System Security and Policy Implementation

COSCare

Jacob Metcalfe

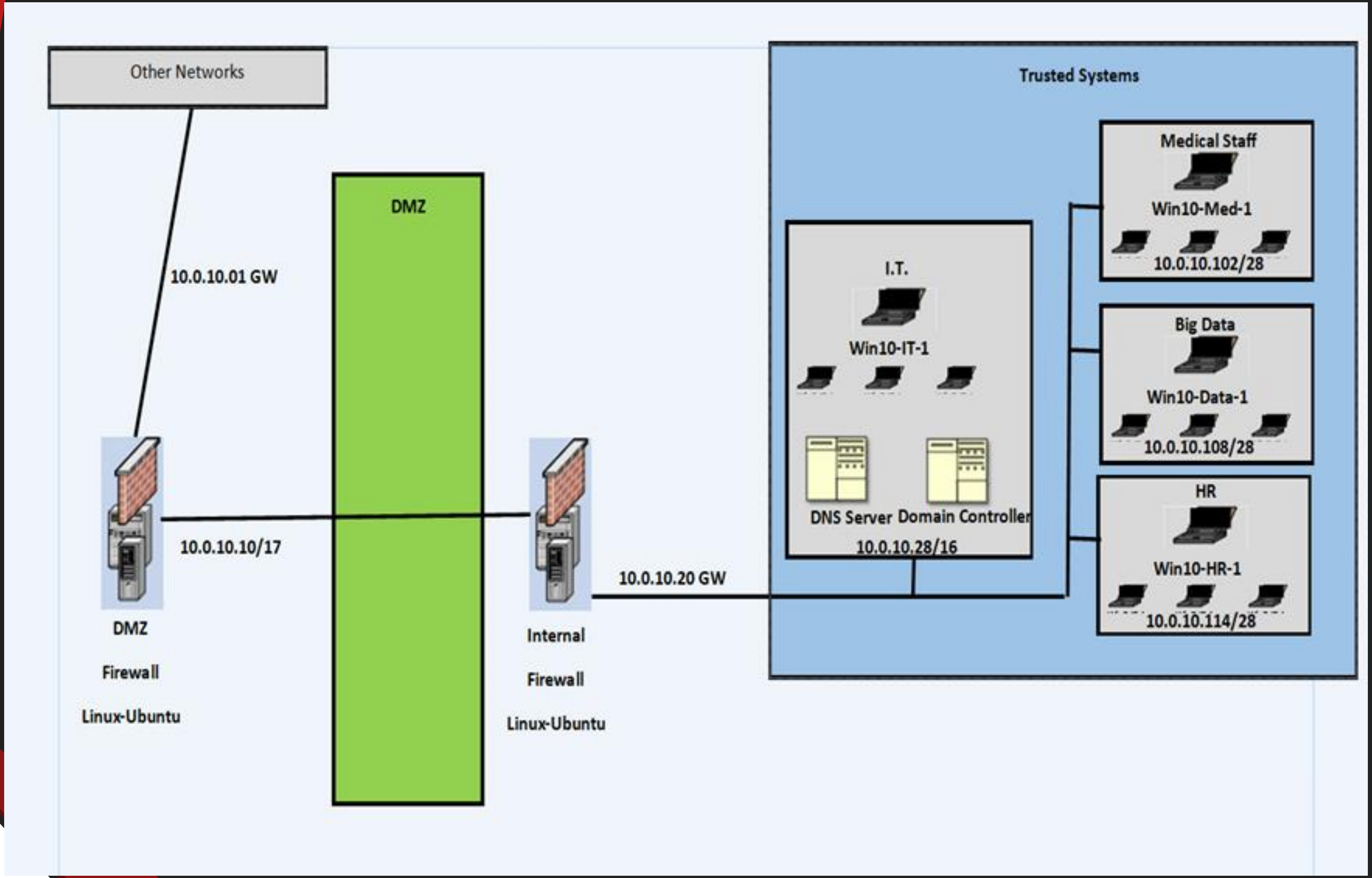
Who We Are

COS Care is a full-service care facility in Colorado Springs, Colorado. We have staff from all over Colorado, including medical staff, HR, IT, and a new Big Data team. The Big Data team is responsible for ensuring that the outbreaks are stopped at the quickest possible time and that vaccinations/masks are ordered as soon as an outbreak appears. In the future. A software development team is to come that will make products with the Big Data team to ensure COS Care can respond to all problems medical.

