Scenario:

Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result, is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI, we are happy to bring you on as our first InfoSec employee! Once you are settled in and finished orientation, we have your first 2-Weeks assignments ready.

Week One:

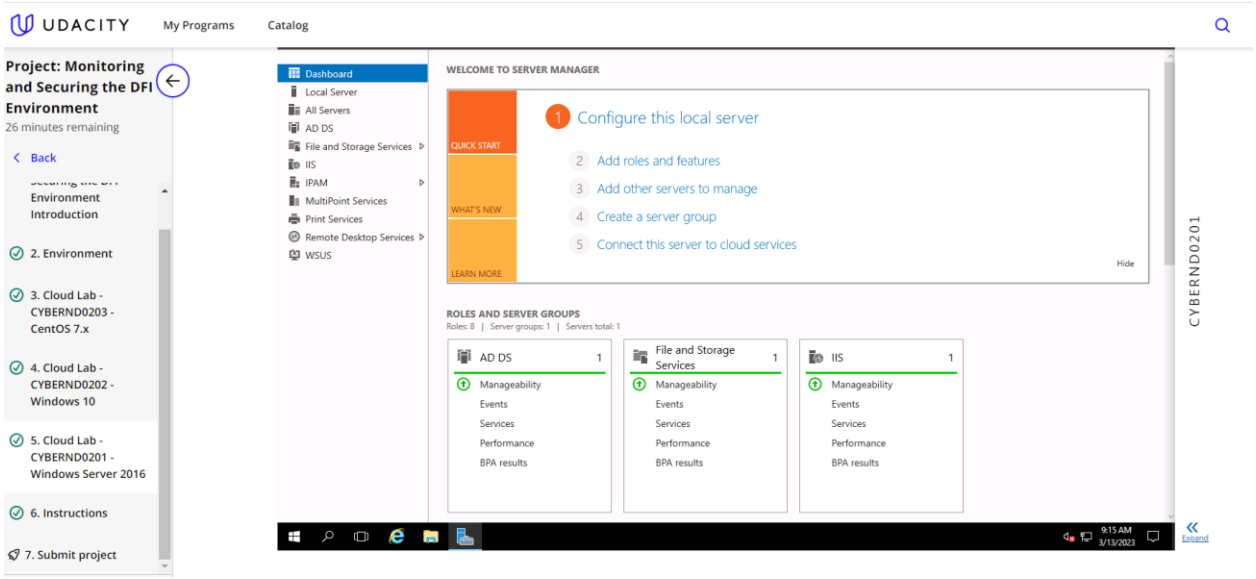
1. **Connect to the servers:**

All of the subsequent steps will take place in the DFI environment. To get started, connect to the Windows server 2016 and Linux (CentOS) machines.

- **Windows server 2016** - If you are using Udacity cloud lab, you can directly log into the machine in the classroom. If you have set up the Windows server 2016 VM in your personal Azure account, you will have to use the RDP to connect.
- **Linux (CentOS) server** - If you are using Udacity cloud lab, you can log in using via SSH using Terminal/Gitbash/OpenSSH/Bastion. If you have set up the Linux server in your personal Azure account, you will have to use SSH to connect.
- Alternatively, you can use the **Windows 10** machine as a JumpVM for the other two VMs. Meaning, that you can use the Windows 10 VM to:
    - log into the Windows server 2016 via RDP
    - log into the Linux server via SSH using PuTTy, Gitbash, or OpenSSH.

[Please provide screenshots to show:]

- a connection to Windows server 2016.



- a connection to the Linux server using SSH.

2. **Security Analysis:**

DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with our file and application servers.

Please perform an analysis of the Windows server and provide a written report detailing any security configuration issues found and a brief explanation and justification of the changes you recommend. DFI is a PCI-compliant organization and will likely be Sarbanes-Oxley in the near future.

Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege, and other resources to determine the changes that should be made. Note changes can be to **add/remove/change** services, permissions, and other settings. Defense-in-Depth documentation. NIST 800-123 (other NIST documents could also apply.)

[Place your security analysis here.]

Based on the fact that DFI there are 4 types of departments: HR, IT, Operation, Public, the admin and the users within do not have the appropriate permissions, and that needs to change. On The admin of each department needs full control and the users needs read-execute rights to be able to do their job.- when the situation requires elevated rights, then the rights will be granted. The permissions needs a periodic review from management, and for the user that left the company, theirs accounts to be deleted. Some features are outdated and requires update or system patches.

And finally on my plate, the windows firewall needs to be activated in order to limit outside access to internal resource.

On IT department, the creator owner have special permissions, the system have full permissions, the HR have full control, Admin have full control, On Operation department , the creator owner have special permissions, the system have full permissions, the HR have full control, Admin have full control,

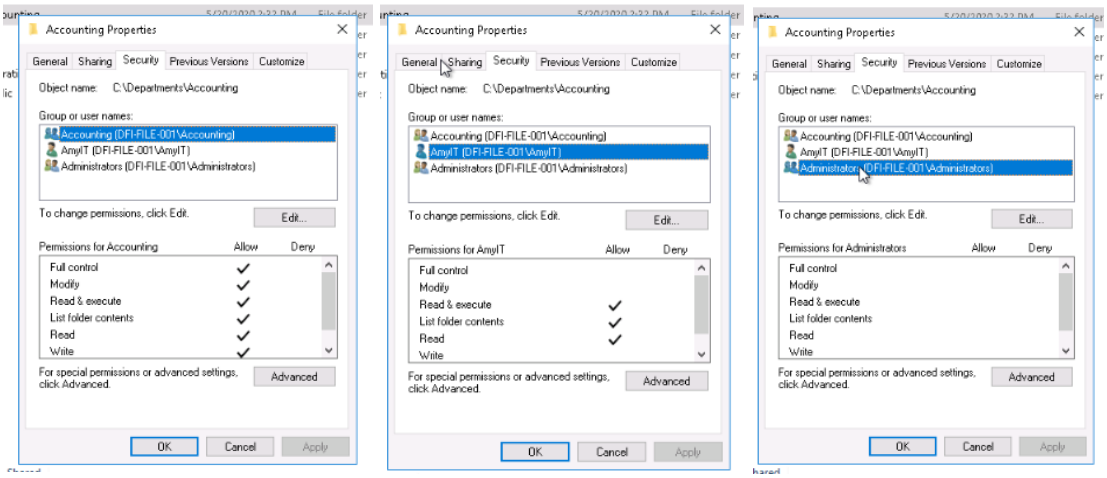
On Public department, the creator owner have no permissions, the system have limited/restricted to some folders or files permissions, Admin have limited/restricted to some folders or files permissions, and Users have modify and write permissions.

Write a report detailing 3 primary areas

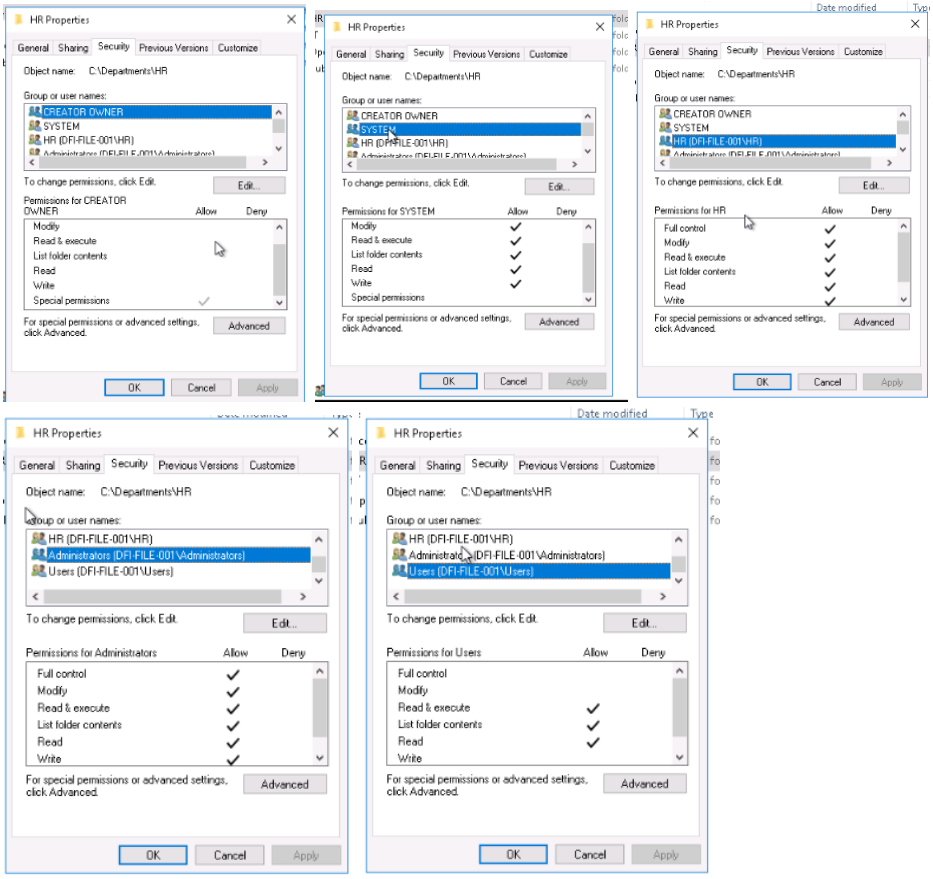
We did the following:

