DinoSquad LLC

Table of Contents

Policies

Audit Policy

1.0 Purpose The purpose of this agreement is to set forth our agreement regarding network security scanning offered at DinoSquad. The IT department will be responsible for performing all electronic scans of networks, firewalls, and systems utilizing the DinoSquad software. Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to DinoSquad security policies
- Monitor user or system activity where appropriate.

2.0 Scope This policy covers all computer and communication devices owned or operated by DinoSquad. This policy also covers any computer and communications device that are present on DinoSquad premises, but which may not be owned or operated by DinoSquad including personal phones and tablets. The IT department will not perform Denial of Service activities.

3.0 Policy By accepting the offer for employment at DinoSquad, all employees consent to access by members of the IT department. This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on DinoSquad equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on DinoSquad networks.

3.1 Service Degradation and/or Interruption Network performance and/or availability may be affected by the network scanning. DinoSquad releases any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result DinoSquad's gross negligence or intentional misconduct.

3.2 Scanning period DinoSquad and the IT department's Scanning Team shall identify in writing the allowable dates for the scan to take place.

3.3 Enforcement Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Backup Policy

1.0 Overview This policy defines the backup policy for computers within DinoSquad which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server. This policy may contain descriptions about how various systems and types of systems are backed up such as Windows or UNIX systems.

2.0 Purpose This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

3.0 Scope This policy applies to all equipment and data owned and operated by DinoSquad.

4.0 Definitions

1. Backup - The saving of files onto offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
2. Archive - The saving of old or unused files onto offline mass storage media for the purpose of releasing online storage room.
3. Restore - The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

5.0 Timing Full backups are performed weekly on Friday nights. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

6.0 Responsibility The IT department manager shall delegate a member of the IT department to develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis. A delegated person will also perform the regular backups.

7.0 Testing The ability to restore data from backups shall be tested at least once per month.

8.0 Data Backed Up

Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. Test database server
7. Test web server

9.0 Archives Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

10.0 Restoration Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

11.0 Dedicated Offline Mass Storage Media Location The offline mass storage media location used for weekly backups shall be stored in an offsite building in an undisclosed location.

DB Password and Password Policy

1.0 Overview Passwords are a main aspect of computer security and if you make stupid, non-secure passwords, you will immediately be fired and fed to the dinosaurs or not hired at DinoSquad in the first place.

2.0 Purpose The purpose of this policy is to estable requirements for the creation of secure passwords, protection of the passwords, and the changing of those passwords.

3.0 Scope This policy applies to all personnel who have an account and who are responsible for that account or any form of access that requires a password on any system that resides at any DinoSquad facility, has access to the DinoSquad network, or stores any private DinoSquad information.

4.0 Policy

4.1 General

- All system-level passwords must be changed on a quarterly basis
- All production system-level passwords must be included in the DinoSquad global password management database
- All user-level passwords must be changed every four months
- User accounts that have system-level privileges granted through groups such as “sudo” must have a unique password from all other accounts held by that user
- Passwords must not be transmitted through email messages or any other form of electronic communication
- All user-level and system-level passwords must conform to the guidelines described below

4.2 Specific Requirements

4.2.1. Storage of DataBase Usernames and Passwords

- Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may not reside in the documents tree of a web server.

- Pass through authentication must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or passphrases used to access a database must adhere to the Password Policy.

4.2.2. Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

4.2.3 Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the Password Policy.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

4.3 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at DinoSquad thus everyone should be aware of how to select strong passwords.

4.4 Guidelines

A. General Password Construction Guidelines

Poor, weak passwords have the following characteristics (and should not be done) :

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "DinoSquad", "ducks", "dinosaur" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Minimum of 12 characters long and is a passphrase (!IAmAMighty_Duck1542)
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~=\`{}[]:";'<>?,./)
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for DinoSquad accounts as for other non-DinoSquad access. Where possible, don't use the same password for various DinoSquad access needs. For example,

select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share DinoSquad passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential DinoSquad information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE through voice or text
- Don't reveal a password in an email message
- Don't reveal a password to the supervisor
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "DuckyDuck")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while

If someone demands a password, refer them to this document or have them call someone in the IT Department.
Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).
Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system without encryption.
Your password will expire every four months (except system-level passwords which must be changed quarterly) and you will be prompted to change it.
If an account or password is suspected to have been compromised, report the incident to the IT department and change all passwords.
If you forgot your password and get locked out, contact IT and they will open the account for you and require that you change to a new password that still adheres to this password policy.
Password cracking or guessing may be performed on a periodic or random basis by the IT department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it and be put on dinosaur cleanup crew for the rest of the day.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the DinoSquad Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and possible feeding to the dinosaurs.

Disaster Recovery Policy

A disaster recovery team shall be appointed with members from IT, and the executive staff and will be reviewed annually for relevance. The disaster recovery team will perform the following duties:

- Perform an initial risk assessment to determine current information systems vulnerabilities.
- Perform an initial business impact analysis to document and understand the interdependencies among business processes and determine how the business would be affected by an information systems outage.
- Take an inventory of information systems assets such as computer hardware, software, applications, and data.
- Identify critical applications, systems, and data.
- Prioritize key business functions.
- Conduct simulated disasters to test effectiveness of policies and capabilities of the disaster recovery team.

Company personnel will carry out the following procedures in the implementation of a disaster recovery policy:

- Document and distribute the recovery plan.
- Distribute copies of the written plans to everyone involved and also store extra copies in an offsite, fireproof vault.

The following are ongoing procedures that must be followed:

- Continuously perform data backups, store at least weekly backup's offsite, and test those backups regularly for data integrity and reliability.
- Test plans at least annually, document and review the results, and update the plans as needed.
- Analyze plans on an ongoing basis to ensure alignment with current business objectives and requirements.
- Provide security awareness and disaster recovery education for all team members involved.
- Continuously update information security policies and network diagrams.

- Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.

(All employees must sign the policy below)

Acknowledging Receipt of Disaster Recovery Policy

I have received my copy of the TEKS Disaster Recovery Policy and I have read and understand the information contained herein.

I further acknowledge my understanding that my employment with TEKS may be terminated at any time with or without cause.

_____

Date

_____

Employee's Signature

_____

Name [Please Print]

DinoSquad Ethics Policy

1. Overview DinoSquad purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every DinoSquad employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.
DinoSquad is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When DinoSquad addresses issues proactively and uses correct judgment, it will help set us apart from competitors. DinoSquad will not tolerate any wrongdoing or impropriety at anytime. DinoSquad will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2. Purpose Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

3. Scope This policy applies to employees, contractors, consultants, temporaries, and other workers at DinoSquad, including all personnel affiliated with third parties.

4. Policy

4.1. Executive Commitment to Ethics

4.1.1. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the workforce.

4.1.2. Executives at DinoSquad will operate above reproach as all times in all business practices and relationship in which they are acting as agents of DinoSquad.

4.1.3 Executive must disclose any conflict of interests regarding their position within DinoSquad.

4.2. Employee Commitment to Ethics

4.2.1. DinoSquad employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

4.2.2. Every employee needs to apply effort and intelligence in maintaining ethics value.

4.2.3. Employees must disclose any conflict of interests regard their position within DinoSquad.

4.3. Company Awareness

4.3.1. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

4.3.2. DinoSquad will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. Maintaining Ethical Practices

4.4.1. DinoSquad will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

4.4.2. Employees at DinoSquad should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.4.3. DinoSquad has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.5. Unethical Behavior

4.5.1. DinoSquad will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.5.2. DinoSquad will not tolerate harassment or discrimination.

4.5.3. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

4.5.4. DinoSquad employees will not use corporate assets or business relationships for personal use or gain.

4.5.5 DinoSquad employees will not share on any social media site, verbally, or in writing any proprietary information, concepts, designs, or secrets that are protected by company policy.

5. Enforcement Any infractions of this code of ethics will not be tolerated and DinoSquad will act quickly in correcting the issue if the ethical code is broken.
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or feeding to the dinosaurs.

Acceptable Internet Use Policy

These guidelines are intended to help you make the best use of the Internet resources at your disposal. You should understand the following:

- DinoSquad provides Internet access to staff to assist them in carrying out their duties for the Company. It should not be used for personal reasons such as online shopping, checking social media, or watching inappropriate content.
- You may only access the Internet by using DinoSquad's content scanning software, firewall and router.
- You may only access the Internet after you have been authorized to do so by your department manager.

When using DinoSquad Internet access facilities you should comply with the following guidelines.