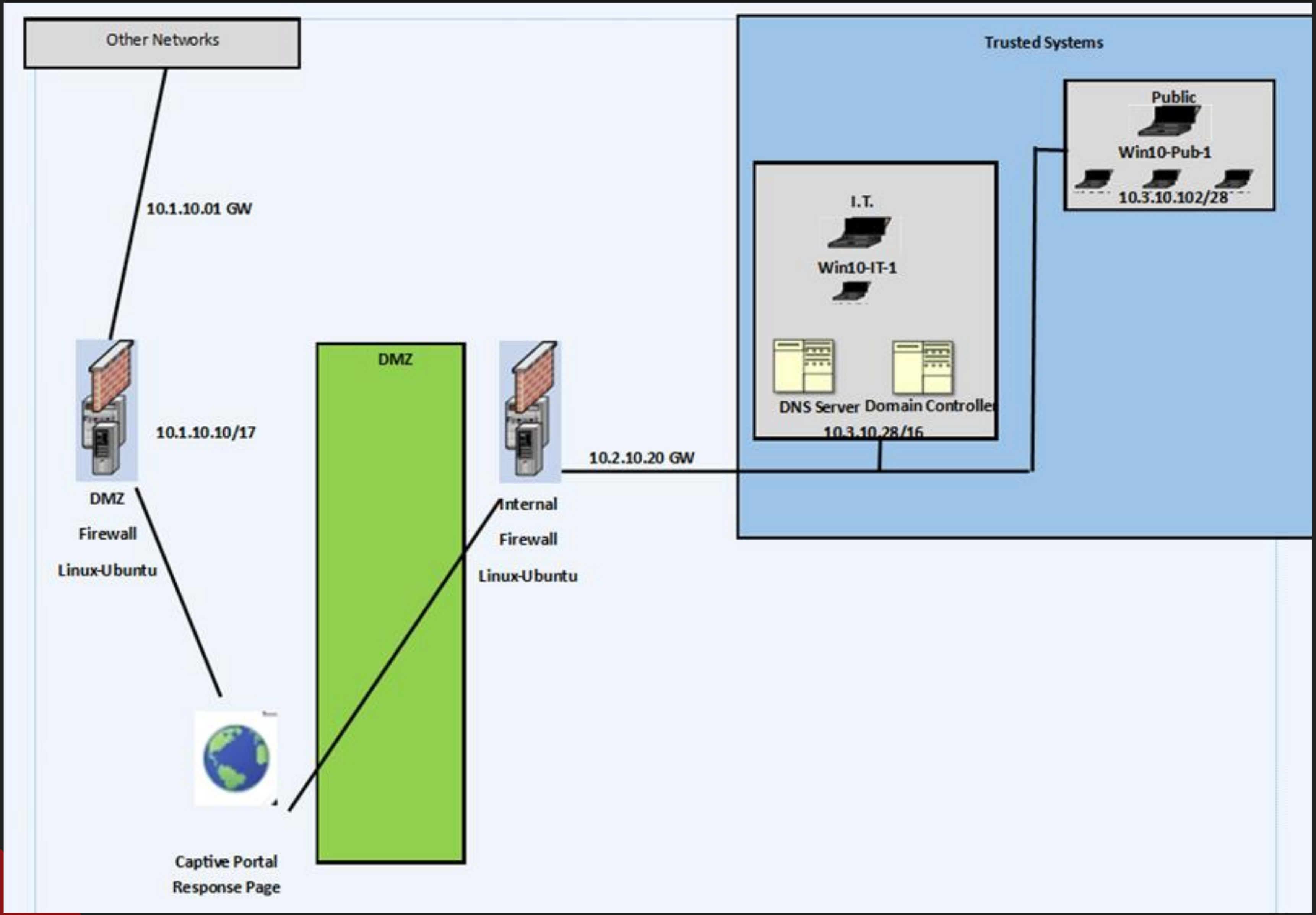
The COS Care is creating a new infrastructure for the hospital to ensure Personal Health Information is always secure , while also allowing guests to use our network. This presentation and network document was made exclusively by COS Care internally to ensure that this goal becomes a reality.

