured to full randomization.

ASLR, DEP/NX must be enabled and loaded into the kernel as modules.

SELinux, AppArmor services must be enabled.

Linux and Unix Servers: Secure Software Package Installation

Preparation for Software Package Installation

List of required packages with versions must be composed before installation.

Documentation based on list must contain package name, package version, URL of the package if applicable, package supplier.

Installation

Hash must be compared in case of manual download from a supplier website.

A package version must be provided when installed using the package manager.

Packages that are supplied as source code must be compiled using non-privileged users only.

If applicable, a service for compiled packages must be created.

Linux and Unix Servers: Group and User Management

https://www.redhat.com/en/blog/linux-user-group-management

https://medium.com/@workofviswa/user-and-group-management-in-linux-c652a8ece739

User Creation

User must be created using 'useradd' command.

User UID must be assigned according to the Identification Assignment procedure.

User Deletion

User directory must be backed up before deletion.

User must be deleted using 'userdel' command.

User Modification

User must be modified using 'usermod' command.

Creating a New Group

Group must be created using 'groupadd' command.

Deleting a Group

Group must be deleted using 'groupdel' command.

Adding a User to a Group

User must be added to the Group using ‘usermod’ command.

Configuration Files Management

Editing /etc/passwd, /etc/shadow, /etc/group is prohibited using text editors.

Modifying the sudoers file

/etc/sudoers must be edited only using ‘visudo’ command, editing using text editor is prohibited.

Syntax and changes must be checked before saving changes.

Documentation

Created user documentation must contain username, related employee, user UID, user groups, user permissions and users’ purpose.

Modified user documentation must contain changes made to the user and commands used.

Deleted user documentation must contain deletion cause, commands used, backed directory name.

Created group documentation must contain group names, associated users, purpose of the group, group permission.

Modified group documentation must contain changes made to the group and commands used.

Deleted group documentation must contain reasons for deletion, affected users, commands used.

When adding user to a group documentation must contain username, user UID, reason for addition to the group.

Sudoers file modifications documentation must contain affected users, groups, privileges modifications with their purposes.

Linux and Unix Servers: Secure SSH Configuration and Data Transfer

https://www.digitalocean.com/community/tutorial-collections/how-to-protect-ssh-with-fail2ban

Initial Server Configuration

OpenSSH service must be installed if missing using package manager.

Fail2Ban must be installed and configured according to official documentation and guides.

Configuration of SSH Daemon

Root login via SSH must be always disabled.

Password Authentication must be always disabled, except first configuration connection to the server.

Only v2 SSH protocol must be allowed for SSH communication.

SSH access must be restricted to specific users and/or groups.

SSH configuration file must be documented.

Key Generation and Exchange

Each user must generate a different key for each server secured by a password.
Key addition to the server must be done only by system administrator, using ssh-copy with password for a user is prohibited.

Added keys must be documented containing related user, related employee.

Disable insecure protocols

Any insecure protocols like FTP, Telnet must be disabled.

All disabled services and ports must be documented containing service name, ports affected.

Linux and Unix Servers: Privilege Escalation Prevention

LXC and docker containers must be reviewed for vulnerability and their impact on the system.

Vulnerabilities must be eliminated before deployment.

Found vulnerabilities and remediation actions must be documented.

Virtualization

Virtualization: Virtualization Implementation

Prior analysis

Hardware prior to installation of virtualization solution must be checked: CPU for virtualization support, RAM amount for sufficiency, network interfaces for sufficient throughput.

A list of appropriate virtualization solutions must be composed prior to implementation. Final decision of choosing virtualization solution must be justified and documented.

Access Control and Privilege Management

Role-based access control must be established and configured.

Users must be assigned roles according to Principle of least privilege.

Roles must be documented with related employee name and privileges granted.

Continuous Monitoring

Continuous Monitoring must be established and configured to collect at least performance metrics, security events and resources utilization.

For each collected metric an alert rule must be configured to send out alerts to system administrators.

Virtualization: Virtualization Environment Security Configuration

Network Segmentation and Firewall

A management network for management of virtualization host must be established.

VLANs of guest systems must be configured to have no access to the management network of the host.

Host firewall must be configured to deny all incoming traffic from guest systems with the exception of essential protocols used for management.

Management interface must be configured to allow traffic only from whitelisted IP addresses.

Persistent Data Storage Volume Creation and Host System File Access

Guest systems are allowed to create persistent data storage volumes and utilize them if necessary.

Allocating virtual disks to guest systems must be preferred over persistent data storage creation.

Guest systems are allowed to access time zone configuration files. Access must be configured in read-only mode.

Virtualization: Virtualization Management System Security

Administrative Access Control

Administrative access to the Management System must be restricted to designated personnel only.

All employees who have access to the Management System must be documented containing the employees’ name and servers’ name.