A. Verify the folders **permissions** for every department.

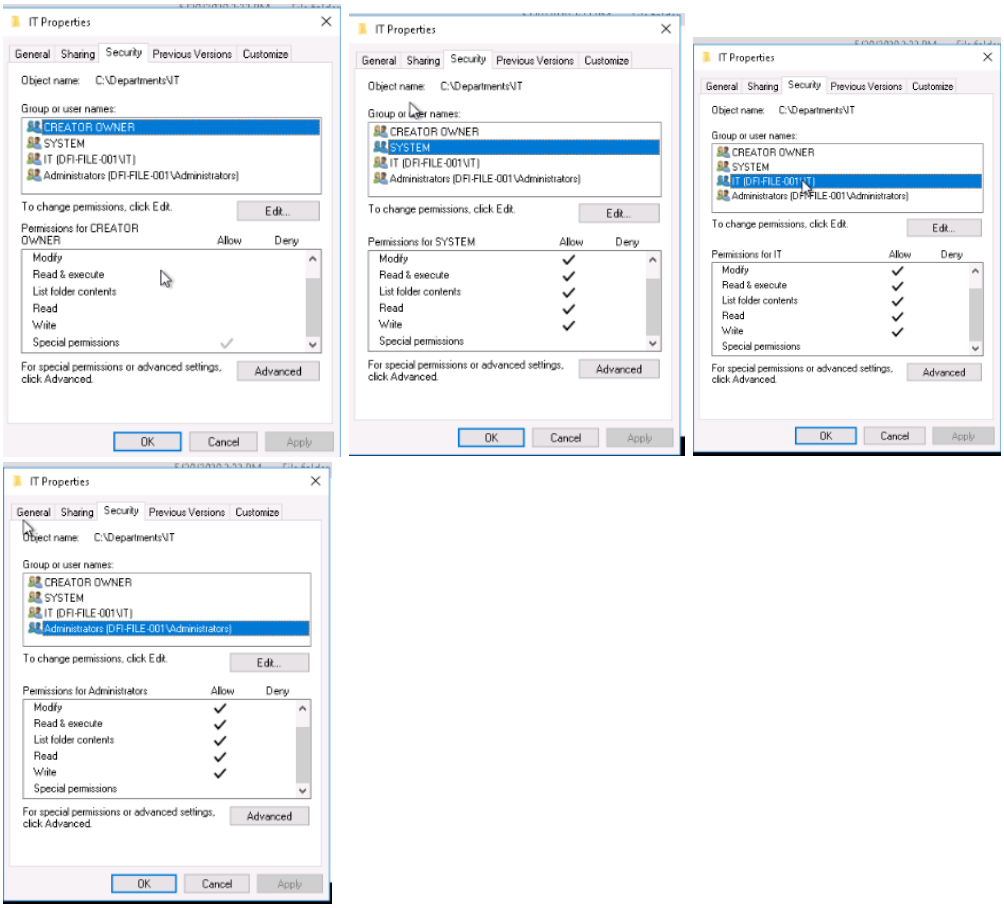
1. Right clicked the folder and then clicked Properties
2. Select Security Tab
3. Select Edit
4. Select add typed maintenance, click check names, and
5. Verified the permissions for every user the permissions, then clicked ok



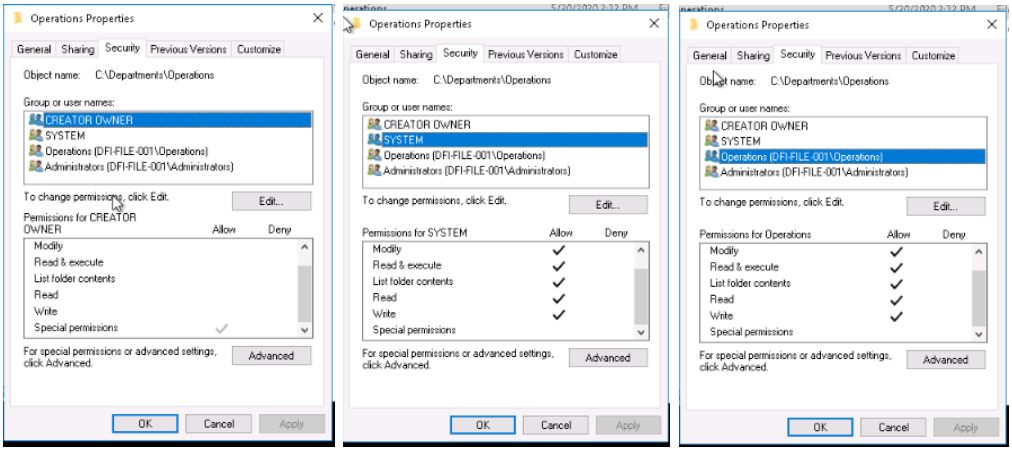
HR.

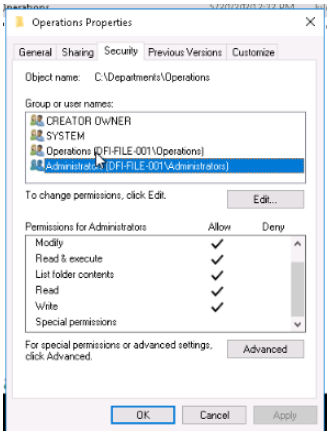

HR Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\HR
Group or user names:
CREATOR OWNER
SYSTEM
HR (DFI-FILE-001\HR)
Administrators (DFI-FILE-001\Administrators)
Users (DFI-FILE-001\Users)
To change permissions, click Edit.
Edit...
Permissions for CREATOR OWNER
Permissions for SYSTEM
Permissions for HR
Permissions for Administrators
Permissions for Users
Allow
Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
Full control
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

IT

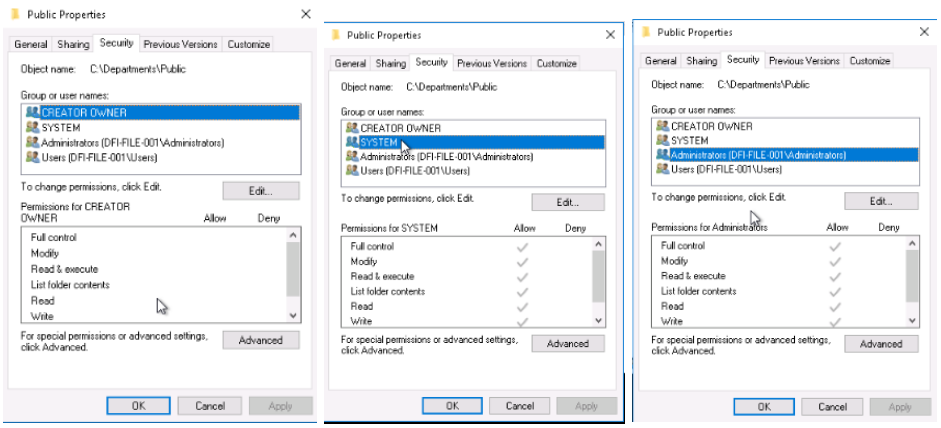

IT Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\IT
Group or user names:
CREATOR OWNER
SYSTEM
IT (DFI-FILE-001\IT)
Administrators (DFI-FILE-001\Administrators)
To change permissions, click Edit.
Edit...
Permissions for CREATOR OWNER
Allow Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply
IT Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\IT
Group or user names:
CREATOR OWNER
SYSTEM
IT (DFI-FILE-001\IT)
Administrators (DFI-FILE-001\Administrators)
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply
IT Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\IT
Group or user names:
CREATOR OWNER
SYSTEM
IT (DFI-FILE-001\IT)
Administrators (DFI-FILE-001\Administrators)
To change permissions, click Edit.
Edit...
Permissions for IT
Allow Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply
IT Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\IT
Group or user names:
CREATOR OWNER
SYSTEM
IT (DFI-FILE-001\IT)
Administrators (DFI-FILE-001\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Administrators
Allow Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply

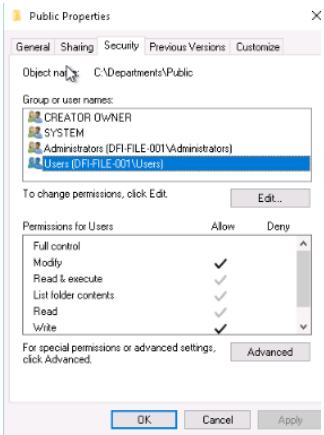
Operation:


Operations Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\Operations
Group or user names:
CREATOR OWNER
SYSTEM
Operations (DFI-FILE-001\Operations)
Administrators (DFI-FILE-001\Administrators)
To change permissions, click Edit.
Edit...
Permissions for CREATOR OWNER
Allow Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply
Operations Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\Operations
Group or user names:
CREATOR OWNER
SYSTEM
Operations (DFI-FILE-001\Operations)
Administrators (DFI-FILE-001\Administrators)
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply
Operations Properties
General Sharing Security Previous Versions Customize
Object name: C:\Departments\Operations
Group or user names:
CREATOR OWNER
SYSTEM
Operations (DFI-FILE-001\Operations)
Administrators (DFI-FILE-001\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Operations
Allow Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply

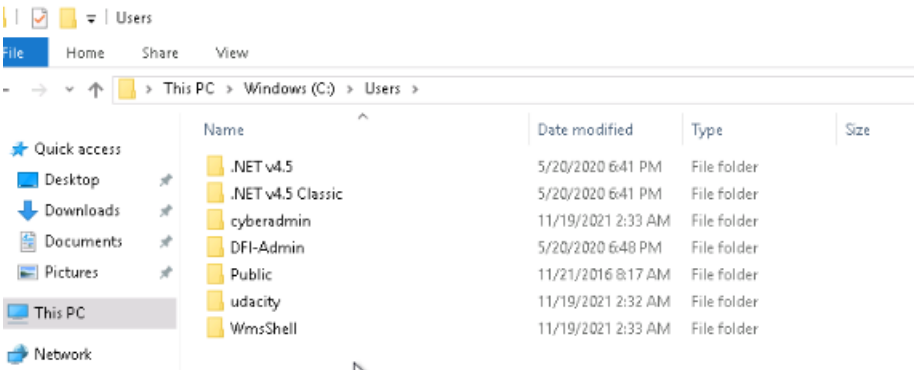


Public:





