# Lesson 20

Implementing Cybersecurity Resilience

# Topic 20A

## Implement Redundancy Strategies

# Syllabus Objectives Covered

- 2.5 Given a scenario, implement cybersecurity resilience

# High Availability

- Maximum tolerable downtime (MTD)
- Scheduled service intervals versus unplanned outages
- Scalability
  - Increase capacity within similar cost ratio
  - Scale out versus scale up
- Elasticity
  - Cope with changes to demand in real time
- Fault tolerance and redundancy

| Availability | Annual Downtime |
|---:|---:|
| 99.9999% | 00:00:32 |
| 99.999% | 00:05:15 |
| 99.99% | 00:52:34 |
| 99.9% | 08:45:36 |
| 99.0% | 87:36:00 |

# Power Redundancy

- Power problems
  - Spikes and surges
  - Blackouts and brownouts
- Dual power supplies
  - Component redundancy for server chassis
- Managed power distribution units (PDUs)
  - Protection against spikes, surges, and brownouts
  - Remote monitoring
- Battery backups and uninterruptible power supply (UPS)
  - Battery backup at component level
  - UPS battery backups for servers and appliances
- Generators

# Network Redundancy

- Network interface card (NIC)/adapter teaming
  - Adapters with multiple ports
  - Multiple adapters
  - More bandwidth (except during failover)
- Switching and routing
  - Design network with multiple paths
- Load balancers
  - Load balancing switch to distribute workloads
  - Clusters provision multiple redundant servers to share data and session information

# Disk Redundancy

- Redundant array of independent disks (RAID)
- RAID 1
  - Mirroring
  - 50% storage efficiency
- RAID 5 and RAID 6
  - Striping with distributed parity
  - Better storage efficiency
- Nested RAID
  - Better performance or redundancy
- (RAID 0)
- Multipath
  - Controller and cabling redundancy

# Geographical Redundancy and Replication

- Replication context
  - Local storage (RAID)
  - Storage area network (SAN)
  - Database
  - Virtual machine (VM)
- Geographic dispersal
- Asynchronous and synchronous replication
  - Synchronous (must be written at both sites—expensive)
  - Asynchronous (one site is primary and the others secondary)
  - Optimum distances between sites
- On-premises versus cloud