Currently, everyone within the group has a job and we looked at the IT policies already set in place and adapted off of there. We listed everything needed in an IT infrastructure and chose the most important pieces to add to the document/project.

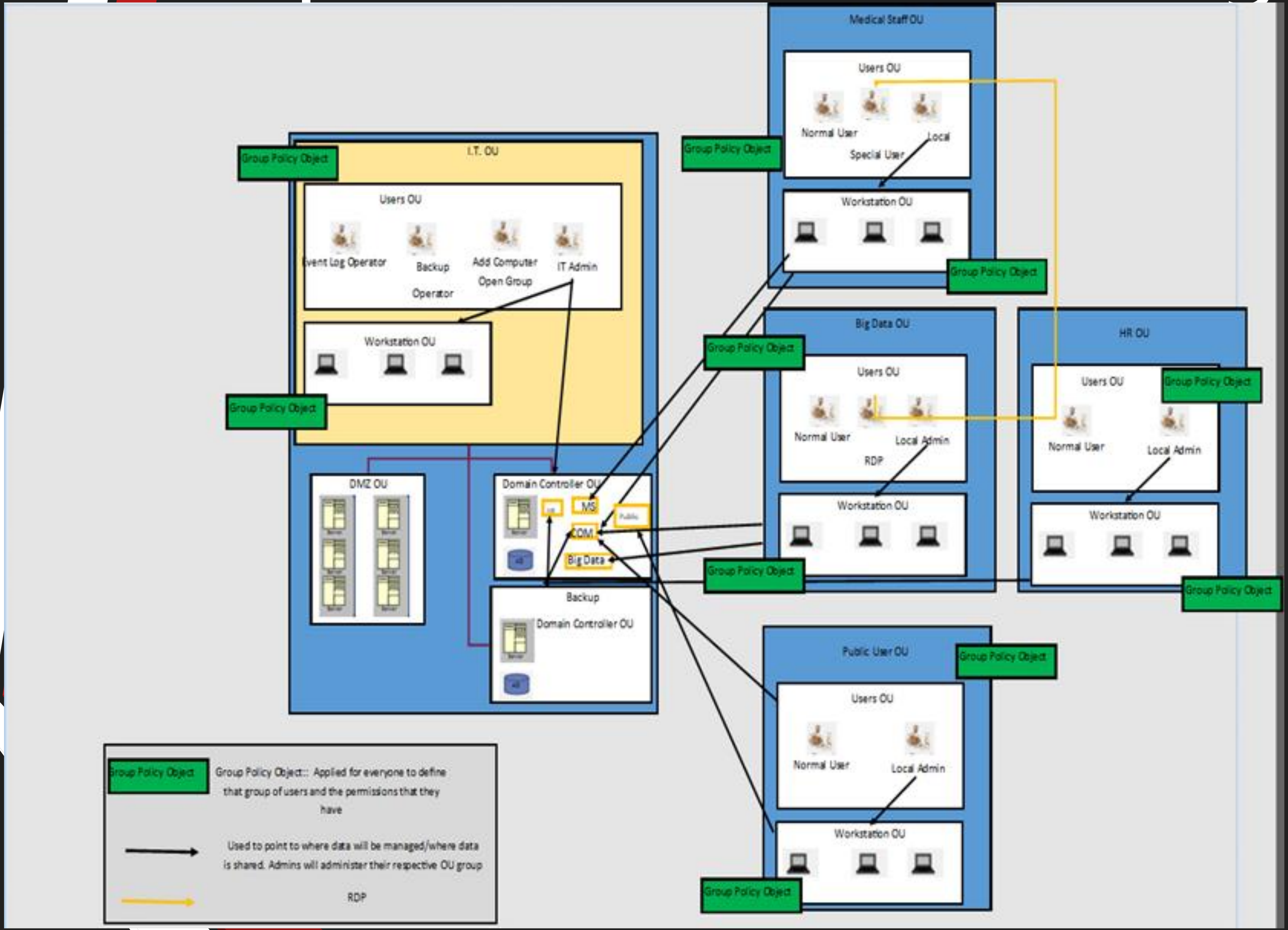
Proposed COS Care Network Topology



Proposed COS Care Guest Network Topology



Proposed Business Design



Group Policy Object:: Applied for everyone to define that group of users and the permissions that they have

Used to point to where data will be managed/where data is shared. Admins will administer their respective OU group

RDP

Key Features

- Statistical Data from the medical staff is reported to a separate computer for big data analysis via RDP.
- Technical Policy to use batch scripts for ensuring permissions and respective department group policy.
- Each department has own Local IT Admin ensuring success among all department specific systems.
- Each department has own network share to ensure proper bandwidth usage and allocation when needed.