Users:



B. Type "**Services**" in search bar and clicked on services app.
There we browsed throughout the services and identified the followings that are not needed on a professional computer:

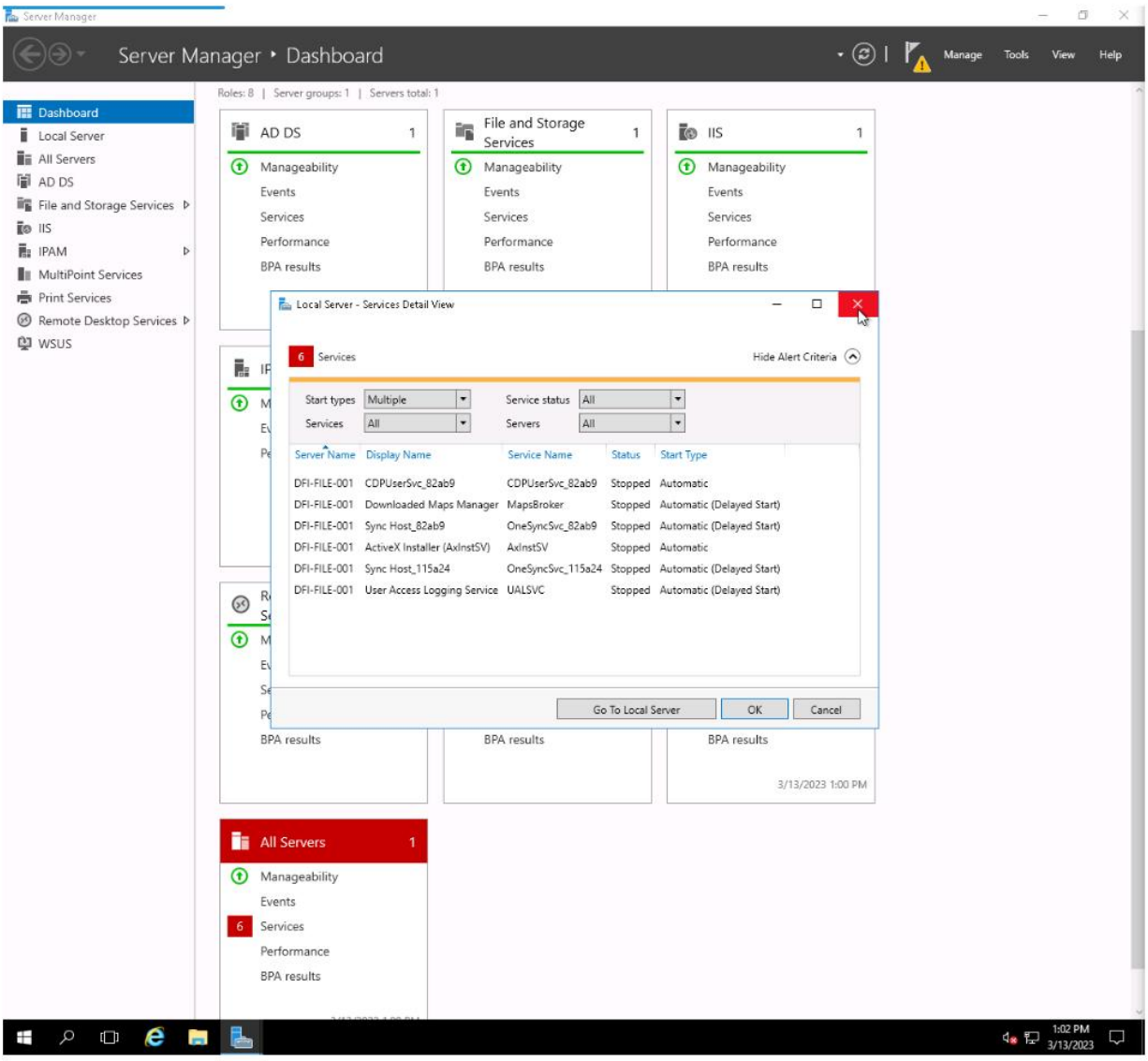
Xbox Live Game save – Startup type = Manual (Trigger Startup),

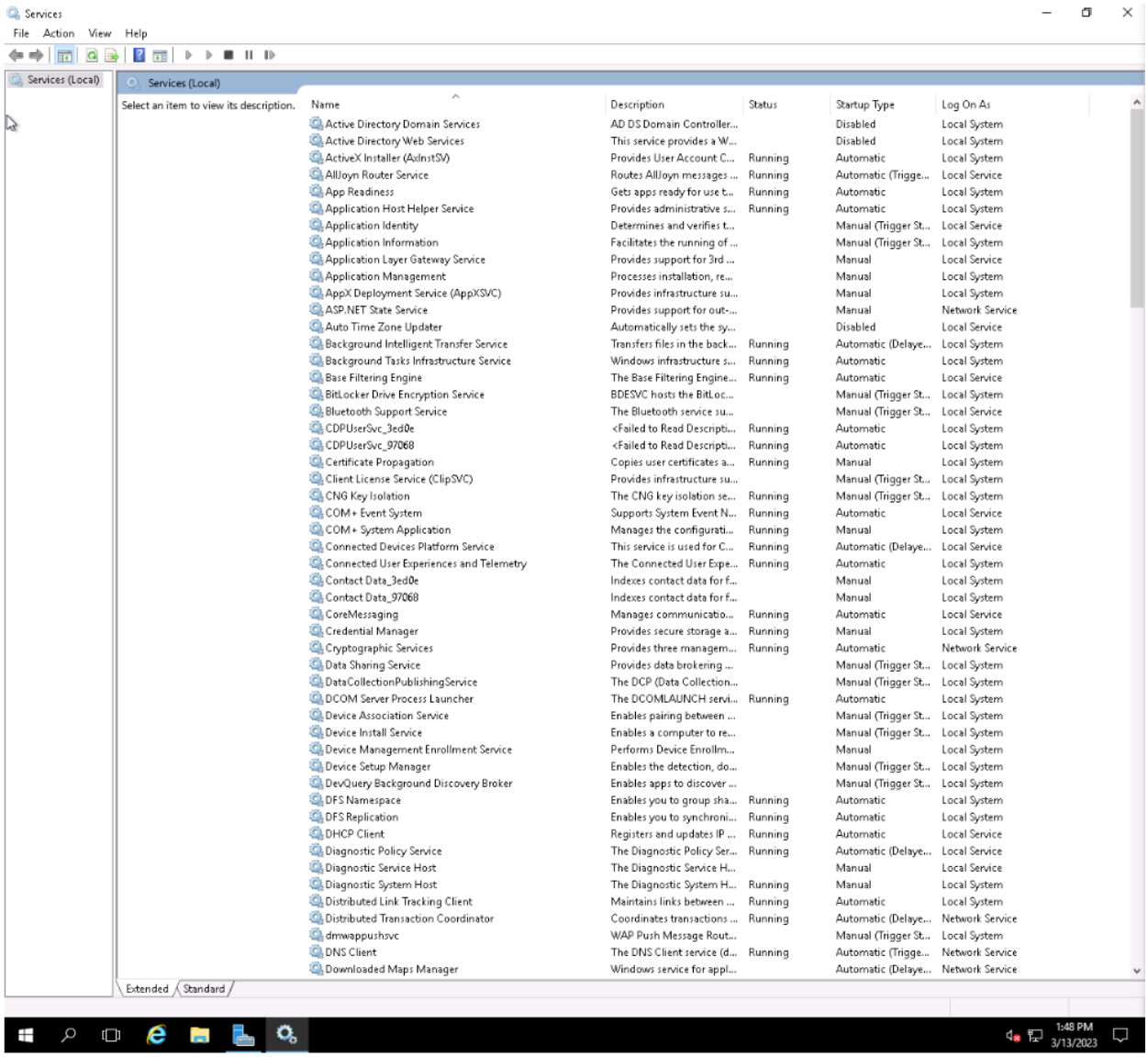
Xbox Live Auth Manager – Startup type = Manual