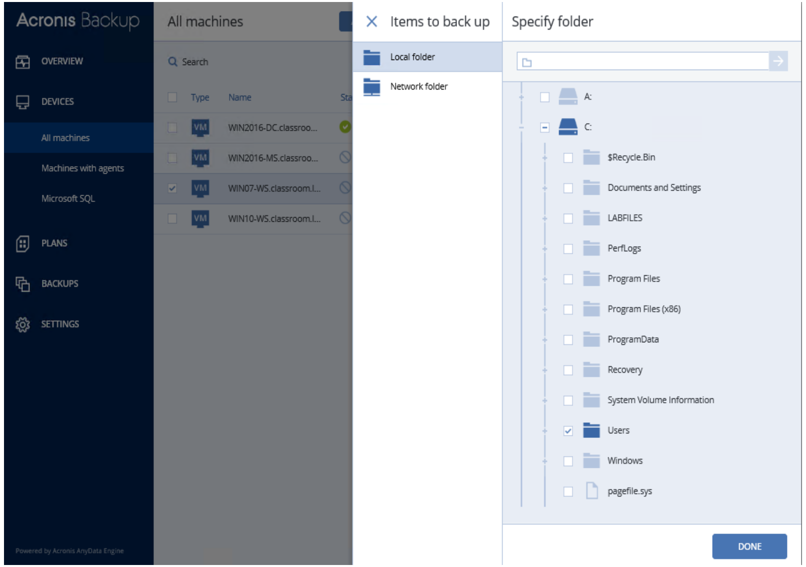
# Topic 20B

Implement Backup Strategies

# Syllabus Objectives Covered

- 2.5 Given a scenario, implement cybersecurity resilience

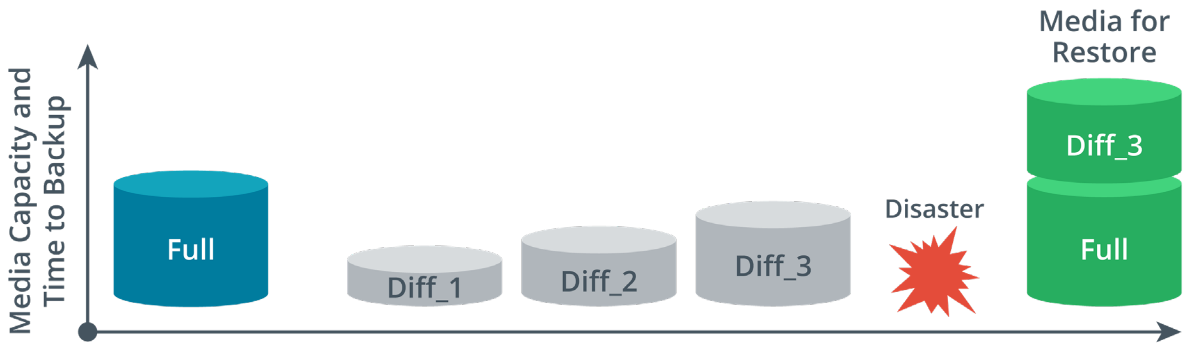
# Backups and Retention Policy



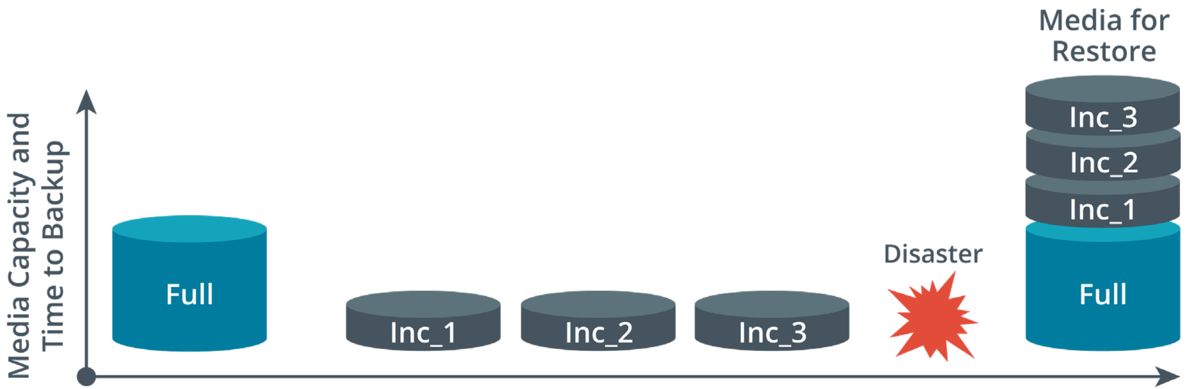
*Screenshot used with permission from Acronis.*

- Short term retention
  - Version control and recovery from corruption/malware
- Long term retention
  - Regulatory/business requirements
- Recovery window
  - Recovery point objective (RPO)

# Backup Types

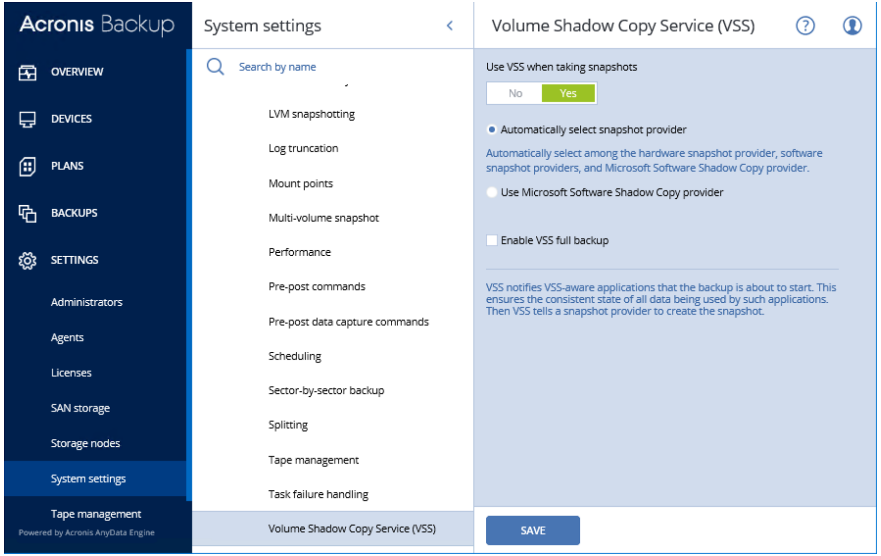


Differential-based Backup Schedule



Incremental-based Backup Schedule

# Snapshots



Volume Shadow Copy Service (VSS)

Use VSS when taking snapshots

No [✓ Yes]

● Automatically select snapshot provider

Automatically select among the hardware snapshot provider, software snapshot providers, and Microsoft Software Shadow Copy provider.