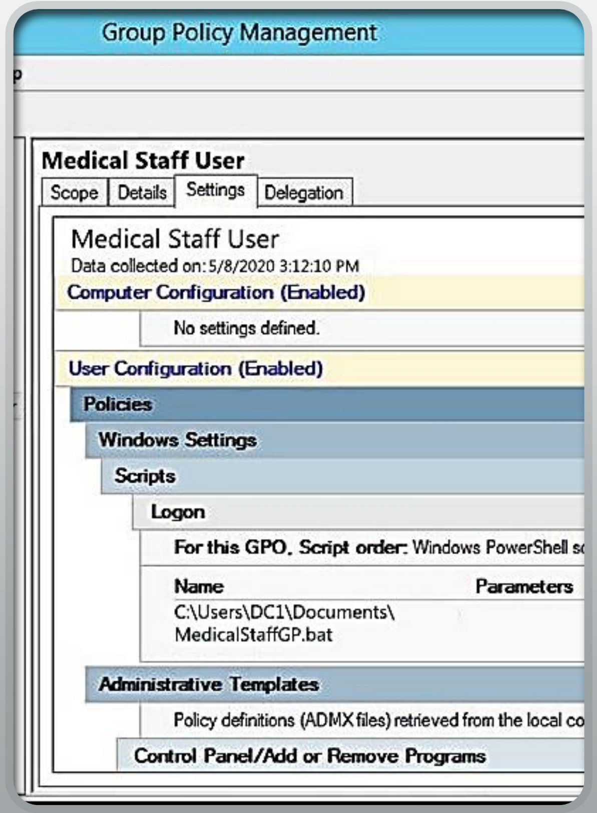
Requirement	Design
Department will have two Domain Controllers (DCs) set up in a way that keeps the system up and running in the event of having one of those DCs down.	Backup Controller added to COS Care forest.
IT department crew is composed of system administrator, a person responsible of backups scheduled every weekend, another one that monitors the logs of the system, and finally a person that joins workstations into the system.	User Roles added to Linux roles, and logic diagrams.
There are local administrators for each of the departments, excluding the IT. These local administrators will use the local administrator account on each department to add local user accounts via scripts that will read the new users' credentials from a text file. These local administrators will use a local account on each department for purposes of installing applications, updating/patching software, etc. This local account is not the administrator account, but a user account that is member of the local administrator's group.	Local IT Admins added to sudoers file and logic file and has access to their respective group policy.
For auditing purposes, the person that joins workstations into the system uses three different accounts: one account for the IT department, and one account for each of the remaining departments	Auditor has credentials to every department according to audit policy.
Departments, excluding IT, will have accounts for normal users. Those users cannot remotely access the workstations in those departments. However, there is a need of having a special account used in one department to remotely access workstations in the other department, i.e. an account that allows a user in department A to remotely access workstations in department B.	Big Data can access statistical data in Medical Staff through port 3389.
Normal users cannot install/uninstall applications on their workstation.	From AUP and group policy, users cannot install applications on their workstations, must be done by IT Admin.
System administrator can remotely access the DCs	DCs on Linux with port 22 open for the IT Department only.

Requirements Review Cont.