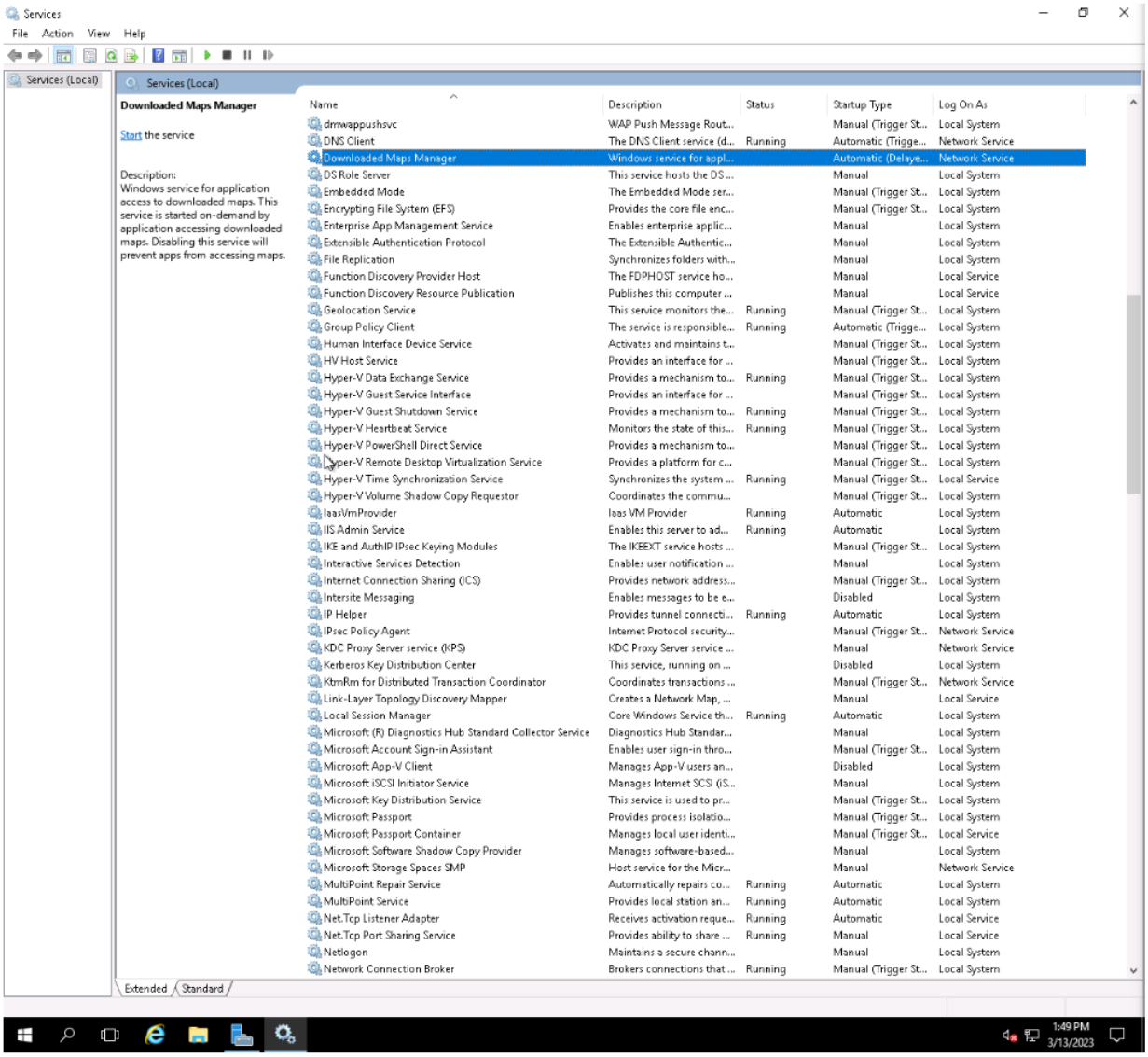
Bluetooth Support Service - Startup type = Manual (Trigger Startup),

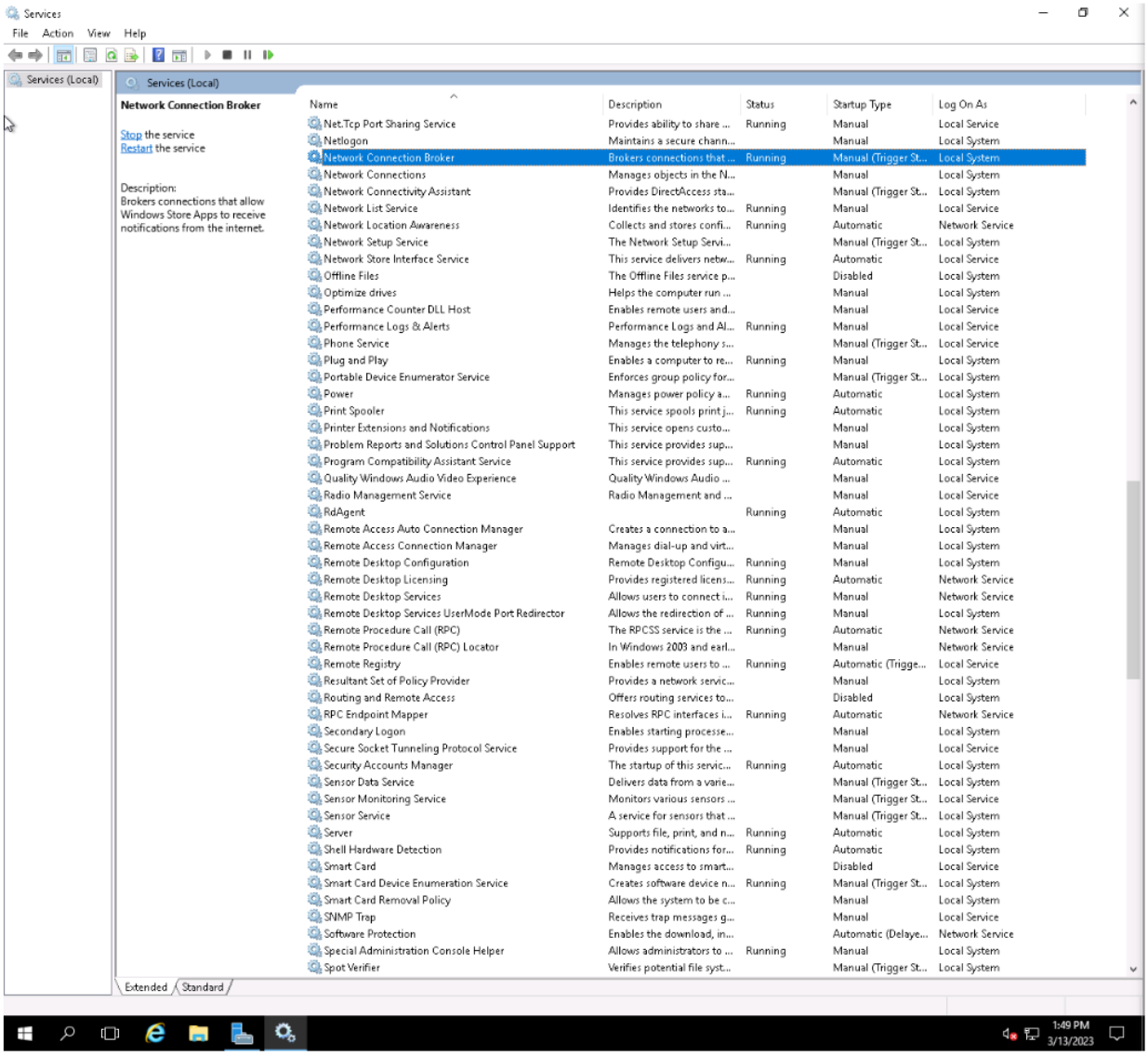
ActiveX installer Startup type = Automatic.

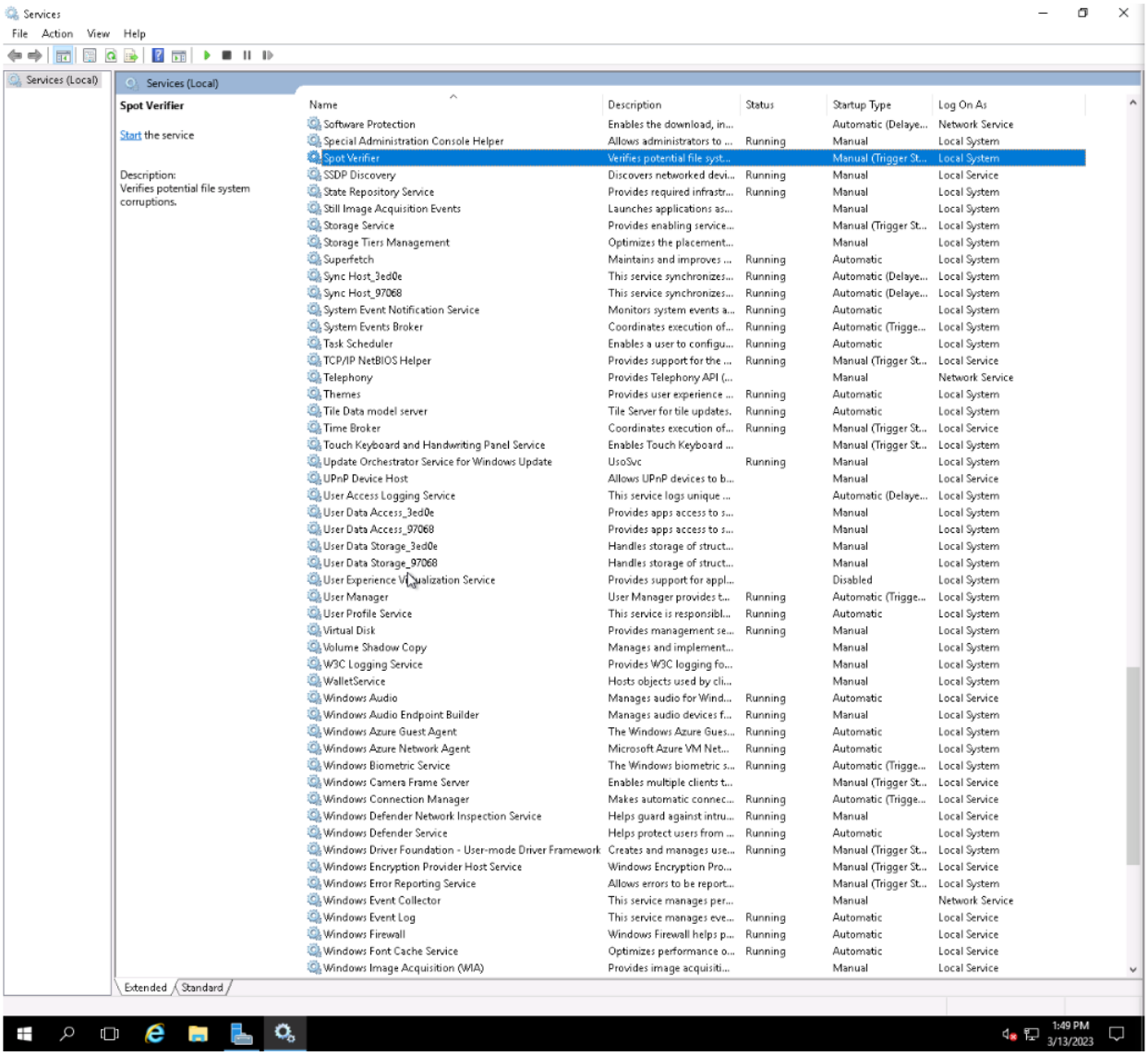
Also, the Server Manager shows that 6 services on the server are stopped. (further investigation is required)