○ Use Microsoft Software Shadow Copy provider

□ Enable VSS full backup

VSS notifies VSS-aware applications that the backup is about to start. This ensures the consistent state of all data being used by such applications. Then VSS tells a snapshot provider to create the snapshot.

*Screenshot used with permission from Acronis.*

- Snapshots
  - Feature of file system allowing open file copy
  - Volume Shadow Copy Service (VSS)
  - VM snapshots and checkpoints
- Image-based backup
  - System images

# Backup Storage Issues

- Backup security
  - Access control and encryption
- Offsite storage
  - Distance consideration
  - Physical transfer
  - Network/cloud backups
- Online versus offline backups
  - Speed of restore operations
  - Risk to online backup data
- 3-2-1 rule

# Backup Media Types

- Disk
  - SOHO backups
  - Lack enterprise-level capacity and manageability
- Network attached storage (NAS)
  - File-level/protocol-based access
  - No offsite option
- Tape
  - Enterprise-level capacity and manageability
- Storage area network (SAN) and cloud
  - Block-level access to storage devices
  - Highly configurable
  - Mix storage technologies to implement performance tiers

# Restoration Order

1. Power delivery systems
2. Switch infrastructure then routing appliances and systems
3. Network security appliances
4. Critical network servers
5. Backend and middleware and verify data integrity
6. Front-end applications
7. Client workstations and devices and client browser access

# Non-Persistence

- Separate compute instance from data
    - Snapshot/revert to known state
    - Rollback to known configuration
    - Live boot media
- Provisioning
    - Master image
    - Automated build from template
- Configuration validation

# Topic 20C

## Implement Cybersecurity Resiliency Strategies

# Syllabus Objectives Covered

- 2.1 Explain the importance of security concepts in an enterprise environment
- 2.5 Given a scenario, implement cybersecurity resilience
- 5.3 Explain the importance of policies to organizational security

# Configuration Management

- Service assets
- Configuration items (CIs)
  - Assets that require configuration management
- Baseline configuration
- Configuration management system (CMS)
- Creating and updating diagrams
  - Workflows
  - Physical and logical network topologies
  - Network rack layouts
  - …

# Asset Management

- Inventory/asset management database
- Asset identification and standard naming conventions
  - Barcodes and RFID tags
  - Standard naming conventions for asset IDs
  - Attribute fields and tags
- Internet protocol (IP) schema
  - Static allocation versus DHCP ranges
  - IP address management (IPAM) software suites

# Change Control and Change Management

- Change control
  - Assess whether a change should be made
  - Classifying change (reactive, proactive, risk)
  - Request for Change (RFC)
  - Change Advisory Board (CAB)
- Change management
  - Ensure changes are applied with minimum disruption
  - Rollback plan

# Site Resiliency

- Alternate processing sites/recovery sites
  - Provide redundancy for damage to resources stored on the primary site
  - Failover to alternate processing site (or system)
- Hot site
  - Instantaneous failover
- Warm site
  - Some delay or manual configuration before failover occurs
- Cold site
  - Significant delay and configuration before failover can occur

# Diversity and Defense in Depth

- Layered security and defense in depth
- Technology and control diversity
  - Provision different classes and types of controls
  - Mix technical, administrative, and physical controls
  - Deploy controls to prevent, deter, detect, and correct
- Vendor diversity
  - Use more than one supplier
- Crypto diversity

# Deception and Disruption Strategies

- Asymmetry of attack and defense
- Active defense
- Fake/decoy assets
  - Honeypots, honeynets, and honeyfiles
  - Breadcrumbs
- Disruption strategies
  - Bogus DNS records
  - Decoy directories and resources
  - Port spoofing to return fake telemetry/monitoring data
  - DNS sinkholes

# Lesson 20

## Summary