Access Granting Process

A written access request must be submitted containing the employee's name, servers name and reason for access.

The system administrator must review the access request.

Network Security for Management System Interface

Access from outside companies' networks must be restricted.

It is prohibited to expose Management System Interface to WAN.

Users must connect using companies VPN software.

Only secure connection protocols for management must be used (e.g. HTTPS, SSH).

Virtualization: Procedures for Virtualization System Logging

Monitoring Virtualization Host System State

Monitoring tools must be configured to constantly monitor the state of the host.

Metrics must be collected containing at least CPU usage, RAM usage, Storage usage, Disk I/O, Network I/O.

Alert rules must be configured to fire alarms and notifying the system administrator for each metric.

Guest System Resource Usage Monitoring

Resource Usage Monitoring must be configured for each guest system.

In the event of the exhaustion of host resources troubleshooting must be done and if no errors are found a relocation of the guest system must be considered.

Review of Virtualization Host System Logs

Weekly review of logs must be done.

Anomalies detected during review must be documented and addressed immediately.

Virtualization: Virtualization System Time

Synchronization of Virtualization System Time

All guest systems' time must be synchronized.

The NTP server must be configured on the host system.

All guest systems must be configured to use the same NTP server as host system.

Virtualization: Virtualization System Architecture Planning

Define Requirements

List application and services must be composed.

A review of companies' policies and local legislation must be done and documented containing affected requirements.

Based on review of requirements, it determines the impact on the design.

Architecture Design Draft

Composed drafts of the design must contain hardware requirements, network diagram, storage requirements, security measures (e.g. firewall rules, upgrade management).

Drafted design must be approved before implementation.

Unified Security for Multiple Guest Systems

In the case of multiple guest systems, their security must be aligned by the highest required security requirements.

Automated configuration must be used to consistently apply configuration across all guest systems.

Continuous Monitoring

Integration with monitoring solutions must be considered when composing the draft.

Virtualization: Virtualization System Network Architecture Planning

Requirements Gathering

Review of virtualization implementation plan must be done and possibility in purpose-based network segmentation considered (e.g. Storage Network, Management Network).

Network Isolation and Security

Network diagrams must be composed for each LAN and VLAN.

Firewall rules must be predefined for each LAN and VLAN.

Virtualization: Virtualization Infrastructure Maintenance Rights and Roles

Roles Establishment

Roles for employees that are authorized to access Virtualization Infrastructure must be established.

At least Administrator and Read-Only user roles must be established.

Required Access Rights

Administrator role must be configured to have full rights over Virtualization Infrastructure.

Read-Only user rights must be limited to only view configuration with an exception to sensitive data.

Review and Approval Process

Employees must submit a written request for access that contains employees' name, virtualization infrastructure name and reason for access.

Every access request granted must be documented containing employees' name, virtualization infrastructure name and reason for access.

Virtualization: Virtualization Infrastructure Unified Configuration Requirements

Standard Configurations

Unified Configuration must be composed. Unified Configuration must comply with local legislation and the security requirements of the guest system.

Host and Guest system can be configured with the same configuration if the security requirements match.

Automated Configuration tools must be used for configuration.

Configuration Review

Unified Configuration must be reviewed at least annually. Non-compliances found during the review must be documented and fixed.

Any changes in unified configuration must be tested.

Virtualization: Isolation of Virtual Guest with Different Security Requirement

https://www.vpnunlimited.com/help/cybersecurity/hardware-enforced-virtualization?srsltid=AfmBOooRS4DSE3kB-BNEjpfEdEDv0HqYkbdFs43QYDHtAOEo2wa9gj0m

Isolation

Guest systems must be always isolated.

Any exception must be documented and justified.

Guest systems with different security requirements are prohibited from using resource sharing.

Hardware enforced virtualization must be enabled.

Files transfer between guest systems must be disabled.

Virtualization: Virtualization Server Resource and Configuration Checks

Resource Sufficiency of the Virtualization Host System

Review of metrics must be done for guest systems weekly.

CPU usage, Memory usage, Disk I/O, Network I/O must be reviewed. Resource exhaustion must be documented and additional resource allocation considered.

Before allocating new resources to the guest systems, resource overlap absence must be confirmed.

Monthly reports on resource utilization must be done.

Testing Configuration Changes

All changes to the configuration must be made before deploying to the production environment.

Configuration Changes must be documented containing changeset and justification.

Configuration Changes must be approved by system administrator.

Old configuration must be backed up.

Virtualization: Virtualization System Regular Checks

Regular Review

Regular Review must be scheduled and planned.

Check list of common metrics, log files must be composed.

Regular review frequency must be environment-based (e.g. production, test).

Production environment must be checked not less than once weekly.

Configuration and environment variables must be checked.

Anomalies and non-compliances must be documented and fixed immediately.