<u>DO</u>

1. Do keep your use of the Internet to a minimum
2. Do check that any information you access on the Internet is accurate, complete and current.
3. Do check the validity of the information found.
4. Do respect the legal protections to data and software provided by copyright and licenses.
5. Do inform the I.T. Department immediately of any unusual occurrence.

<u>DO NOT</u>

1. Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
2. Do not download content from Internet sites unless it is work related.

3. Do not download software from the Internet and install it upon DinoSquad's computer equipment.
4. Do not use DinoSquad computers to make unauthorised entry into any other computer or network.
5. Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990.
6. Do not represent yourself as another person.
7. Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

Please note the following:

- All activity on the Internet is monitored and logged.
- All material viewed is scanned for viruses.
- All the content viewed is scanned for offensive material.
- If you are in any doubt about an issue affecting Internet Access you should consult the I.T. Department.
- Any breach of DinoSquad Acceptable Internet Use Policy may lead to disciplinary action such as termination or being fed to the dinosaurs.

Remote Access Policy

1.0 Purpose The purpose of this policy is to define standards for connecting to DinoSquad's network from any host. These standards are designed to minimize the potential exposure to DinoSquad from damages which may result from unauthorized use of DinoSquad resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical DinoSquad internal systems, etc.

2.0 Scope This policy applies to all DinoSquad employees, contractors, vendors and agents with a DinoSquad-owned or personally-owned computer or workstation used to connect to the DinoSquad network. This policy applies to remote access connections used to do work on behalf of DinoSquad, including reading or sending email and viewing intranet web resources.

3.0 Policy

3.1 General

1. It is the responsibility of DinoSquad employees, contractors, vendors and agents with remote access privileges to DinoSquad's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DinoSquad.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong passphrase see the Password Policy.
2. At no time should any DinoSquad employee provide their login or email password to anyone, not even family members.
3. DinoSquad employees and contractors with remote access privileges must ensure that their DinoSquad-owned or personal computer or workstation, which is remotely connected to DinoSquad's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. DinoSquad employees with remote access privileges to DinoSquad's corporate network must not use non-DinoSquad email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct DinoSquad business, thereby ensuring that official business is never confused with personal business.
5. All hosts that are connected to DinoSquad internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
6. Personal equipment that is used to connect to DinoSquad's networks must meet the requirements of DinoSquad-owned equipment for remote access.

4.0 Enforcement Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or feeding to the dinosaurs.

Router Security Policy

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of DinoSquad.

2.0 Scope

All routers and switches connected to DinoSquad production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the Internet DMZ Equipment Policy.

3.0 Policy Every router must meet the following configuration standards:

1. No local user accounts are configured on the router.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.

4.0 Enforcement Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or feeding to the dinosaurs.

Internet DMZ Equipment Policy

1.0 Purpose The purpose of this policy is to define standards to be met by all equipment owned and/or operated by DinoSquad located outside DinoSquad's corporate Internet firewalls. These standards are designed to minimize the potential exposure to DinoSquad from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of DinoSquad resources.

Devices that are Internet facing and outside the DinoSquad firewall are considered part of the "demilitarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the corporate firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

2.0 Scope All equipment or devices deployed in a DMZ owned and/or operated by DinoSquad (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by DinoSquad, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "DinoSquad.com" domain or appears to be owned by DinoSquad.

All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents. All existing and future equipment deployed on DinoSquad's un-trusted networks must comply with this policy.

3.0 Policy

3.1. Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by the IT department for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.
- Password groups must be maintained in accordance with the corporate wide password management system/process.

- Immediate access to equipment and system logs must be granted to members of IT upon demand.
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

3.2. General Configuration Policy All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by IT as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards
- Services and applications not serving business requirements must be disabled.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by the IT department) must be replaced with more secure equivalents whenever such exist.
- All host content updates must occur over secure channels.
- Security-related events must be logged and saved to IT-approved logs. Security related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.

3.3. Equipment Outsourced to External Service Providers The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

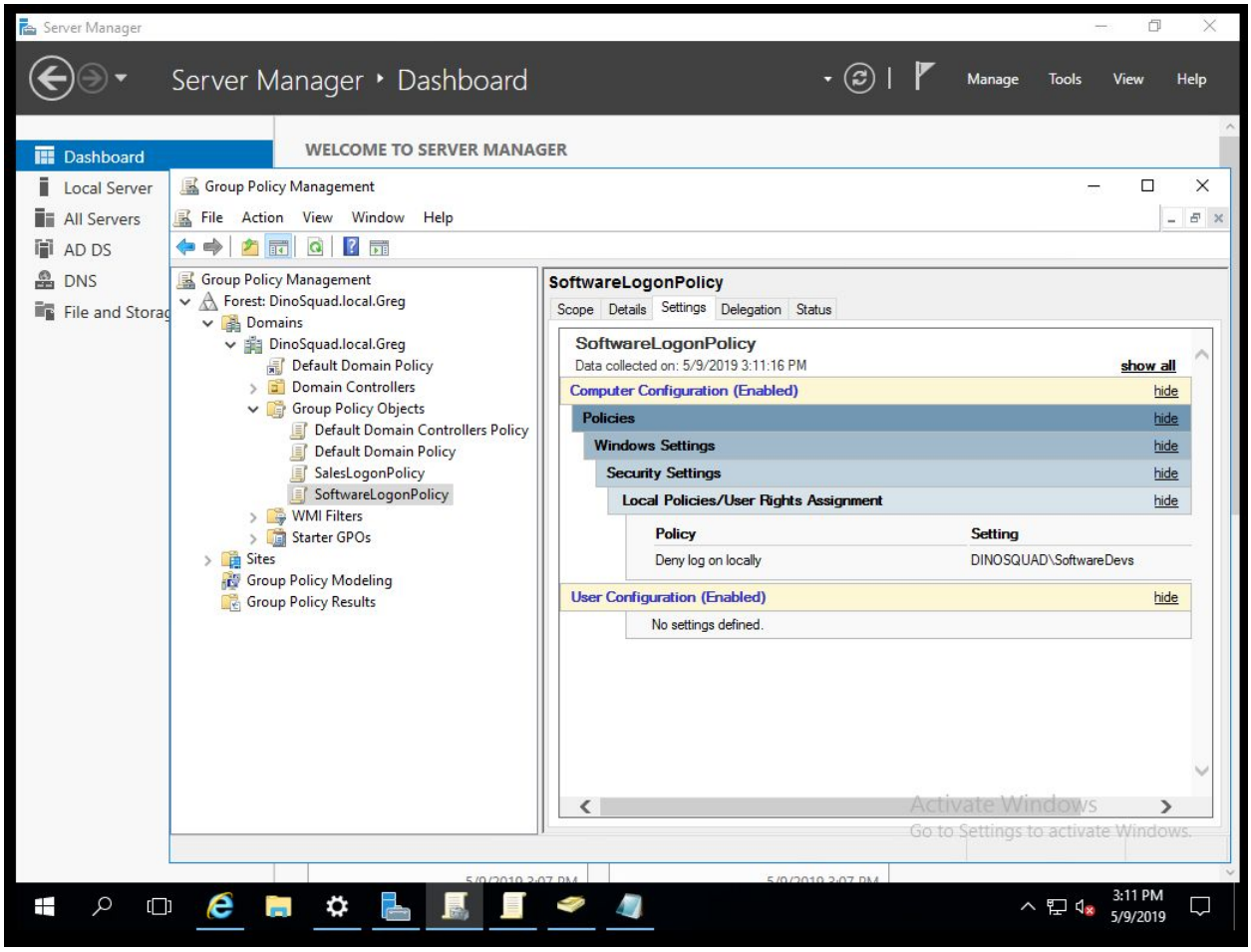
4.0 Enforcement Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or feeding to the dinosaurs.