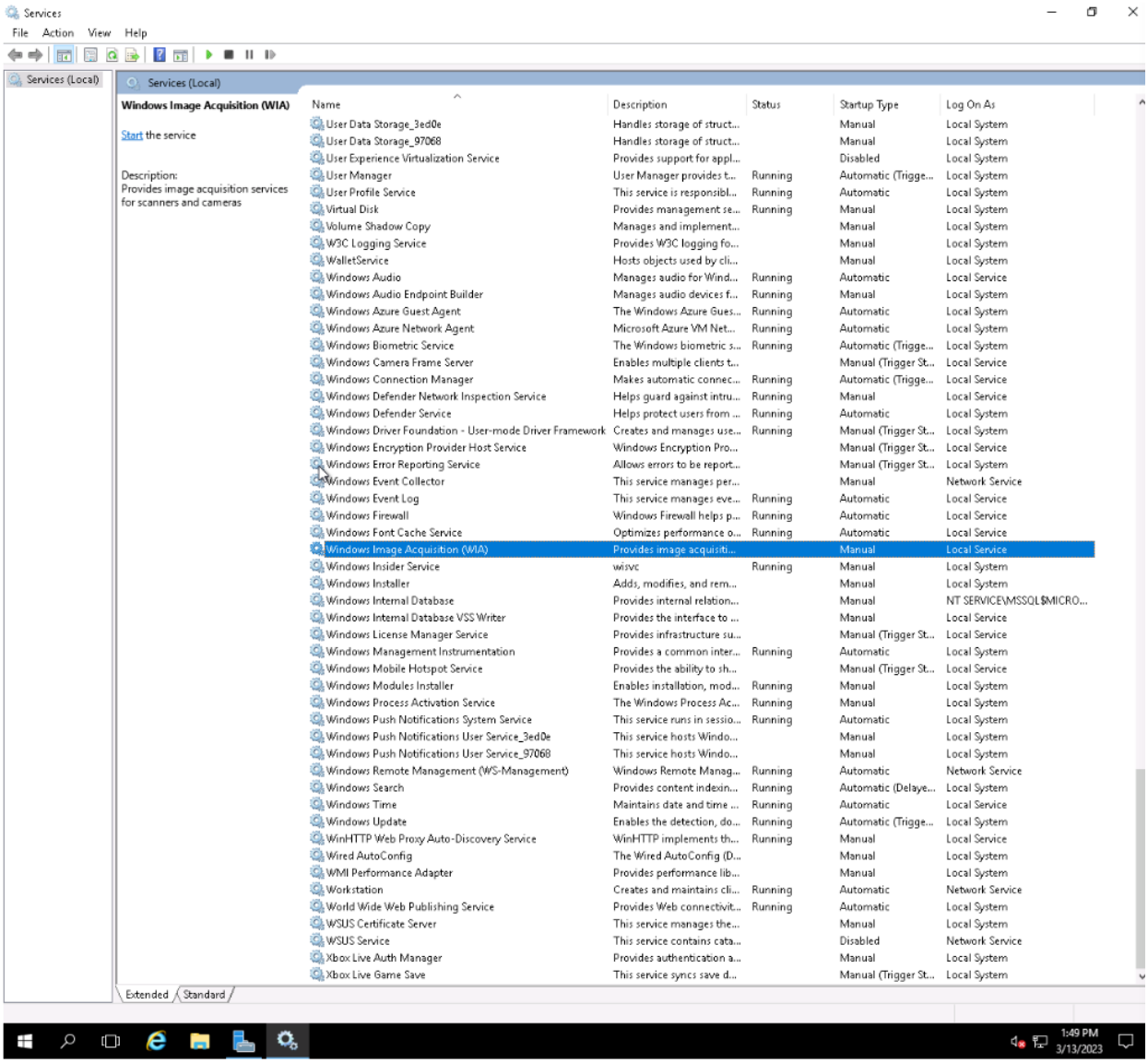

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Roles: 8 | Server groups: 1 | Servers total: 1
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
IIS
IPAM
MultiPoint Services
Print Services
Remote Desktop Services
WSUS
AD DS 1
Manageability
Events
Services
Performance
BPA results
File and Storage Services 1
Manageability
Events
Services
Performance
BPA results
IIS 1
Manageability
Events
Services
Performance
BPA results
Local Server - Services Detail View
6 Services
Hide Alert Criteria
Start types Multiple
Service status All
Services All
Servers All
Server Name
Display Name
Service Name
Status
Start Type
DFI-FILE-001 CDPUserSvc_82ab9 CDPUserSvc_82ab9 Stopped Automatic
DFI-FILE-001 Downloaded Maps Manager MapsBroker Stopped Automatic (Delayed Start)
DFI-FILE-001 Sync Host_82ab9 OneSyncSvc_82ab9 Stopped Automatic (Delayed Start)
DFI-FILE-001 ActiveX Installer (AxInstSV) AxInstSV Stopped Automatic
DFI-FILE-001 Sync Host_115a24 OneSyncSvc_115a24 Stopped Automatic (Delayed Start)
DFI-FILE-001 User Access Logging Service UALSVC Stopped Automatic (Delayed Start)
Go To Local Server
OK
Cancel
BPA results
BPA results
BPA results
3/13/2023 1:00 PM
All Servers 1
Manageability
Events
6 Services
Performance
BPA results
1:02 PM
3/13/2023


Services
File Action View Help
Services (Local)
Services (Local)
Select an item to view its description.
Name
Description
Status
Startup Type
Log On As
Active Directory Domain Services
AD DS Domain Controller...
Disabled
Local System
Active Directory Web Services
This service provides a W...
Disabled
Local System
ActiveX Installer (AxInstSV)
Provides User Account C...
Running
Automatic
Local System
AllJoyn Router Service
Routes AllJoyn messages ...
Running
Automatic (Trigge...
Local Service
App Readiness
Gets apps ready for use t...
Running
Automatic
Local System
Application Host Helper Service
Provides administrative s...
Running
Automatic
Local System
Application Identity
Determines and verifies t...
Manual (Trigger St...
Local Service
Application Information
Facilitates the running of ...
Manual (Trigger St...
Local System
Application Layer Gateway Service
Provides support for 3rd ...
Manual
Local Service
Application Management
Processes installation, re...
Manual
Local System
AppX Deployment Service (AppXSVC)
Provides infrastructure su...
Manual
Local System
ASP.NET State Service
Provides support for out-...
Manual
Network Service
Auto Time Zone Updater
Automatically sets the sy...
Disabled
Local Service
Background Intelligent Transfer Service
Transfers files in the back...
Running
Automatic (Delaye...
Local System
Background Tasks Infrastructure Service
Windows infrastructure s...
Running
Automatic
Local System
Base Filtering Engine
The Base Filtering Engine...
Running
Automatic
Local Service
BitLocker Drive Encryption Service
BDESVC hosts the BitLoc...
Manual (Trigger St...
Local System
Bluetooth Support Service
The Bluetooth service su...
Manual (Trigger St...
Local Service
CDPUserSvc_3ed0e
<Failed to Read Descripti...
Running
Automatic
Local System
CDPUserSvc_97068
<Failed to Read Descripti...
Running
Automatic
Local System
Certificate Propagation
Copies user certificates a...
Running
Manual
Local System
Client License Service (ClipSVC)
Provides infrastructure su...
Manual (Trigger St...
Local System
CNG Key Isolation
The CNG key isolation se...
Running
Manual (Trigger St...
Local System
COM+ Event System
Supports System Event N...
Running
Automatic
Local Service
COM+ System Application
Manages the configurati...
Running
Manual
Local System
Connected Devices Platform Service
This service is used for C...
Running
Automatic (Delaye...
Local Service
Connected User Experiences and Telemetry
The Connected User Expe...
Running
Automatic
Local System
Contact Data_3ed0e
Indexes contact data for f...
Manual
Local System
Contact Data_97068
Indexes contact data for f...
Manual
Local System
CoreMessaging
Manages communicatio...
Running
Automatic
Local Service
Credential Manager
Provides secure storage a...
Running
Manual
Local System
Cryptographic Services
Provides three managem...
Running
Automatic
Network Service
Data Sharing Service
Provides data brokering ...
Manual (Trigger St...
Local System
DataCollectionPublishingService
The DCP (Data Collection...
Manual (Trigger St...
Local System
DCOM Server Process Launcher
The DCOMLAUNCH servi...
Running
Automatic
Local System
Device Association Service
Enables pairing between ...
Manual (Trigger St...
Local System
Device Install Service
Enables a computer to re...
Manual (Trigger St...
Local System
Device Management Enrollment Service
Performs Device Enrollm...
Manual
Local System
Device Setup Manager
Enables the detection, do...
Manual (Trigger St...
Local System
DevQuery Background Discovery Broker
Enables apps to discover ...
Manual (Trigger St...
Local System
DFS Namespace
Enables you to group sha...
Running
Automatic
Local System
DFS Replication
Enables you to synchroni...
Running
Automatic
Local System
DHCP Client
Registers and updates IP ...
Running
Automatic
Local Service
Diagnostic Policy Service
The Diagnostic Policy Ser...
Running
Automatic (Delaye...
Local Service
Diagnostic Service Host
The Diagnostic Service H...
Manual
Local Service
Diagnostic System Host
The Diagnostic System H...
Running
Manual
Local System
Distributed Link Tracking Client
Maintains links between ...
Running
Automatic
Local System
Distributed Transaction Coordinator
Coordinates transactions ...
Running
Automatic (Delaye...
Network Service
dmwappushsvc
WAP Push Message Rout...
Manual (Trigger St...
Local System
DNS Client
The DNS Client service (d...
Running
Automatic (Trigge...
Network Service
Downloaded Maps Manager
Windows service for appl...
Automatic (Delaye...
Network Service
Extended
Standard
1:48 PM
3/13/2023