Requirement	Design
When a user logs into any workstation, he/she will see a welcome message showing what department he/she is accessing, and a short warning regarding the use of resources in the organization.	Batch script added to group policy to notify user upon logging in so that their system is configured to the right image.
IT Users on those two departments will have access to network shares: one network share for all users in department A, one for department B, and another one accessible for both departments.	Network shares enabled from logic diagram, and on both Servers for proper allocation of servers.
Passwords for accounts need to be set in function of a security policy, i.e. not too short, not too long, they need to be changed after a reasonable time, and they cannot be reused immediately.	Password policy set in group policy. Sudoers password policy also set, warnings are turned on as well, allowing the user know the password policy.
This organization will have a software development team in the near future. They would like to have a small application that shows the benefits of using embedded user rights and access to resources at the application level (respond to this requirement in how you would go about doing this logically).	Application whitelisting will still be in play, decided by the local IT admin. Can develop through RDP or SSH on a secure server through VPN, so that local network is protected from outside malware/replay attacks.
The organization also needs a very simple (1 page) website that is public facing, but also needs departmental websites. They would like you to use apache for this.	Front facing website added using apache and can be viewed in network infrastructure document.
The Sales and Software department websites must be able to communicate to each other, but not be publicly.	Internal website can be viewed by both departments.
The Software development team has to have a development space on the internal network.)They use Linux servers as their platform for development so they must have their own space, but they expect the server to be secure.	Big Data team has access to Linux Servers only available through ssh (port 22).

Active Directory Design

- Group Policy Edits affecting the entire organization are to be made by the IT Department. Each OU has their respective Local IT Admin to further limit permissions. Any further technical policy is to be made by the Local IT Admin that may be required for their specific environment.
- Workstations, Groups, Users etc. encompassing a department are organized in the Domain as a department. This allows flexibility in deployment, permissions, and further policies to meet department needs.



Medical Staff User

Data collected on: 5/8/2020 3:12:10 PM

Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

Policies

Windows Settings

Scripts

Logon

For this GPO, Script order: Windows PowerShell s

Name	Parameters
C:\Users\DC1\Documents\MedicalStaffGP.bat	

Administrative Templates

Policy definitions (ADMX files) retrieved from the local co

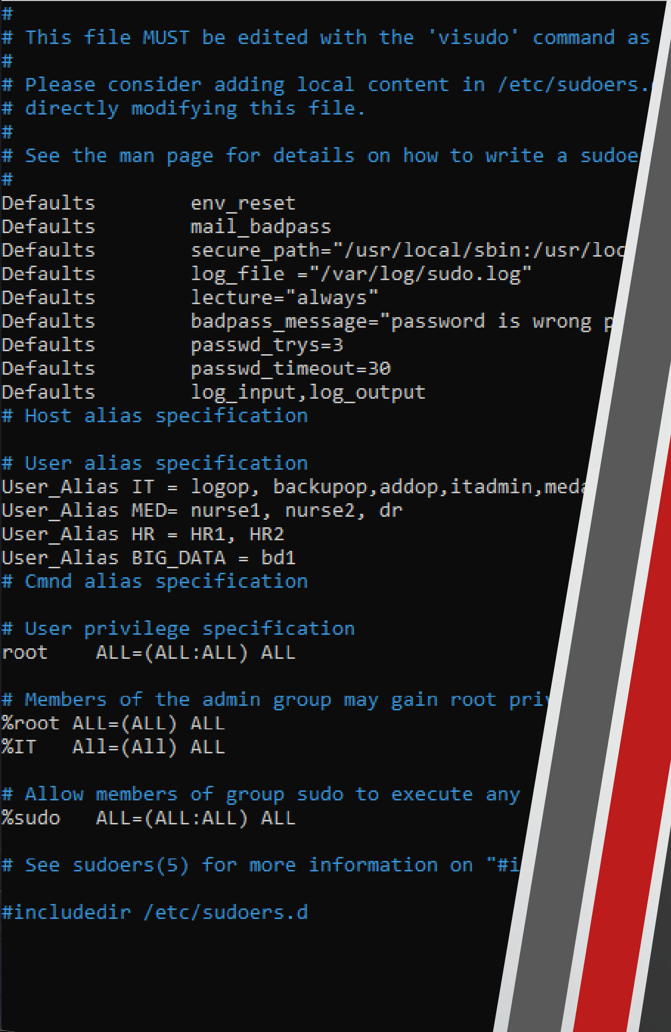
Control Panel/Add or Remove Programs

Technical Policies

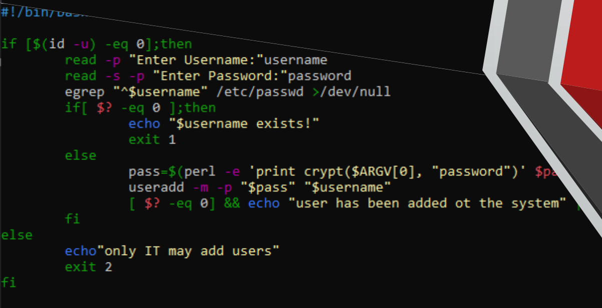
- Group Policy: Ensures System Image is correct for correct software
- Shared Drive Capabilities with correct permissions
- RDP Enabled from Big Data to Med Staff
- Ensures all security measures are taken into account and all permissions are set.
- Ensures users can only access their computer from 8AM-5PM
- Uses Windows screensaver after 15 minutes of inactivity
- Local IT Admin has ability to change their department policy
- Admins can add users by running makeusers.sh located in the network infrastructure document.