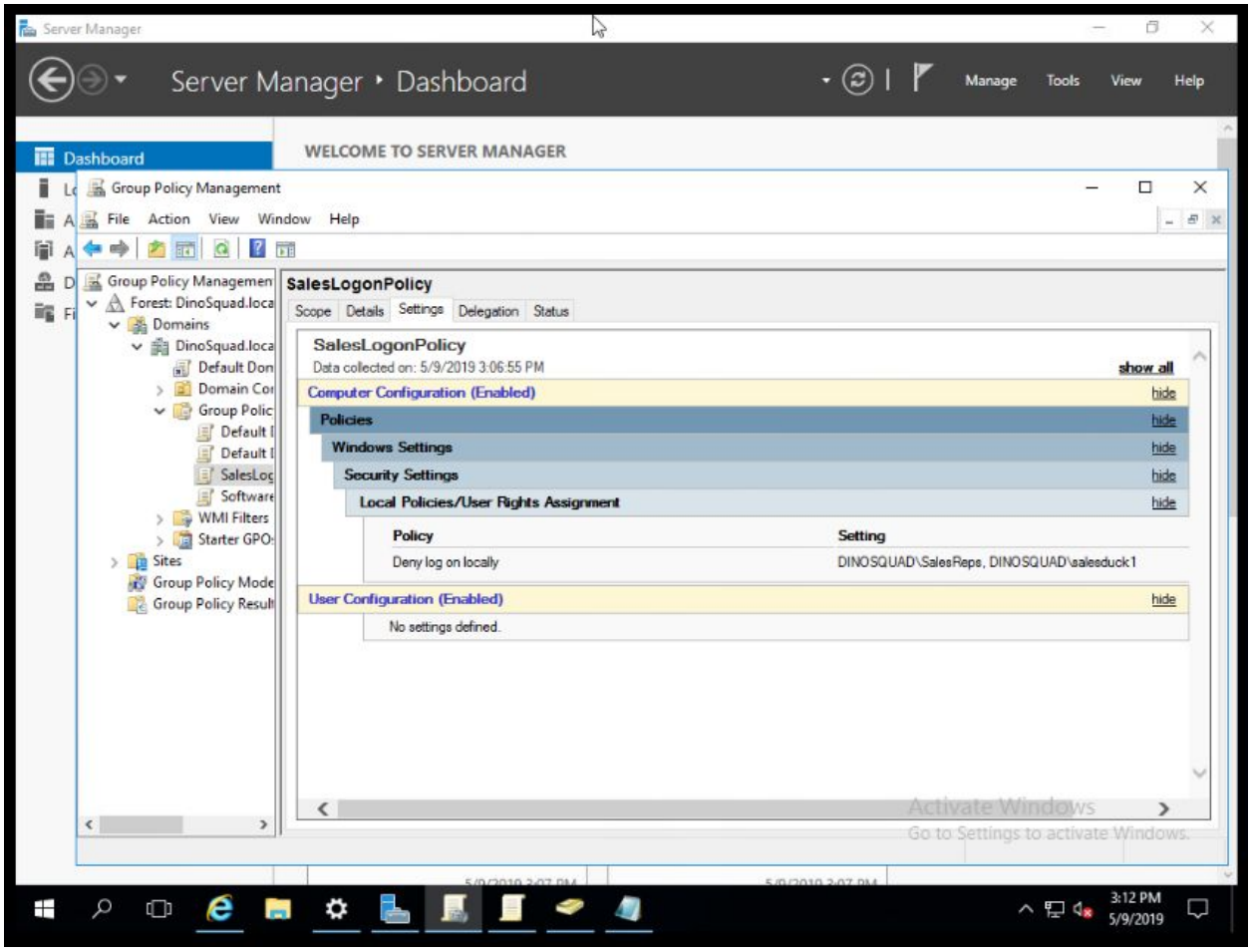
External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

