Disaster Recovery Plan

Aberdeen School District

Millennium Consulting Service
Updated Aug 9, 2022

Table of Contents

1. Equipment Lists

Below are the core network infrastructure components. Not all equipment is listed.

A. Physical Infrastructure Servers

IP Address	Hostname	Serial	Model	Purpose
10.98.251.80	CMC-4QG2H13	4QG2H13		Dell VRTX CMC
10.98.251.82	iDRAC-4PXXG13		iDRAC 9 Enterprise	VRTX Slot 1 iDRAC
10.98.251.83	iDRAC-4PXZG13		iDRAC 9 Enterprise	VRTX Slot 1 iDRAC
10.98.251.84	iDRAC-4PXYG13		iDRAC 9 Enterprise	VRTX Slot 1 iDRAC
10.98.251.86	VRTX-ESXi1	4PXXG13	Dell PE M640	VMware ESXi Host
10.98.251.87	VRTX-ESXi2	4PXZG13	Dell PE M640	VMware ESXi Host
10.98.251.88	VRTX-ESXi3	4PXYG13	Dell PE M640	VMware ESXi Host

B. Virtual Infrastructure Servers

IP Address	Hostname	Purpose
10.98.251.10	ASD-DC4	Domain Controller
10.98.251.11	ASD-DC5	Domain Controller
10.98.251.13	ASD-DHCP	DHCP Server
10.98.251.12	vCenter	VMware vCenter Server
10.98.8.12	ASD-FS1	File Server
10.98.251.31	ASD-RADIUS	RADIUS Server
10.98.251.29	ASD-Vipre	Antivirus Server
10.98.251.34	ASD-Veeam	Backup Server

C. Network

IP Address	Hostname	Serial	Model	Purpose
10.98.0.9		FG6H1ETB21908675	Fortinet FortiGate 601E	Firewall
10.98.251.81			R1-2210	VRTX Internal Switch
10.98.251.1			Cisco C3750X	AHS Core
10.98.99.4			Cisco C3750X	Resource Center MDF

D. Other Equipment

IP Address	Hostname	Serial	Model	Purpose
10.98.251.5		APM00143504322	EMC VNXe 3200	Production SAN
10.98.99.10		12080164	Cybernetics iSAN	Backup SAN

2. Configuration Overview

The server infrastructure, core switch stack, and production SAN are in the Aberdeen High School server room located adjacent to the gym.

The backup SAN, which contains the Veeam virtual machine and its backup storage, are located in the Resource Center.

Backups of all servers are taken every weeknight.

The backup server and SAN use strong, unique passwords. The backup server is not joined to Active Directory and has strict firewall rules preventing access from most other systems on the network.

3. Disaster Recovery Plans

The following steps would be necessary depending on the type of incident.

A. Loss of Server Room

Loss of the AHS server room would result in a complete network and server outage.

1. Set up one or more replacement VMware ESXi servers.
2. Route needed AHS subnets to new location.
3. Connect iSCSI backup SAN datastore.
4. Add ASD-Veeam virtual machine to a server's inventory and boot it up.
5. Restore VMs as needed from backup to replacement ESXi servers.

B. Loss of Resource Center

Loss of the resource center would not directly impact network viability or production servers.

1. Set up replacement backup storage server or SAN.
2. Create new Veeam VM.
3. Set up and run new backup jobs.

C. Data Corruption/Accidental Deletion

1. Files can be recovered fastest from volume shadow copies on some servers.
2. All server backups support file-level recovery from any available recovery point.

D. Server Malware Attack

1. Determine the extend of the attack and take all affected servers offline.
2. If server security can be reasonably assured, necessary data should be migrated to new servers, and the old servers should be decommissioned.
3. If server security cannot be reasonably assured, they should be kept permanently offline until wiped and restored from backup. Servers restored from backup should be checked for viruses before attaching to the network. This can be done by Veeam as part of the restore process.

E. Workstation Malware Attack

1. Any workstation found to have been infected by malware should be wiped and reloaded.
2. The files and portable media of affected users should be scanned for viruses.
3. The users should change their passwords and use two-factor authentication where possible.