IT Policies

- Acceptable Use Policy – To establish a standard for rules and responsibilities when connecting to the COS Care network, or when using workplace network systems
- Audit Policy - To provide guidelines for employees to follow regarding network scanning policies
- Backup Policy - To protect hospital data and to ensure most data recovery is possible
- Captive Portal Policy – To establish a standard for all devices and their activity connecting to the COS Care guest network
- Database Password Policy - To inform employees about what makes strong password as well as general guidelines to protect any password
- Disaster Recovery Policy - To outline the Disaster Recovery Team and their responsibilities to the hospital
- DMZ Internet Policy - To define what equipment is considered in the DMZ zone as well as outline procedures to keep such equipment protected
- Ethics Policy - To set the expectations of what the hospital deems ethical in dealing with the internet, coworkers, and external media
- Internet Use Policy - To show employees how the hospital expects the internet provided to be used, as well as warnings of what not to do with the internet (both for network security and professional security)



```
#
# This file MUST be edited with the 'visudo' command as
#
# Please consider adding local content in /etc/sudoers.
# directly modifying this file.
#
# See the man page for details on how to write a sudoe
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/loc
Defaults        log_file ="/var/log/sudo.log"
Defaults        lecture="always"
Defaults        badpass_message="password is wrong p
Defaults        passwd_trys=3
Defaults        passwd_timeout=30
Defaults        log_input,log_output
# Host alias specification

# User alias specification
User_Alias IT = logop, backupop,addop,itadmin,meda
User_Alias MED= nurse1, nurse2, dr
User_Alias HR = HR1, HR2
User_Alias BIG_DATA = bd1
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root pri
%root ALL=(ALL) ALL
%IT   All=(All) ALL

# Allow members of group sudo to execute any
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#i

#includedir /etc/sudoers.d
```



```
#!/bin/ba

if [$(id -u) -eq 0];then
        read -p "Enter Username:"username
        read -s -p "Enter Password:"password
        egrep "^$username" /etc/passwd >/dev/null
        if[ $? -eq 0 ];then
                echo "$username exists!"
                exit 1
        else
                pass=$(perl -e 'print crypt($ARGV[0], "password")' $pa
                useradd -m -p "$pass" "$username"
                [ $? -eq 0] && echo "user has been added ot the system"
        fi
else
        echo"only IT may add users"
        exit 2
fi
```

Group Policies

- All IT personnel have sudo access.
- Added Groups for all departments
  - Human Resources (HR)
  - Information Technology (IT)
  - Big Data (BD)
  - Medical (MED)

- Big Data has RDP access for grabbing only medical statistics from the shared drive
- All new members to be placed in the admin group to where the local admin then places them in their respective department with respective permissions.
- All file information logged with exception to PHI, all users aware of their system with welcome message upon login.

Future Growth

- Reliability – Having a network that will not go down
- Scalability – Being able to expand COS Care's system
- Cost – Securing a cost-effective system for the hospital
- Manageability – Adapt the system to the hospital's need
- Updating system security, Physically and Virtually
- Expanding Departments of the Hospital
  - Adding Additional Departments
  - Implementing RBAC
  - Keeping the website up to date

Project Challenges

- Can create countless amount of IT Policies, difficult to figure out which is most important in qa start of a company.
- Azure trial ended, had to resort to other resources such as AWS.
- Figuring out the correct defaults to use in the sudoers file, ensuring the group file was set up correctly. Overall, the groups file sets the baseline, there is not too much to add however sets the organizational infrastructure for the business.
- In the future, it will be difficult to setup firewalls at every department without bringing the network down.
- It will also be difficult in the future to make more and more preventative measures towards the ever evolving use of malware.