CompTIA Security+ Exam SY0-701

Lesson 7

Explain Resiliency and Site Security Concepts

Lesson 7

Topic 7A

Asset Management

Asset Tracking

- Assets
  - Anything with value!
  - Cyber asset tracking is IT centric
- Assignment and Ownership

Asset Tracking

- Asset Tracking and Monitoring
- Manual Inventory
- Network Scanning
- Asset Management Software
- Configuration Management Database (CMDB)
- Mobile Device Management (MDM)
- Cloud Asset Discovery

Asset Protection Concepts

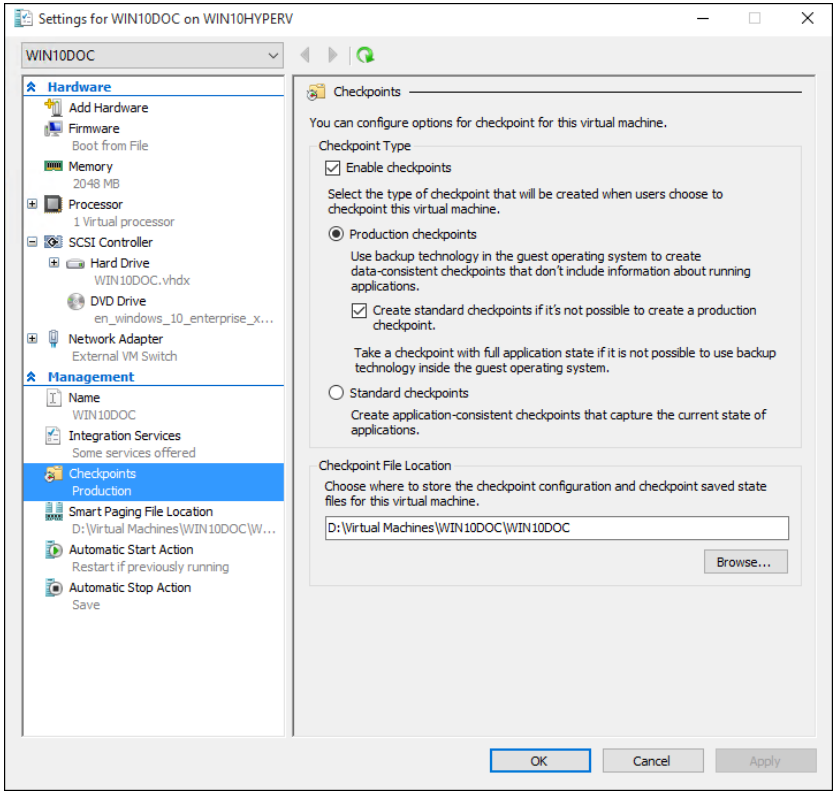
- Identify and prioritize assets based on sensitivity and impact
- Standard naming convention
- Configuration management
- Change control and change management

Data Backups

- Ensure the availability and integrity of an organization's critical data and systems
- Simple backups vs Enterprise Data Protection Strategy
- Critical capabilities for enterprise backup solutions typically include:
  - Support for various environments (virtual, physical, and cloud)
  - Data deduplication and compression to optimize storage space
  - Instant recovery and replication for quick failover
  - Ransomware protection and encryption for data security
  - Granular restore options for individual files, folders, or applications
  - Reporting, monitoring, and alerting tools for effective management
  - Integration with virtualization platforms, cloud providers, and storage systems
  - Encryption to protect copies of sensitive data stored in backup sets