Services
File Action View Help
Services (Local)
Services (Local)
Downloaded Maps Manager
Start the service
Description:
Windows service for application access to downloaded maps. This service is started on-demand by application accessing downloaded maps. Disabling this service will prevent apps from accessing maps.
Name
Description
Status
Startup Type
Log On As
dmwappushsvc
WAP Push Message Rout...
Manual (Trigger St...
Local System
DNS Client
The DNS Client service (d...
Running
Automatic (Trigge...
Network Service
Downloaded Maps Manager
Windows service for appl...
Automatic (Delaye...
Network Service
DS Role Server
This service hosts the DS ...
Manual
Local System
Embedded Mode
The Embedded Mode ser...
Manual (Trigger St...
Local System
Encrypting File System (EFS)
Provides the core file enc...
Manual (Trigger St...
Local System
Enterprise App Management Service
Enables enterprise applic...
Manual
Local System
Extensible Authentication Protocol
The Extensible Authentic...
Manual
Local System
File Replication
Synchronizes folders with...
Manual
Local System
Function Discovery Provider Host
The FDPHOST service ho...
Manual
Local Service
Function Discovery Resource Publication
Publishes this computer ...
Manual
Local Service
Geolocation Service
This service monitors the...
Running
Manual (Trigger St...
Local System
Group Policy Client
The service is responsible...
Running
Automatic (Trigge...
Local System
Human Interface Device Service
Activates and maintains t...
Manual (Trigger St...
Local System
HV Host Service
Provides an interface for ...
Manual (Trigger St...
Local System
Hyper-V Data Exchange Service
Provides a mechanism to...
Running
Manual (Trigger St...
Local System
Hyper-V Guest Service Interface
Provides an interface for ...
Manual (Trigger St...
Local System
Hyper-V Guest Shutdown Service
Provides a mechanism to...
Running
Manual (Trigger St...
Local System
Hyper-V Heartbeat Service
Monitors the state of this...
Running
Manual (Trigger St...
Local System
Hyper-V PowerShell Direct Service
Provides a mechanism to...
Manual (Trigger St...
Local System
Hyper-V Remote Desktop Virtualization Service
Provides a platform for c...
Manual (Trigger St...
Local System
Hyper-V Time Synchronization Service
Synchronizes the system ...
Running
Manual (Trigger St...
Local Service
Hyper-V Volume Shadow Copy Requestor
Coordinates the commu...
Manual (Trigger St...
Local System
IaasVmProvider
Iaas VM Provider
Running
Automatic
Local System
IIS Admin Service
Enables this server to ad...
Running
Automatic
Local System
IKE and AuthIP IPsec Keying Modules
The IKEEXT service hosts ...
Manual (Trigger St...
Local System
Interactive Services Detection
Enables user notification ...
Manual
Local System
Internet Connection Sharing (ICS)
Provides network address...
Manual (Trigger St...
Local System
Intersite Messaging
Enables messages to be e...
Disabled
Local System
IP Helper
Provides tunnel connecti...
Running
Automatic
Local System
IPsec Policy Agent
Internet Protocol security...
Manual (Trigger St...
Network Service
KDC Proxy Server service (KPS)
KDC Proxy Server service ...
Manual
Network Service
Kerberos Key Distribution Center
This service, running on ...
Disabled
Local System
KtmRm for Distributed Transaction Coordinator
Coordinates transactions ...
Manual (Trigger St...
Network Service
Link-Layer Topology Discovery Mapper
Creates a Network Map, ...
Manual
Local Service
Local Session Manager
Core Windows Service th...
Running
Automatic
Local System
Microsoft (R) Diagnostics Hub Standard Collector Service
Diagnostics Hub Standar...
Manual
Local System
Microsoft Account Sign-in Assistant
Enables user sign-in thro...
Manual (Trigger St...
Local System
Microsoft App-V Client
Manages App-V users an...
Disabled
Local System
Microsoft iSCSI Initiator Service
Manages Internet SCSI (iS...
Manual
Local System
Microsoft Key Distribution Service
This service is used to pr...
Manual (Trigger St...
Local System
Microsoft Passport
Provides process isolatio...
Manual (Trigger St...
Local System
Microsoft Passport Container
Manages local user identi...
Manual (Trigger St...
Local Service
Microsoft Software Shadow Copy Provider
Manages software-based...
Manual
Local System
Microsoft Storage Spaces SMP
Host service for the Micr...
Manual
Network Service
MultiPoint Repair Service
Automatically repairs co...
Running
Automatic
Local System
MultiPoint Service
Provides local station an...
Running
Automatic
Local System
Net.Tcp Listener Adapter
Receives activation reque...
Running
Automatic
Local Service
Net.Tcp Port Sharing Service
Provides ability to share ...
Running
Manual
Local Service
Netlogon
Maintains a secure chann...
Manual
Local System
Network Connection Broker
Brokers connections that ...
Running
Manual (Trigger St...
Local System
Extended
Standard
1:49 PM
3/13/2023


Services
File Action View Help
Services (Local)
Services (Local)
Network Connection Broker
Stop the service
Restart the service
Description:
Brokers connections that allow Windows Store Apps to receive notifications from the internet.
Name
Description
Status
Startup Type
Log On As
Net.Tcp Port Sharing Service
Provides ability to share ...
Running
Manual
Local Service
Netlogon
Maintains a secure chann...
Manual
Local System
Network Connection Broker
Brokers connections that ...
Running
Manual (Trigger St...
Local System
Network Connections
Manages objects in the N...
Manual
Local System
Network Connectivity Assistant
Provides DirectAccess sta...
Manual (Trigger St...
Local System
Network List Service
Identifies the networks to...
Running
Manual
Local Service
Network Location Awareness
Collects and stores confi...
Running
Automatic
Network Service
Network Setup Service
The Network Setup Servi...
Manual (Trigger St...
Local System
Network Store Interface Service
This service delivers netw...
Running
Automatic
Local Service
Offline Files
The Offline Files service p...
Disabled
Local System
Optimize drives
Helps the computer run ...
Manual
Local System
Performance Counter DLL Host
Enables remote users and...
Manual
Local Service
Performance Logs & Alerts
Performance Logs and Al...
Running
Manual
Local Service
Phone Service
Manages the telephony s...
Manual (Trigger St...
Local Service
Plug and Play
Enables a computer to re...
Running
Manual
Local System
Portable Device Enumerator Service
Enforces group policy for...
Manual (Trigger St...
Local System
Power
Manages power policy a...
Running
Automatic
Local System
Print Spooler
This service spools print j...
Running
Automatic
Local System
Printer Extensions and Notifications
This service opens custo...
Manual
Local System
Problem Reports and Solutions Control Panel Support
This service provides sup...
Manual
Local System
Program Compatibility Assistant Service
This service provides sup...
Running
Automatic
Local System
Quality Windows Audio Video Experience
Quality Windows Audio ...
Manual
Local Service
Radio Management Service
Radio Management and ...
Manual
Local Service
RdAgent
Running
Automatic
Local System
Remote Access Auto Connection Manager
Creates a connection to a...
Manual
Local System
Remote Access Connection Manager
Manages dial-up and virt...
Manual
Local System
Remote Desktop Configuration
Remote Desktop Configu...
Running
Manual
Local System
Remote Desktop Licensing
Provides registered licens...
Running
Automatic
Network Service
Remote Desktop Services
Allows users to connect i...
Running
Manual
Network Service
Remote Desktop Services UserMode Port Redirector
Allows the redirection of ...
Running
Manual
Local System
Remote Procedure Call (RPC)
The RPCSS service is the ...
Running
Automatic
Network Service
Remote Procedure Call (RPC) Locator
In Windows 2003 and earl...
Manual
Network Service
Remote Registry
Enables remote users to ...
Running
Automatic (Trigge...
Local Service
Resultant Set of Policy Provider
Provides a network servic...
Manual
Local System
Routing and Remote Access
Offers routing services to...
Disabled
Local System
RPC Endpoint Mapper
Resolves RPC interfaces i...
Running
Automatic
Network Service
Secondary Logon
Enables starting processe...
Manual
Local System
Secure Socket Tunneling Protocol Service
Provides support for the ...
Manual
Local Service
Security Accounts Manager
The startup of this servic...
Running
Automatic
Local System
Sensor Data Service
Delivers data from a varie...
Manual (Trigger St...
Local System
Sensor Monitoring Service
Monitors various sensors ...
Manual (Trigger St...
Local Service
Sensor Service
A service for sensors that ...
Manual (Trigger St...
Local System
Server
Supports file, print, and n...
Running
Automatic
Local System
Shell Hardware Detection
Provides notifications for...
Running
Automatic
Local System
Smart Card
Manages access to smart...
Disabled
Local Service
Smart Card Device Enumeration Service
Creates software device n...
Running
Manual (Trigger St...
Local System
Smart Card Removal Policy
Allows the system to be c...
Manual
Local System
SNMP Trap
Receives trap messages g...
Manual
Local Service
Software Protection
Enables the download, in...
Automatic (Delaye...
Network Service
Special Administration Console Helper
Allows administrators to ...
Running
Manual
Local System
Spot Verifier
Verifies potential file syst...
Manual (Trigger St...
Local System
Extended
Standard
1:49 PM
3/13/2023