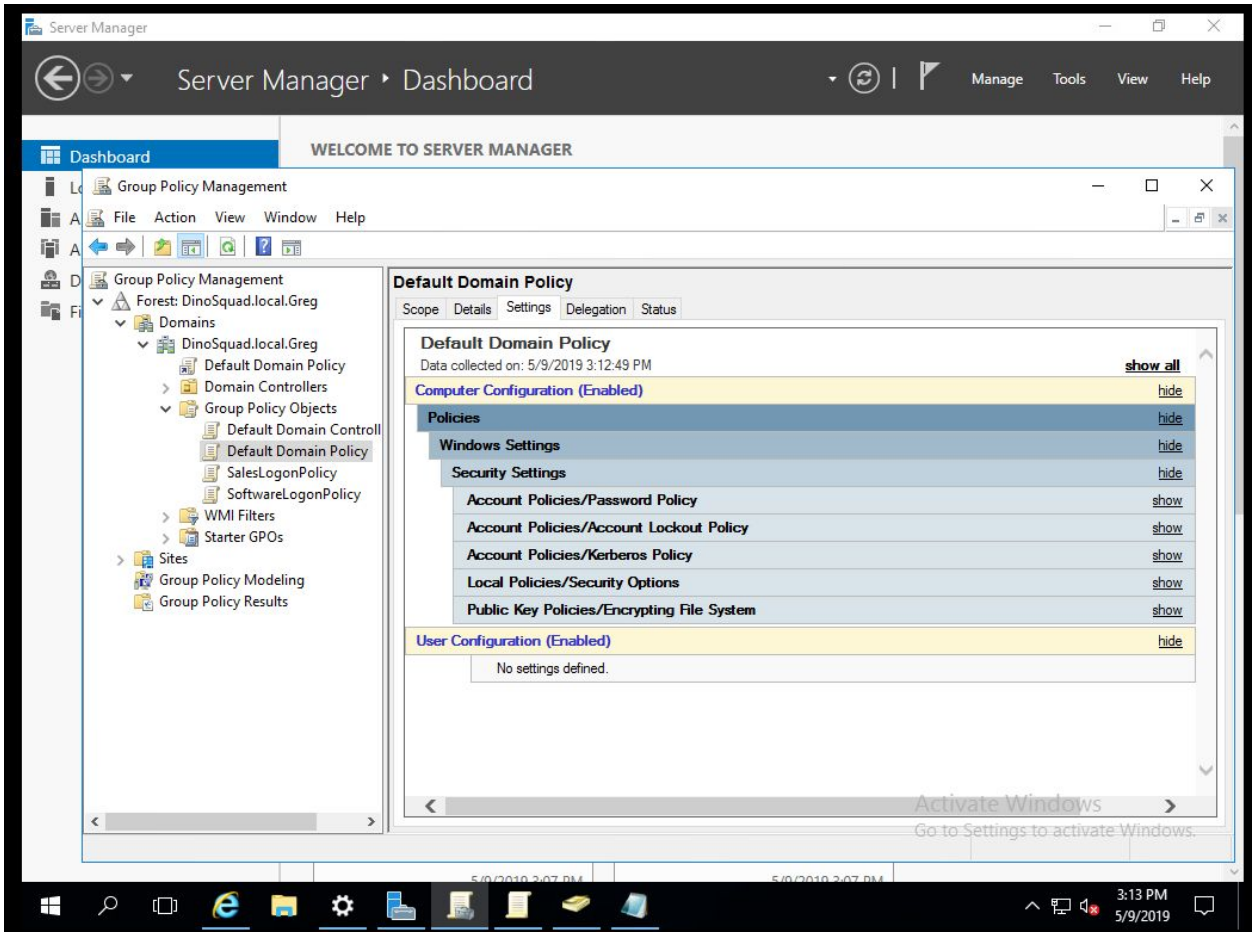
Technical Policies, Programs & Scripts

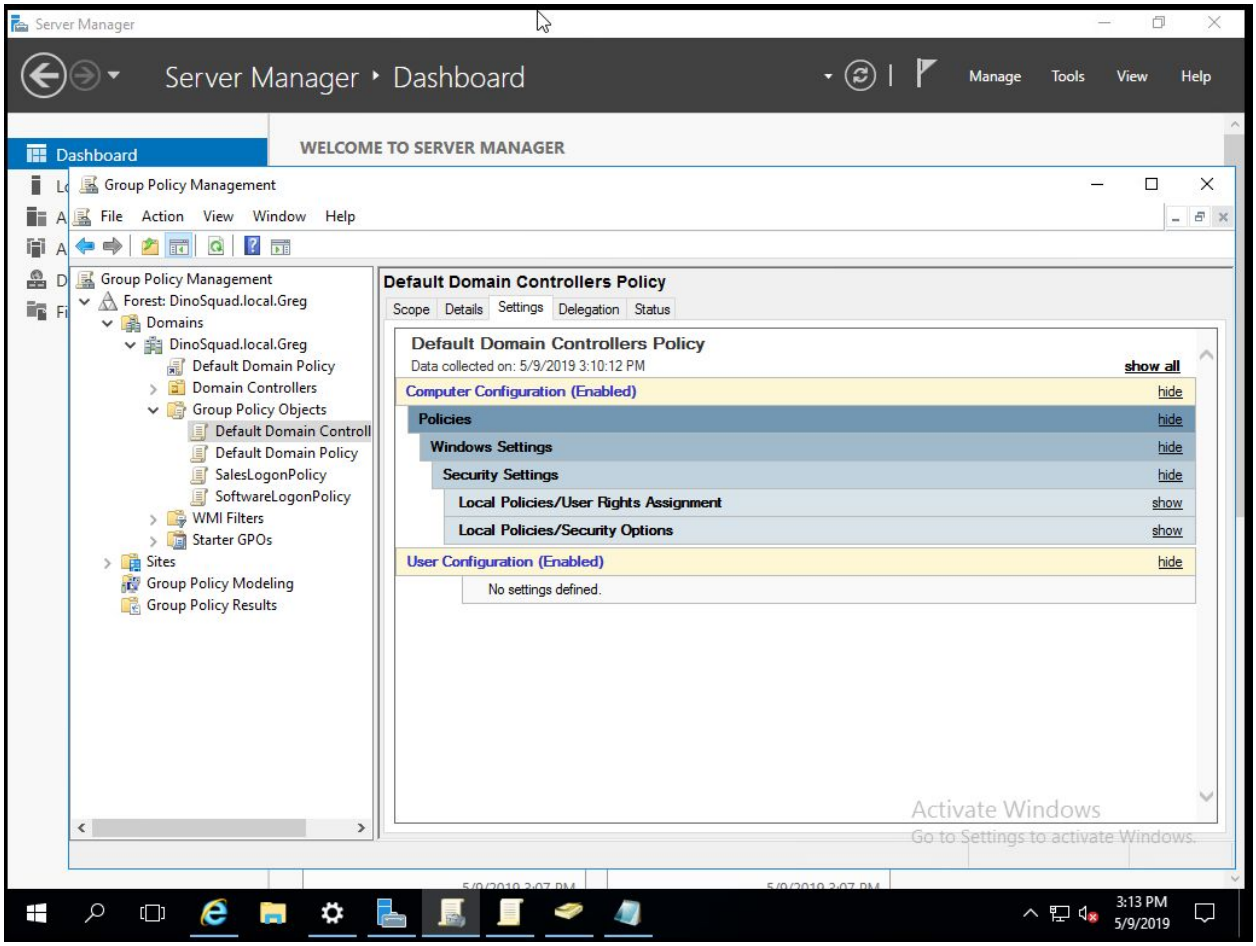
Windows

GPO/Technical Policies

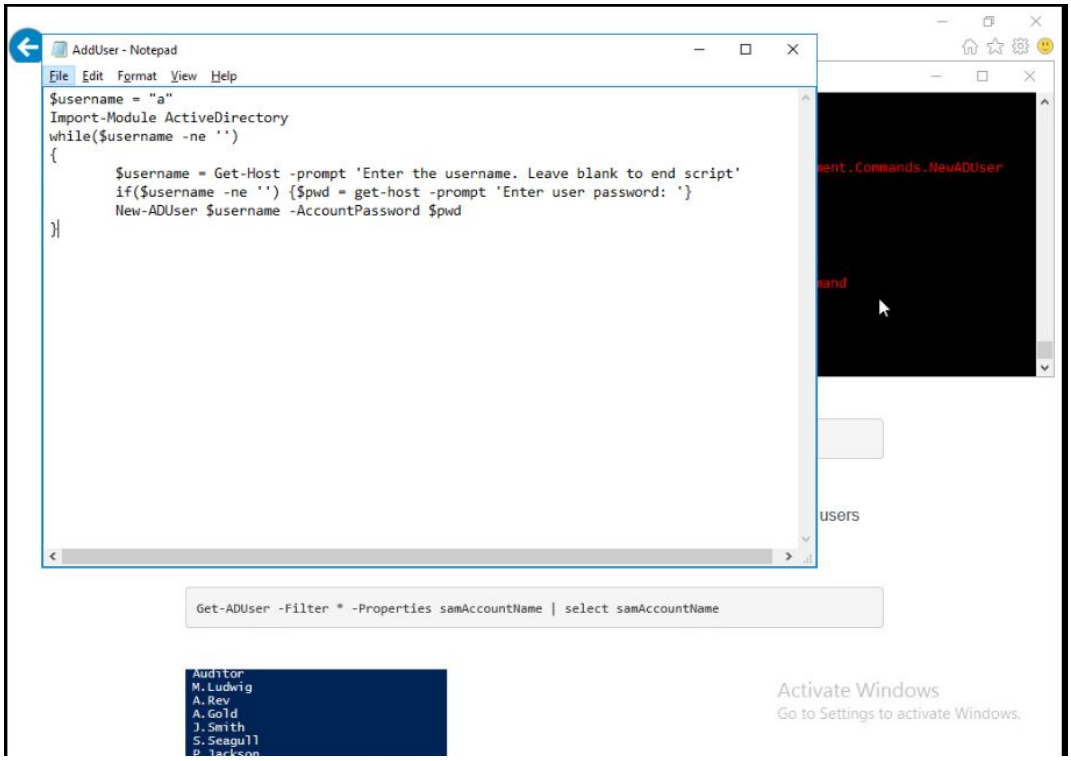



Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
WELCOME TO SERVER MANAGER
Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: DinoSquad.local
Domains
DinoSquad.local
Default Domain
Domain Controllers
Group Policy
Default
Default
SalesLogonPolicy
Software
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
SalesLogonPolicy
Scope
Details
Settings
Delegation
Status
SalesLogonPolicy
Data collected on: 5/9/2019 3:06:55 PM
show all
Computer Configuration (Enabled)
hide
Policies
hide
Windows Settings
hide
Security Settings
hide
Local Policies/User Rights Assignment
hide
Policy
Setting
Deny log on locally
DINOSQUAD\SalesReps, DINOSQUAD\salesduck1
User Configuration (Enabled)
hide
No settings defined.
Activate Windows
Go to Settings to activate Windows.
3:12 PM
5/9/2019


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
WELCOME TO SERVER MANAGER
Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: DinoSquad.local.Greg
Domains
DinoSquad.local.Greg
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controll
Default Domain Policy
SalesLogonPolicy
SoftwareLogonPolicy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Policy
Scope
Details
Settings
Delegation
Status
Default Domain Policy
Data collected on: 5/9/2019 3:12:49 PM
show all
Computer Configuration (Enabled)
hide
Policies
hide
Windows Settings
hide
Security Settings
hide
Account Policies/Password Policy
show
Account Policies/Account Lockout Policy
show
Account Policies/Kerberos Policy
show
Local Policies/Security Options
show
Public Key Policies/Encrypting File System
show
User Configuration (Enabled)
hide
No settings defined.
Activate Windows
Go to Settings to activate Windows.
3:13 PM
5/9/2019