Advanced Data Protection

- Snapshots
- VM snapshots
- Filesystem snapshots
- SAN snapshots



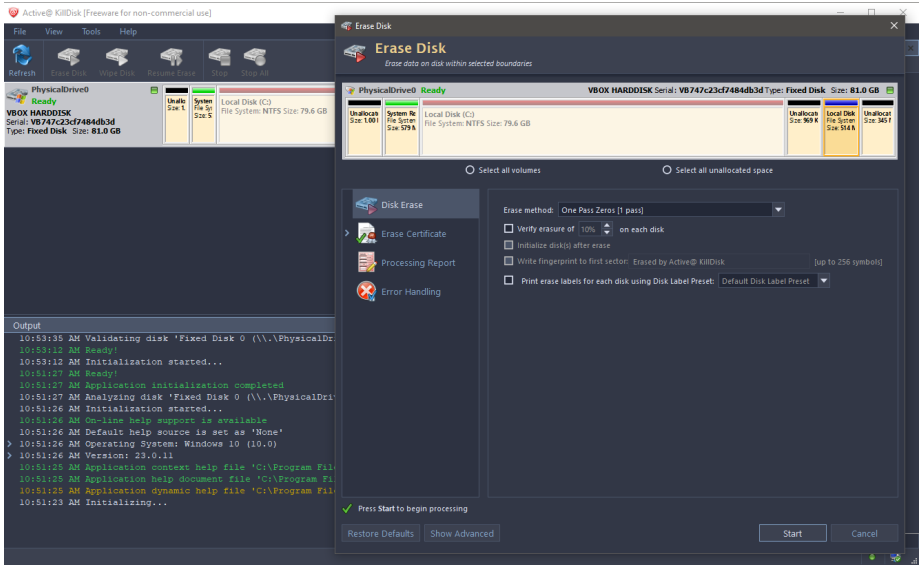
The checkpoint configuration section for a Hyper-V virtual machine. Checkpoints refer to Microsoft's implementation of snapshot functionality. (Screenshot used with permission from Microsoft.)

Advanced Data Protection

- Replication and Journaling
- Database mirroring
- SAN replication
- VM replication

Secure Data Destruction

- Asset Disposal
- Sanitization
- Destruction
- Certification



Active KillDisk data wiping software. (Screenshot used with permission from LSoft Technologies, Inc.)

Review Activity: Asset Management

- Asset Tracking
- Asset Protection Changes
- Data Backups
- Advanced Data Protection
- Secure Data Classification

Lab Activity

- Applied Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization

Lesson 7

Topic 7B

Redundancy Strategies

Continuity of Operations

- Ensuring that an organization can maintain or quickly resume its critical functions in the event of a disruption, disaster, or crisis
- Regular testing and updating of continuity of operations plans (COOP) are crucial to ensure the organization can maintain essential functions during and after disruptive events
- Backups play a critical role in the continuity of operations plans (COOP) by safeguarding against data loss and restoring systems and data in the event of disruptions
- Capacity planning is a critical process in which organizations assess their current and future resource requirements to ensure they can efficiently meet their business objectives

Capacity Planning Risks

- People Risks
- Cross-Training
- Remote Work Plans
- Alternative Reporting Structures

- Changes in Workforce Capacity
- Rapid hiring
- Layoffs

High Availability

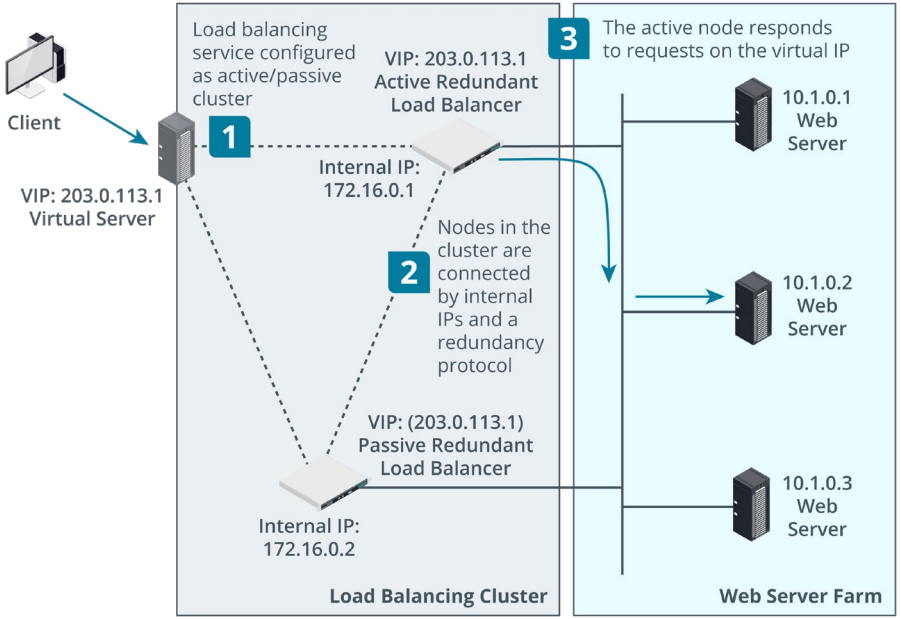
- High Availability
- Scalability and Elasticity
- Fault Tolerance and Redundancy
- Site-level Resiliency
  - Hot
  - Warm
  - Cold
  - Cloud

High Availability

- Testing Redundancy and High Availability
- Load Testing
- Failover Testing
- Validate Monitoring Effectiveness
    - Do warning alerts/notifications work?