Services
File Action View Help
Services (Local)
Services (Local)
Spot Verifier
Start the service
Description:
Verifies potential file system corruptions.
Name
Description
Status
Startup Type
Log On As
Software Protection
Enables the download, in...
Automatic (Delaye...
Network Service
Special Administration Console Helper
Allows administrators to ...
Running
Manual
Local System
Spot Verifier
Verifies potential file syst...
Manual (Trigger St...
Local System
SSDP Discovery
Discovers networked devi...
Running
Manual
Local Service
State Repository Service
Provides required infrastr...
Running
Manual
Local System
Still Image Acquisition Events
Launches applications as...
Manual
Local System
Storage Service
Provides enabling service...
Manual (Trigger St...
Local System
Storage Tiers Management
Optimizes the placement...
Manual
Local System
Superfetch
Maintains and improves ...
Running
Automatic
Local System
Sync Host_3ed0e
This service synchronizes...
Running
Automatic (Delaye...
Local System
Sync Host_97068
This service synchronizes...
Running
Automatic (Delaye...
Local System
System Event Notification Service
Monitors system events a...
Running
Automatic
Local System
System Events Broker
Coordinates execution of...
Running
Automatic (Trigge...
Local System
Task Scheduler
Enables a user to configu...
Running
Automatic
Local System
TCP/IP NetBIOS Helper
Provides support for the ...
Running
Manual (Trigger St...
Local Service
Telephony
Provides Telephony API (...
Manual
Network Service
Themes
Provides user experience ...
Running
Automatic
Local System
Tile Data model server
Tile Server for tile updates.
Running
Automatic
Local System
Time Broker
Coordinates execution of...
Running
Manual (Trigger St...
Local Service
Touch Keyboard and Handwriting Panel Service
Enables Touch Keyboard ...
Manual (Trigger St...
Local System
Update Orchestrator Service for Windows Update
UsoSvc
Running
Manual
Local System
UPnP Device Host
Allows UPnP devices to b...
Manual
Local Service
User Access Logging Service
This service logs unique ...
Automatic (Delaye...
Local System
User Data Access_3ed0e
Provides apps access to s...
Manual
Local System
User Data Access_97068
Provides apps access to s...
Manual
Local System
User Data Storage_3ed0e
Handles storage of struct...
Manual
Local System
User Data Storage_97068
Handles storage of struct...
Manual
Local System
User Experience Virtualization Service
Provides support for appl...
Disabled
Local System
User Manager
User Manager provides t...
Running
Automatic (Trigge...
Local System
User Profile Service
This service is responsibl...
Running
Automatic
Local System
Virtual Disk
Provides management se...
Running
Manual
Local System
Volume Shadow Copy
Manages and implement...
Manual
Local System
W3C Logging Service
Provides W3C logging fo...
Manual
Local System
WalletService
Hosts objects used by cli...
Manual
Local System
Windows Audio
Manages audio for Wind...
Running
Automatic
Local Service
Windows Audio Endpoint Builder
Manages audio devices f...
Running
Manual
Local System
Windows Azure Guest Agent
The Windows Azure Gues...
Running
Automatic
Local System
Windows Azure Network Agent
Microsoft Azure VM Net...
Running
Automatic
Local System
Windows Biometric Service
The Windows biometric s...
Running
Automatic (Trigge...
Local System
Windows Camera Frame Server
Enables multiple clients t...
Manual (Trigger St...
Local Service
Windows Connection Manager
Makes automatic connec...
Running
Automatic (Trigge...
Local Service
Windows Defender Network Inspection Service
Helps guard against intru...
Running
Manual
Local Service
Windows Defender Service
Helps protect users from ...
Running
Automatic
Local System
Windows Driver Foundation - User-mode Driver Framework
Creates and manages use...
Running
Manual (Trigger St...
Local System
Windows Encryption Provider Host Service
Windows Encryption Pro...
Manual (Trigger St...
Local Service
Windows Error Reporting Service
Allows errors to be report...
Manual (Trigger St...
Local System
Windows Event Collector
This service manages per...
Manual
Network Service
Windows Event Log
This service manages eve...
Running
Automatic
Local Service
Windows Firewall
Windows Firewall helps p...
Running
Automatic
Local Service
Windows Font Cache Service
Optimizes performance o...
Running
Automatic
Local Service
Windows Image Acquisition (WIA)
Provides image acquisiti...
Manual
Local Service
Extended
Standard
1:49 PM
3/13/2023