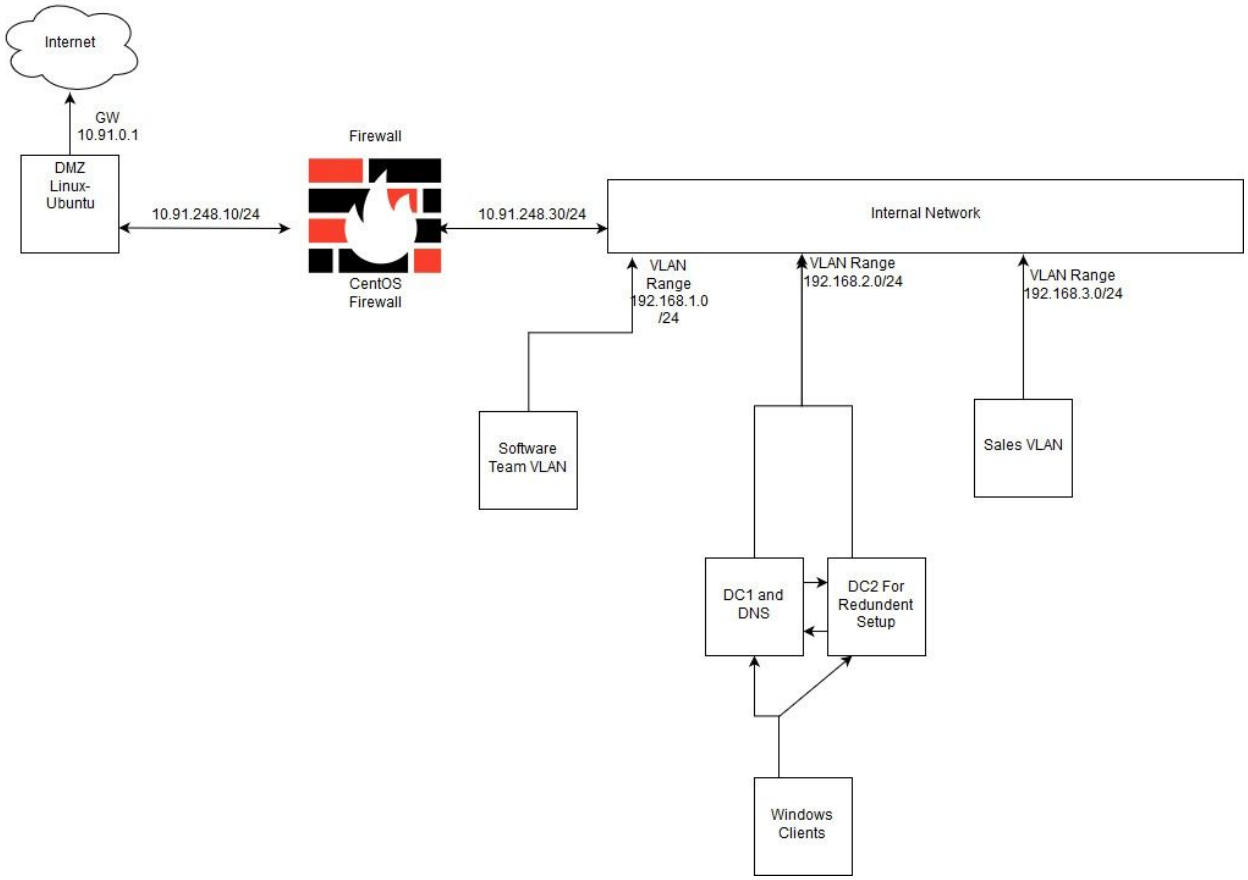


The policies shown above outline that there is user limitations and restrictions within their department. (Tabs must be expanded to show more specifics but were not expanded to save screenshot space)



Programs and Scripts that add users to the domain

Diagram



User Accounts

Servers

- Software Team Server - The software department's server which hosts the software team's website and provides the software department with a serve to develop software on. The server is set-up as a cluster node meaning that the server is set up in such a way that you can add more machines to the cluster to improve cluster computational power.
- Sales Team Server - The sales team department's server which hosts internal website for the sales department.

Network Security

- Internal Firewall - The firewall server which defends our internal network.

- DMZ server - The Demilitarized Zone Server which handles the brute force connections to our network.

Domain Controllers

- DC1 - A domain controller for the network used for authentication with our domain Dinosquad.local.greg.
- DC2 - A backup domain controller in case DC1 fails.

Windows Clients

- Software Machine1 - A general purpose linux workstation in the software department.
- Sales Machine1 - A general purpose windows workstation in the sales department. This is configured with Active Directory so that you can login through the domain into the sales department.

System Administrator

- Responsibilities
    - Running and maintaining the IT department
    - Install all applications for the department and ensure all system patches within the department are installed promptly to maintain network system security
    - Add departments to DinoSquad's network including adding a local administrator account for each department
- Has local access to all workstations in the IT department as well as remote access to DC1 and DC2.

Backup User

- Responsibilities
    - Performs a backup of the server every Friday to a secure external server in an offsite facility.
- Has local access to the IT department

Log Monitoring User

- Responsibilities
    - Monitors all system logs for the company
- Has local access to the IT department

Workstation User

- Responsibilities
    - Joins all of the workstations for each department in the network system.
- Has a local account for each of the departments for auditing purposes.

Local Administrators

- Responsibilities
    - Adding each of the local users
    - Installing department applications
    - Update the system and install any patches for their department
- Created by the System Administrator
- Each department has its own local administrator
- Do not have access to the administrator account on the network

Local Users

- Responsibilities
    - General DinoSquad work
- General employees within the company
- The Software and Sales departments have their own set of local users
- Only allowed to access the workstations during scheduled company hours
- They are not allowed to install or uninstall any applications

Special Users

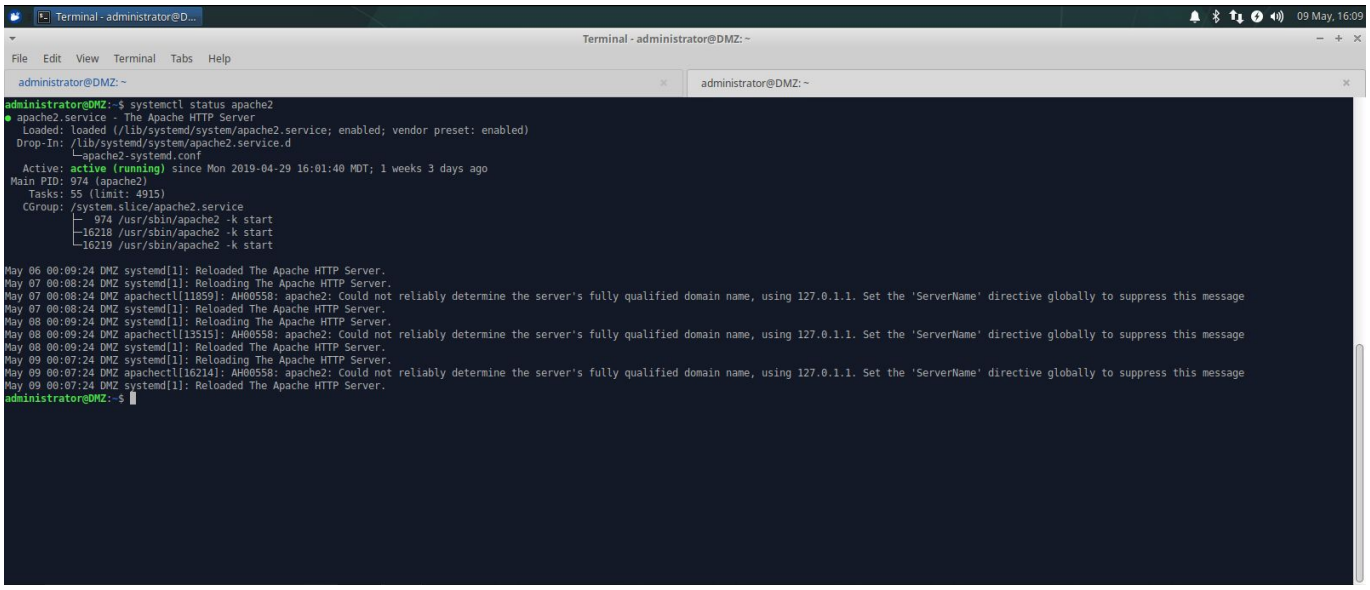
- Similar to the local users but they will have remote access to workstations
- The Software and Sales departments have their own assigned special user

Linux Server Documentation

- Linux server documentation - Including firewall rules, screenshots of websites, syslog of allow/deny requests for websites, sudoers file, /etc/group, /etc/passwd

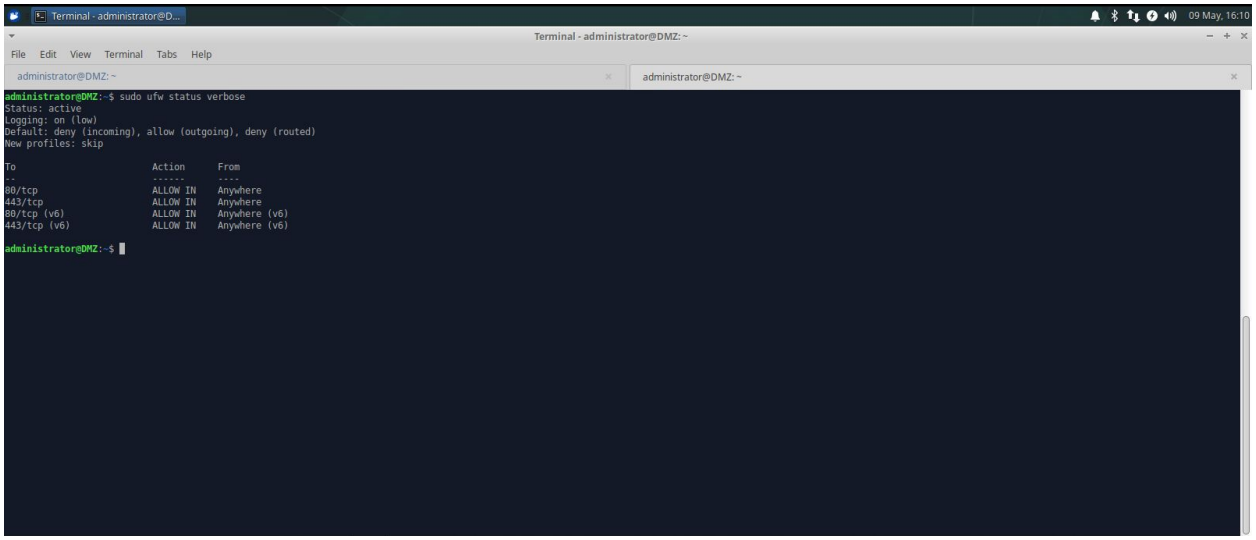
DMZ Server

Services



This server is running the apache2 service which runs web servers. We are not running ssh because we do not feel it is best practice to do so for the DMZ.

