Nerd Platoon Cloud Migration - Group 42

Scope Statement

Project Scope Description

Group 42 will create and deliver a stable and secure cloud based network with an organized Active Directory and easily manageable databases in Azure. These include an Active Directory server, a File Server, and a DNS server

Project Objectives

To create a remotely accessible and secure cloud based network, complete with all the needed IT infrastructure including an Active directory, domain level services and both server and client configuration.

Requirements

The new network will have an Active Directory server running in the cloud on a cloud virtual machine. It will also use a Route53 for DNS and Amazon S3 to serve files. NP would also like to have a database server and web application server in order to support a hosted help desk system called osTicket. These will be on a separate network from the active directory network. Only the web server will have public accessibility.

In Scope

- Networking design, configuration, and setup
- Domain level services including:
    - Active Directory
    - DNS
    - Company-Wide ad-block
    - Web and database
    - VPN
- All servers' configuration and security
- Clients' configuration and security
- Working with other vendors as necessary

Out of Scope

- Management of the Active Directory
- Security of remote machines

Deliverables

The five servers located on the two networks detailed in the requirements. Additionally Group 42 will ensure the implementation of the the following requested features:

Technical requirements

- Windows users should be able to login to domain computers
- Users must use complex passwords and must change their passwords every 180 days.
- A designated group will be given VPN access. VPN users will have access to the resources that they normally have access to.
- The web server be running OSTicket with a public-facing IP address its database on the internal MySQL server with no direct public access.

Security

- Clients running Windows 10 will use Windows Defender antivirus.
- All servers will need to be hardened.
- Only identified and appropriate ports will be opened
- All the latest security updates for servers must be applied
- Self-signed certificates are acceptable where a certificate is needed. The self-signed certificate should be added to the Trusted Root Certificates Computer Setting and deployed to all domain computers via group policy.
- LetsEncrypt certificate should be set up and installed on the web server.

Milestones

Server Infrastructure	Completed NLT 10/31/2022
Active Directory	Completed NLT 11/24/2022
Migration and User Templates	Completed NLT 12/12/2022