Clustering

- Multiple redundant processing nodes that share data with one another
- Virtual IP
- Active/Passive (A/P)
- Active/Active (A/A)
- Application Clustering



Topology of clustered load balancing architecture. (Images © 123RF.com.)

Power Redundancy

- Dual Power Supplies
- Managed Power Distribution Units (PDUs)
- Battery Backups and Uninterruptible Power Supplies (UPSs)
- Generators

Diversity and Defense in Depth

- Platform diversity
- Multi-Cloud
- Vendor Diversity
  - Cybersecurity
  - Business Resilience
  - Innovation
  - Competition
  - Customization and Flexibility
  - Risk Management
  - Compliance

Deception Technologies

- Honeypots
- Honeynets
- Honeyfiles
- Honeytokens
- Fake telemetry

Testing Resiliency

- Tabletop Exercises
- Failover Tests
- Simulations
- Parallel Processing Tests
- Robust Documentation

Review Activity: Redundancy Strategies

- Continuity of Operations
- Capacity Planning Risks
- High Availability
- Clustering
- Power Redundancy
- Diversity and Defense in Depth
- Deception Technologies
- Testing Resiliency

Lesson 7

Topic 7C

Physical Security

Physical Security Controls

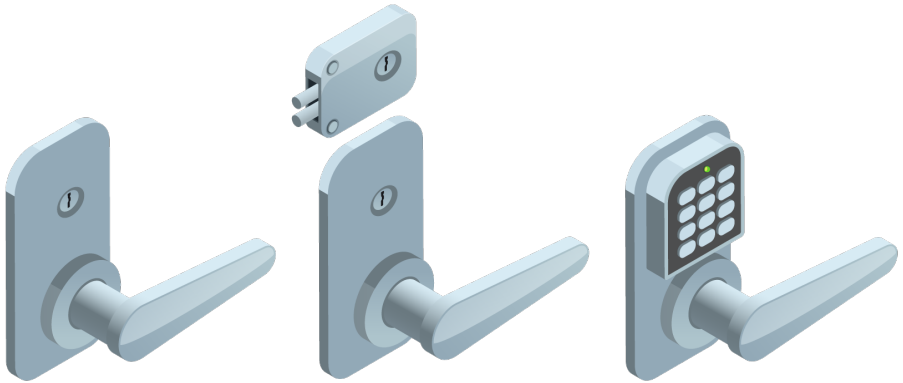
- Provides the first line of defense against physical access to an organization's critical assets

- Protect physical components that store assets, such as
- Servers & Equipment
- Datacenters
- People
- Other critical infrastructure

Site Layout, Fencing, and Lighting

- Physical Security Through Environmental Design
- Barricades and Entry/Exit Points
- Fencing
- Lighting
- Bollards

Gateways and Locks



Generic examples of a biometric thumbprint scanner lock and a token-based key card lock. (Images from user macrovector © 123RF.com.)

- Physical
- Electronic
- Access Control Vestibule (Mantrap)
- Cable Locks
- Access Badges

Security Guards and Cameras

- Surveillance (CCTV)
- Motion Recognition
- Object Detection
- Drones/UAV

CCTV installed to monitor a server room. (Image by Dario Lo Presti © 123RF.com.)

Alarm Systems and Sensors

- Alarms Types
  - Circuit
  - Motion Detection
  - Noise Detection
  - Proximity
  - Duress
- Sensor Types
  - Infrared
  - Pressure
  - Microwave
  - Ultrasonic

Review Activity: Physical Security

- Physical Security Controls
- Site Layout, Fencing, and Lighting
- Gateways and Locks
- Security Guards and Cameras
- Alarm Systems and Sensors

Lesson 7

Summary