Open Ports



THis system has port 80 open for http and port 443 for secure connections.

Sudoers File

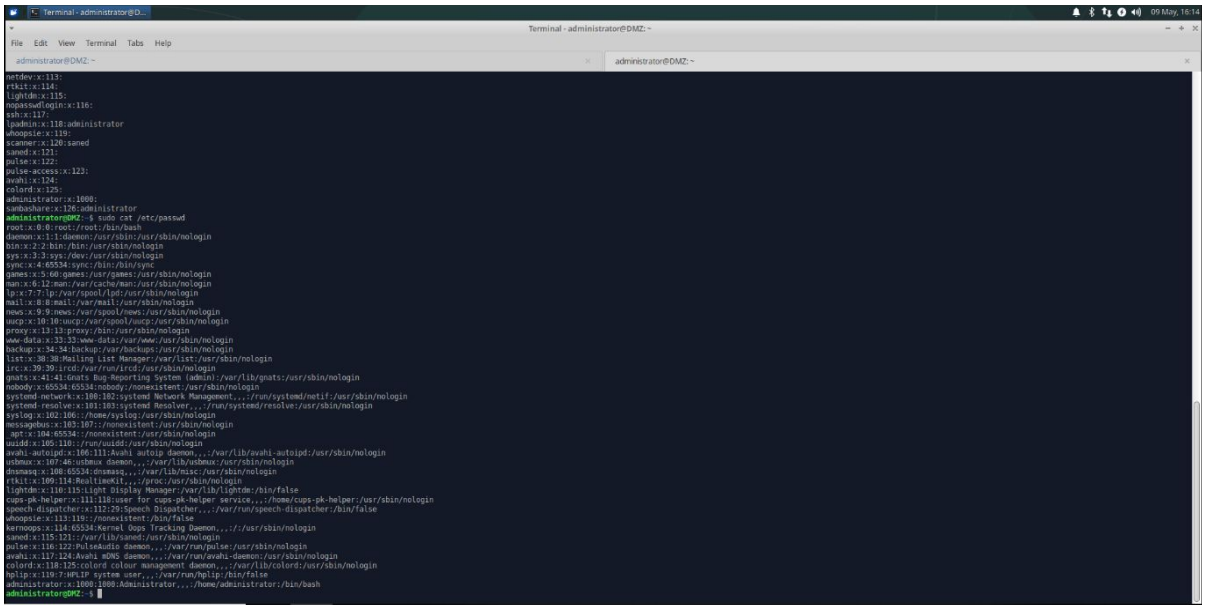
```
Terminal - administrator@DMZ: ~
File  Edit  View  Terminal  Tabs  Help
administrator@DMZ: ~        administrator@DMZ: ~

--                         ------     ----
80/tcp                     ALLOW IN   Anywhere
443/tcp                    ALLOW IN   Anywhere
80/tcp (v6)                ALLOW IN   Anywhere (v6)
443/tcp (v6)               ALLOW IN   Anywhere (v6)

administrator@DMZ:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

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

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

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

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
administrator@DMZ:~$
```

Users

/etc/group

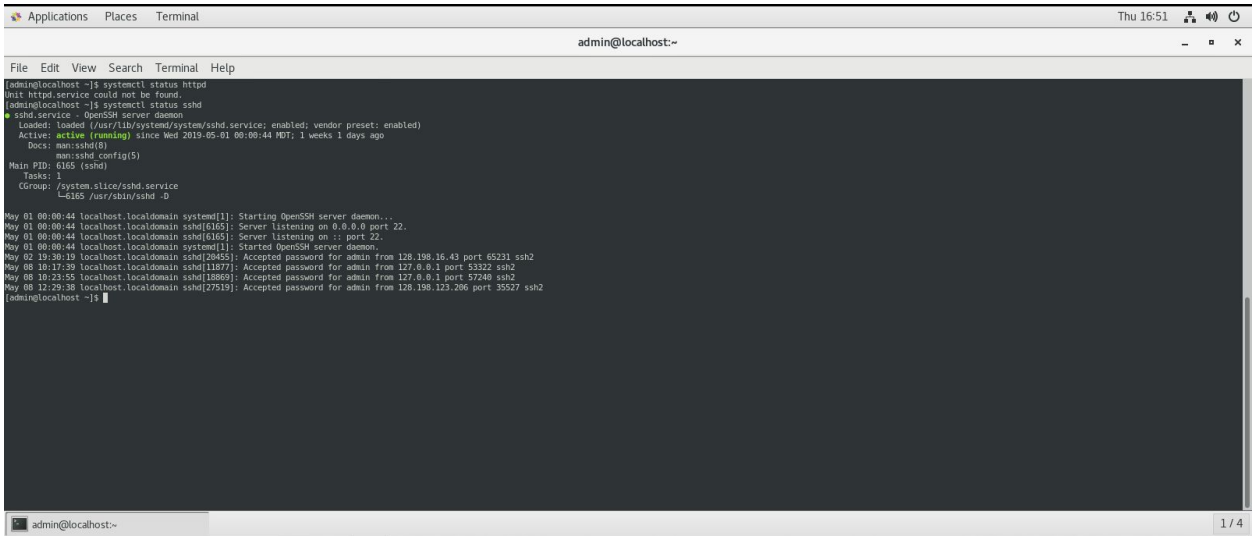
```
Terminal - administrator@DMZ: ~
File  Edit  View  Terminal  Tabs  Help
administrator@DMZ: ~        administrator@DMZ: ~

administrator@DMZ:~$ sudo cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,administrator
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:administrator
floppy:x:25:
tape:x:26:
sudo:x:27:administrator
audio:x:29:pulse
dip:x:30:administrator
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:administrator
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
input:x:104:
crontab:x:105:
syslog:x:106:
messagebus:x:107:
mlocate:x:108:
ssl-cert:x:109:
uuidd:x:110:
avahi-autoipd:x:111:
bluetooth:x:112:
netdev:x:113:
rtkit:x:114:
lightdm:x:115:
nopasswdlogin:x:116:
```

/etc/passwd



Firewall Server

Services

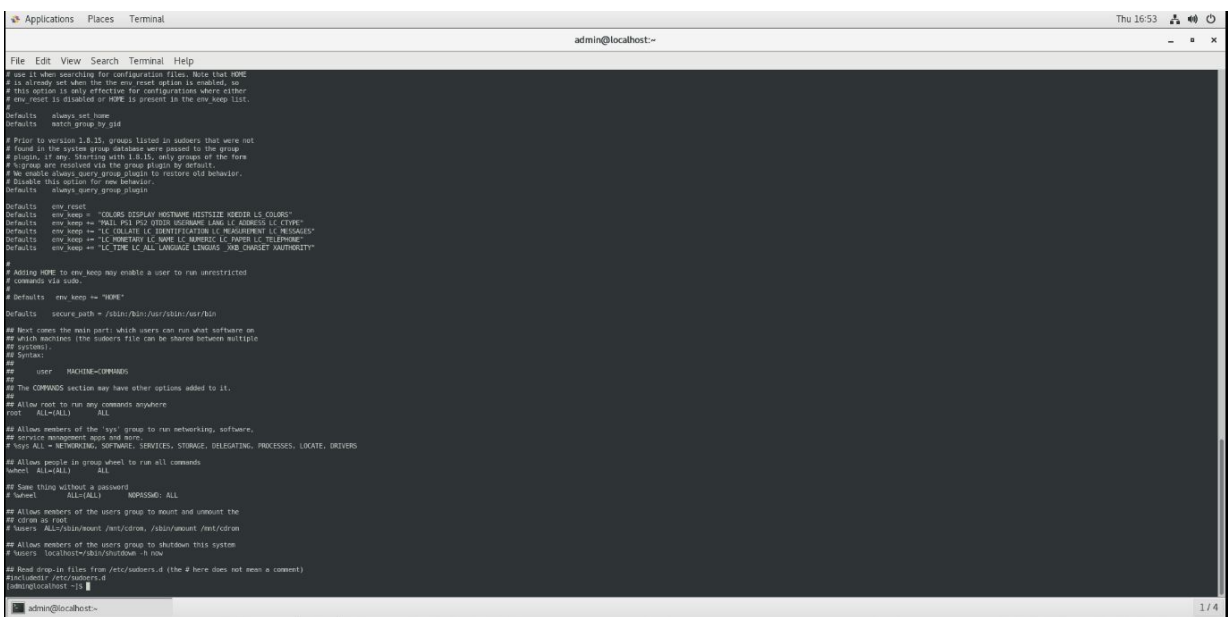


This system is running ssh.

Open Ports

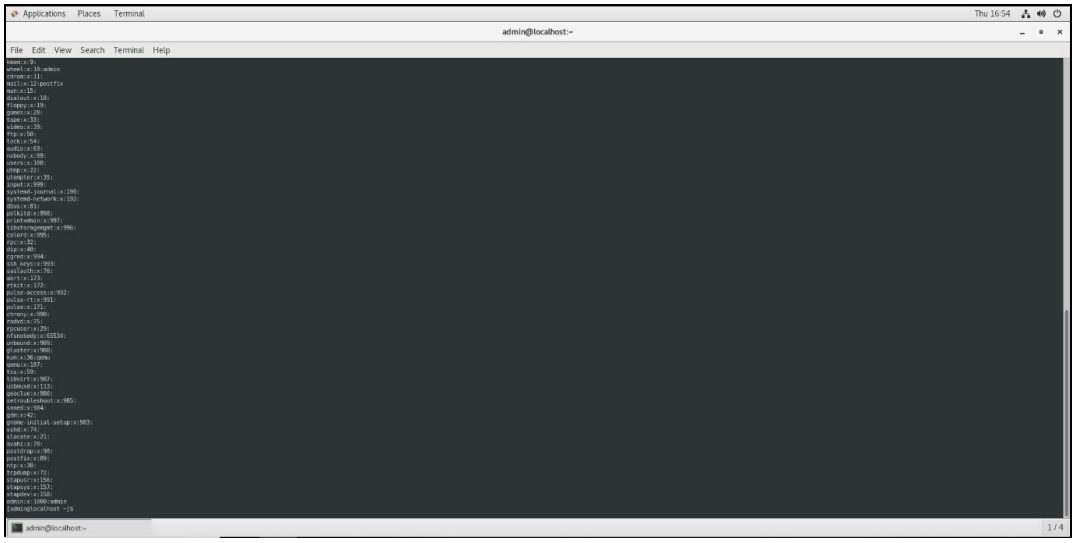
This server has ports 3390 and 3389 open for windows remote desktop. Here we also have the ssh client, samba client, and dhcpv6 client. SSH allows users to connect to this server, samba allows for integration with the windows based systems on the network by allowing you to share files and printers with those windows based systems. We also have a dhcp server on here to assign ip addresses, default gateways, as well as other network specifications to client devices.

Sudoers File

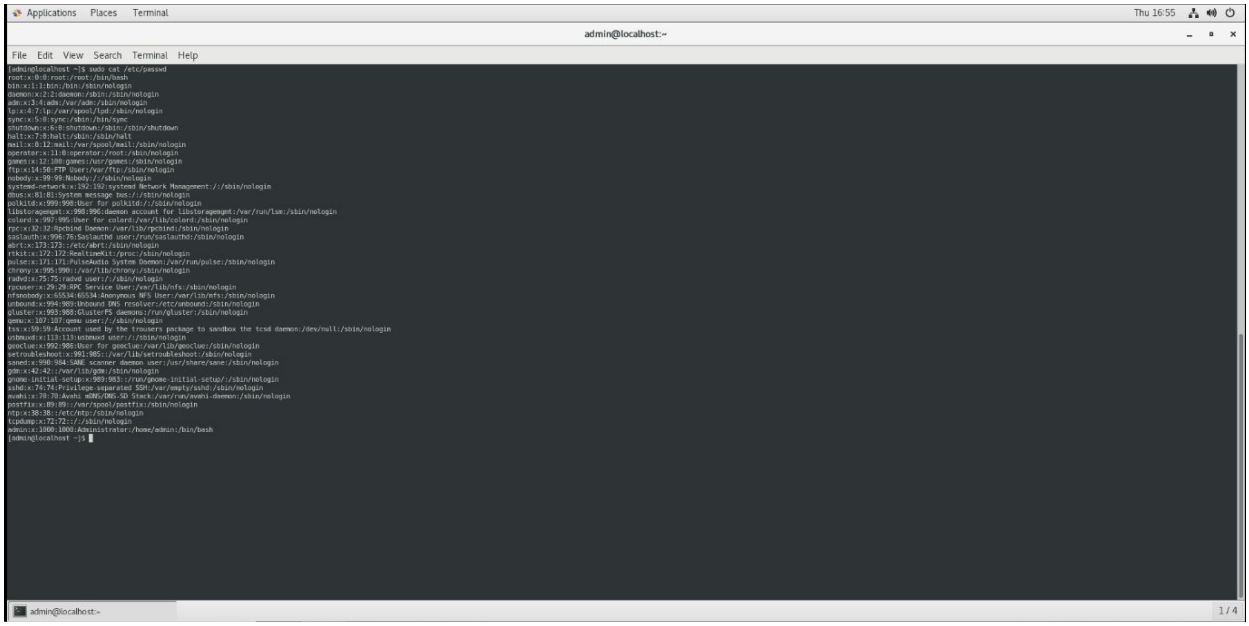


Users

/etc/group



/etc/passwd



Software Team Server

Services

```
Password:
Last login: Wed May  8 10:15:33 from gateway
----------------------------------------------
| Warning you have entered a restricted Zone! |
| All your actions are being monitored        |
----------------------------------------------


[admin@localhost ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-05-07 15:01:44 MDT; 2 days ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 6063 (httpd)
   Status: "Total requests: 4; Current requests/sec: 0; Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─6063 /usr/sbin/httpd -DFOREGROUND
           ├─6239 /usr/sbin/httpd -DFOREGROUND
           ├─6240 /usr/sbin/httpd -DFOREGROUND
           ├─6241 /usr/sbin/httpd -DFOREGROUND
           ├─6243 /usr/sbin/httpd -DFOREGROUND
           ├─6244 /usr/sbin/httpd -DFOREGROUND
           ├─10520 /usr/sbin/httpd -DFOREGROUND
           ├─10521 /usr/sbin/httpd -DFOREGROUND
           └─10522 /usr/sbin/httpd -DFOREGROUND

May 07 15:01:43 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
May 07 15:01:44 localhost.localdomain httpd[6063]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using local... message
May 07 15:01:44 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[admin@localhost ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2019-05-07 15:01:43 MDT; 2 days ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 6065 (sshd)
   CGroup: /system.slice/sshd.service
           └─6065 /usr/sbin/sshd -D

May 07 15:01:43 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
May 07 15:01:43 localhost.localdomain sshd[6065]: Server listening on 0.0.0.0 port 22.
May 07 15:01:43 localhost.localdomain sshd[6065]: Server listening on :: port 22.
May 07 15:01:43 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
May 08 10:13:53 localhost.localdomain sshd[83691]: Accepted password for admin from 192.168.1.1 port 50330 ssh2
May 08 10:15:33 localhost.localdomain sshd[84391]: Accepted password for admin from 192.168.1.1 port 50332 ssh2
[admin@localhost ~]$
```

This server is running both ssh and apache2 for remote connection and web hosting respectively.

Open Ports

```
[admin@localhost ~]$ sudo firewall-cmd --list-all
[sudo] password for admin:
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: ssh dhcpv6-client
  ports: 80/tcp 443/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[admin@localhost ~]$ sudo firewall-cmd --list-services
ssh dhcpv6-client
[admin@localhost ~]$ sudo firewall-cmd --zone=public --list-ports
80/tcp 443/tcp
[admin@localhost ~]$ sudo firewall-cmd --zone=external --list-ports

[admin@localhost ~]$ sudo firewall-cmd --zone=internal --list-ports

[admin@localhost ~]$
```

This server has port 80 for http, port 443 for secure connections as well as a dhcp client.

Sudoers File

```
Defaults    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
[admin@localhost ~]$
```

Users

/etc/group

```
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:admin
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
utmp:x:22:
utempter:x:35:
input:x:999:
systemd-journal:x:190:
systemd-network:x:192:
dbus:x:81:
polkitd:x:998:
libstoragemgmt:x:997:
ssh_keys:x:996:
abrt:x:173:
rpc:x:32:
tss:x:59:
sshd:x:74:
slocate:x:21:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
chrony:x:995:
tcpdump:x:72:
admin:x:1000:admin
apache:x:48:
[admin@localhost ~]$
```

/etc/passwd

```
[admin@localhost ~]$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
admin:x:1000:1000:Administrator:/home/admin:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
[admin@localhost ~]$
```

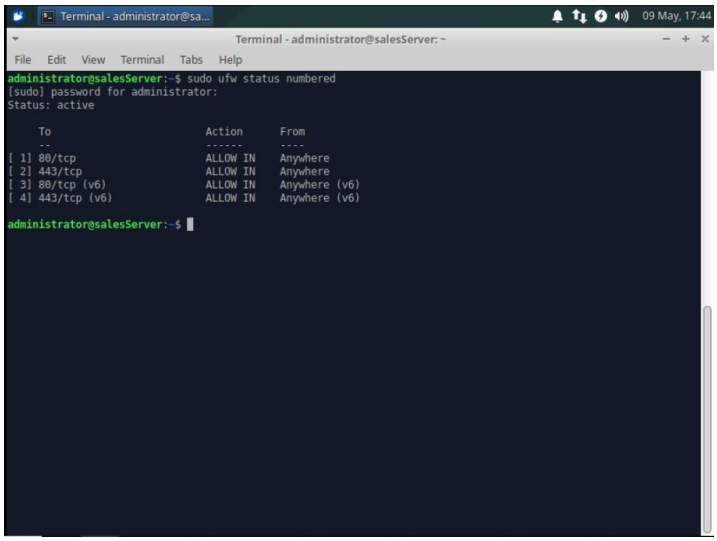
Sales Team Server

Services

```
Terminal - administrator@sa...                                   09 May, 16:56
Terminal - administrator@salesServer: ~
File  Edit  View  Terminal  Tabs  Help
administrator@salesServer:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Wed 2019-05-01 00:01:10 MDT; 1 weeks 1 days ago
 Main PID: 630 (apache2)
    Tasks: 55 (limit: 4588)
   CGroup: /system.slice/apache2.service
           ├─  630 /usr/sbin/apache2 -k start
           ├─11827 /usr/sbin/apache2 -k start
           └─11828 /usr/sbin/apache2 -k start

May 06 00:09:44 salesServer systemd[1]: Reloaded The Apache HTTP Server.
May 07 00:07:57 salesServer systemd[1]: Reloading The Apache HTTP Server.
May 07 00:07:57 salesServer apachectl[8494]: AH00558: apache2: Could not reliably determine the server's fully
May 07 00:07:57 salesServer systemd[1]: Reloaded The Apache HTTP Server.
May 08 00:08:57 salesServer systemd[1]: Reloading The Apache HTTP Server.
May 08 00:08:57 salesServer apachectl[9571]: AH00558: apache2: Could not reliably determine the server's fully
May 08 00:08:57 salesServer systemd[1]: Reloaded The Apache HTTP Server.
May 09 00:07:57 salesServer systemd[1]: Reloading The Apache HTTP Server.
May 09 00:07:57 salesServer apachectl[11823]: AH00558: apache2: Could not reliably determine the server's fully
May 09 00:07:57 salesServer systemd[1]: Reloaded The Apache HTTP Server.
lines 1-22/22 (END)
```

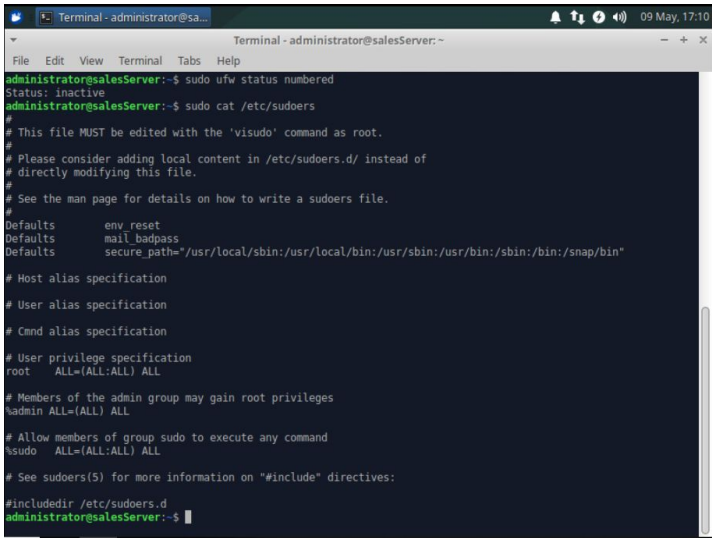
This server is running apache2.

Open Ports



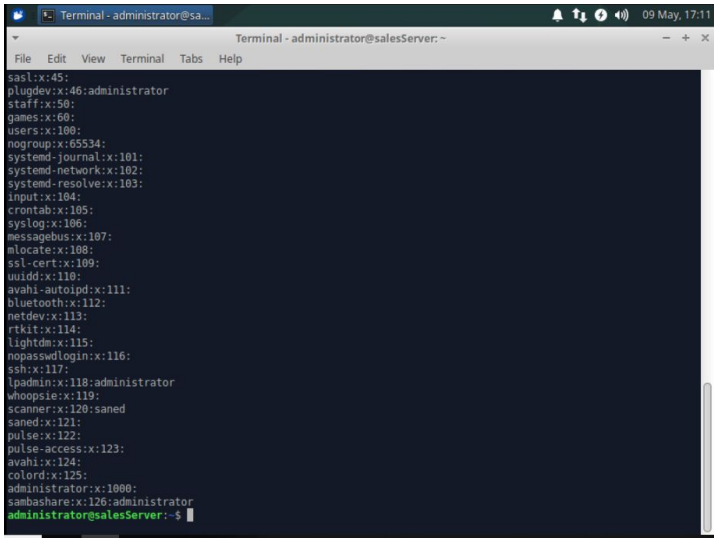
This server also has the usual port 80 and port 443.

Sudoers File

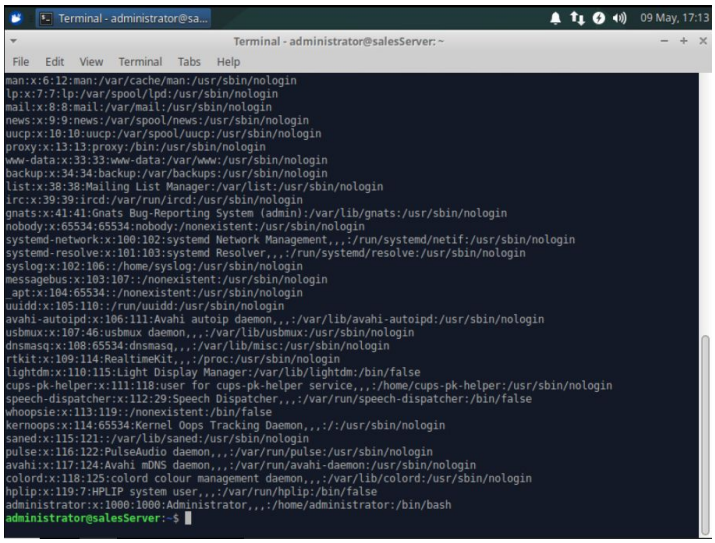


Users

/etc/group



/etc/passwd



Future Growth

With our current system, we could add more servers and clients to our internal network. This allows for growth within our company through the creation of new departments. Our system also

is flexible due to its simplicity which would help with changes in organizational structure. Some examples of additions to our internal network could be new servers for departments or new sets of client workstations designed for different purposes. In other words we could allocate a set of workstations for different departments and segregate them within our network. We could segregate our servers on the network in order to protect certain information. For example, we may want to give sales a seperate ip address so that clients on the network would not be able to access that information. Right now we decided it would be best to stick with a more simple network structure since we are working for such a rapidly developing company. This way if we have to make sudden extreme changes it will be easy to do that or start from scratch if necessary as well. In the future, we plan to add a breeding department which would require a new server and some clients. The server would probably have ssh and apache2 for connection and web hosting as we do with our other servers. Moving forward we would want to segregate the new server in the network to protect the sensitive breeding data and also isolate the clients so that if a system is exploited breeding and sales data would not be at risk. Breeding is a more artistic manner so logically the breeding department may want mac systems for there workstations, which we could implement as well. Our network could also probably use a switch to split these connections and better divi up the network by creating multiple different vlans to protect our systems, as we have discussed .

Participation Notes

Joe:
Setup DC1 and DC2 and windows workstations for employees on the domain controllers

Sean:
Setup the DMZ and public facing website, internal network, sales server and software team server for internal use. Also created the Linux MOTD's for user logins.

Tai:
Wrote the set of policies that describe the implemented business logic into the system.

Mauricio:

Created the technical documentation for the created servers.