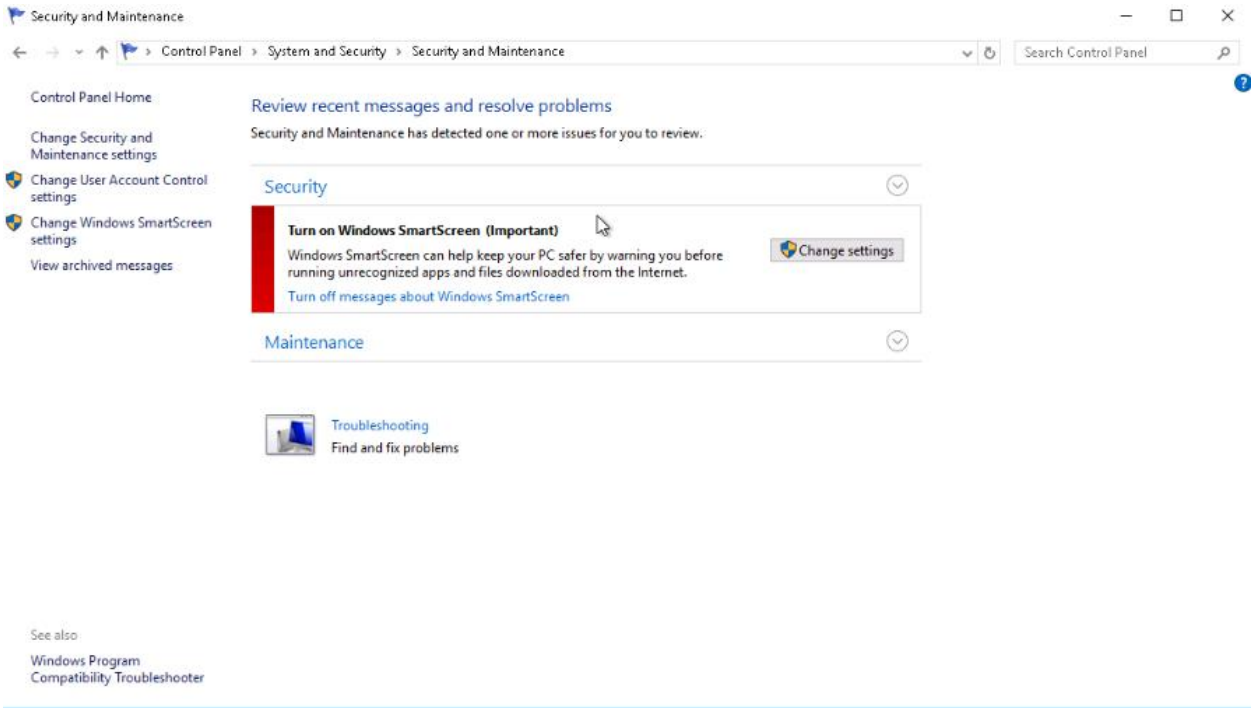
C. Other settings

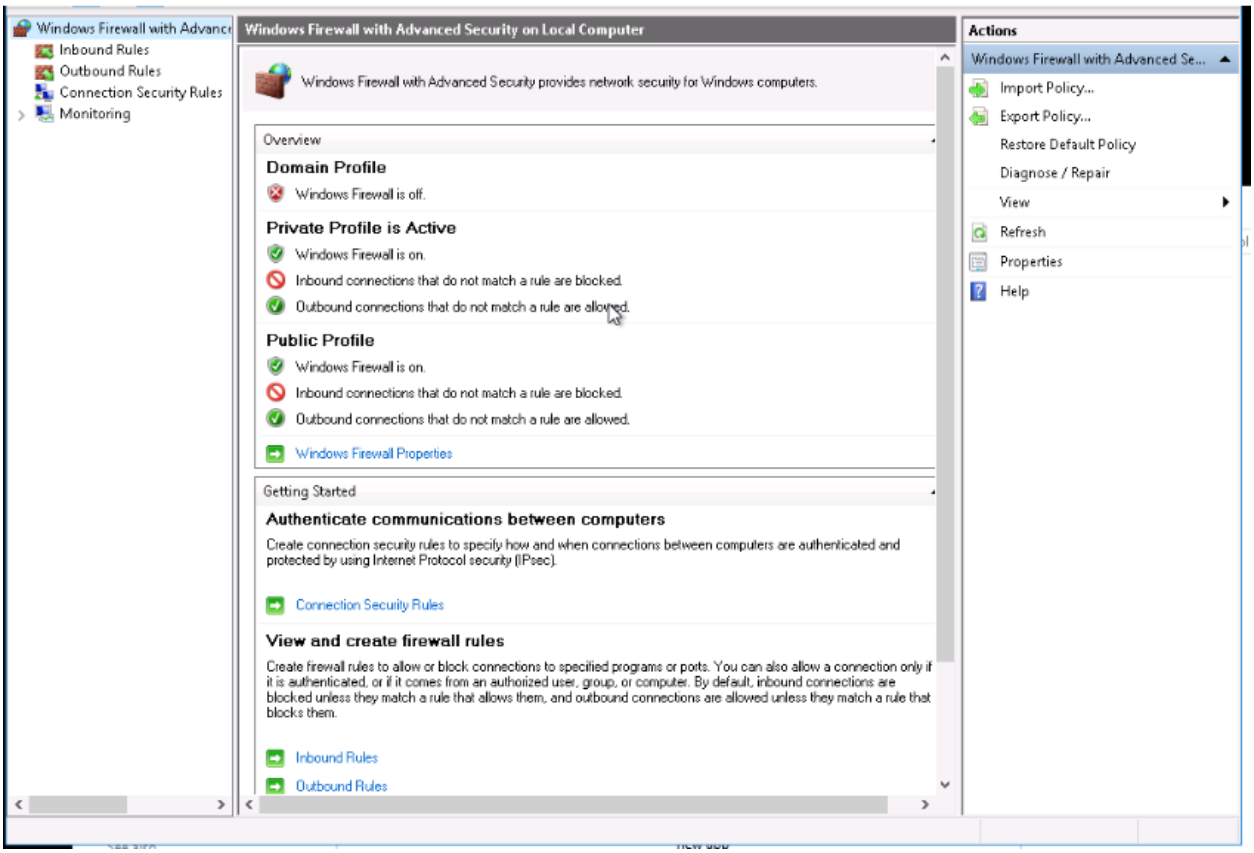
-On CP>System and Security > Security and Maintenance there is an notification classified as "Important" regarding Windows SmartScreen, which prevent running unrecognized apps from internet.

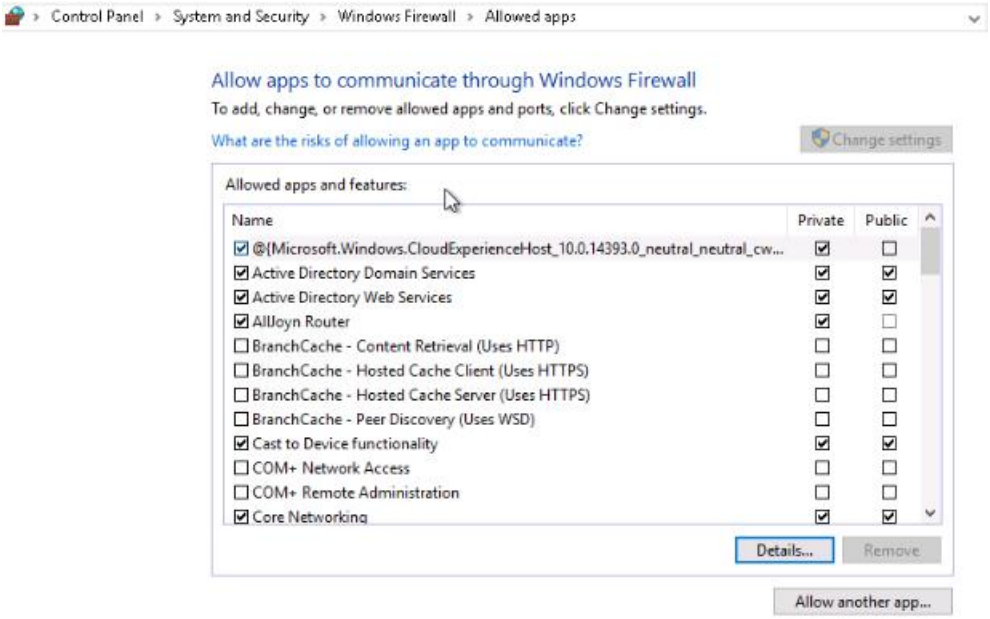
-On windows firewall, we have a notification that inform us that windows firewall is off.

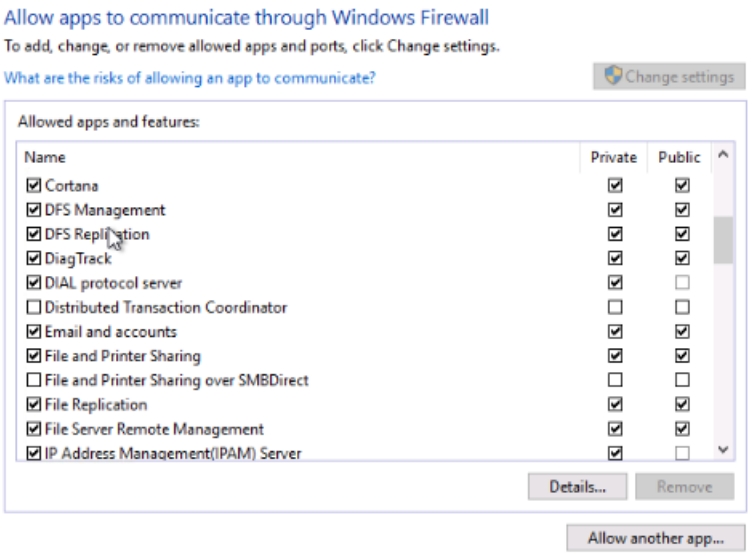
On windows firewall, the allowed apps and features that are allowed to pass through firewall, the "email and accounts" and "file and printer sharing" are set to pass by public network.

-bit Locker encryption is off on the "c" drive.


Security and Maintenance
Control Panel › System and Security › Security and Maintenance
Search Control Panel
Control Panel Home
Change Security and Maintenance settings
Change User Account Control settings
Change Windows SmartScreen settings
View archived messages
Review recent messages and resolve problems
Security and Maintenance has detected one or more issues for you to review.
Security
Turn on Windows SmartScreen (Important)
Windows SmartScreen can help keep your PC safer by warning you before running unrecognized apps and files downloaded from the Internet.
Change settings
Turn off messages about Windows SmartScreen
Maintenance
Troubleshooting
Find and fix problems
See also
Windows Program Compatibility Troubleshooter


Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is off.
Private Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.
Inbound Rules
Outbound Rules
Actions
Windows Firewall with Advanced Se...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help


Control Panel › System and Security › Windows Firewall › Allowed apps
Allow apps to communicate through Windows Firewall
To add, change, or remove allowed apps and ports, click Change settings.
What are the risks of allowing an app to communicate?
Change settings
Allowed apps and features:
Name
Private
Public
@{Microsoft.Windows.CloudExperienceHost_10.0.14393.0_neutral_neutral_cw...
Active Directory Domain Services
Active Directory Web Services
AllJoyn Router
BranchCache - Content Retrieval (Uses HTTP)
BranchCache - Hosted Cache Client (Uses HTTPS)
BranchCache - Hosted Cache Server (Uses HTTPS)
BranchCache - Peer Discovery (Uses WSD)
Cast to Device functionality
COM+ Network Access
COM+ Remote Administration
Core Networking
Details...
Remove
Allow another app...


Allow apps to communicate through Windows Firewall
To add, change, or remove allowed apps and ports, click Change settings.
What are the risks of allowing an app to communicate?
Change settings
Allowed apps and features:
Name
Private
Public
Cortana
DFS Management
DFS Replication
DiagTrack
DIAL protocol server
Distributed Transaction Coordinator
Email and accounts
File and Printer Sharing
File and Printer Sharing over SMBDirect
File Replication
File Server Remote Management
IP Address Management(IPAM) Server
Details...
Remove
Allow another app...

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

Name	Private	Public
☐ iSCSI Service	☐	☐
☑ Kerberos Key Distribution Center	☑	☑
☐ Key Management Service	☐	☐
☑ mDNS	☑	☑
☑ Microsoft Key Distribution Service	☑	☑
☐ Netlogon Service	☐	☐
☑ Network Discovery	☑	☐
☐ Performance Logs and Alerts	☐	☐
☑ Remote Desktop	☑	☑
☑ Remote Desktop Licensing Server	☑	☑
☑ Remote Desktop Services	☑	☑
☐ Remote Event Log Management	☐	☐

Details... Remove

Allow another app...

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

Name	Private	Public
☑ Remote Desktop Licensing Server	☑	☑
☑ Remote Desktop Services	☑	☑
☐ Remote Event Log Management	☐	☐
☐ Remote Event Monitor	☐	☐
☐ Remote Scheduled Tasks Management	☐	☐
☐ Remote Service Management	☐	☐
☐ Remote Shutdown	☐	☐
☐ Remote Volume Management	☐	☐
☐ Routing and Remote Access	☐	☐
☐ Secure Socket Tunneling Protocol	☐	☐
☑ Secure World Wide Web Services (HTTPS)	☑	☑
☑ SmartScreen	☑	☑

Details... Remove

Allow another app...

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

Name	Private	Public
☐ SNMP Trap	☐	☐
☐ Software Load Balancer	☐	☐
☐ TPM Virtual Smart Card Management	☐	☐
☐ Virtual Machine Monitoring	☐	☐
☑ Windows Communication Foundation	☑	☑
☑ Windows Default Lock Screen	☑	☑
☐ Windows Firewall Remote Management	☐	☐
☐ Windows Management Instrumentation (WMI)	☐	☐
☐ Windows Media Player	☐	☐
☑ Windows Remote Management	☑	☑
☐ Windows Remote Management (Compatibility)	☐	☐
☑ Windows Shell Experience	☑	☑

Details... Remove

Allow another app...

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

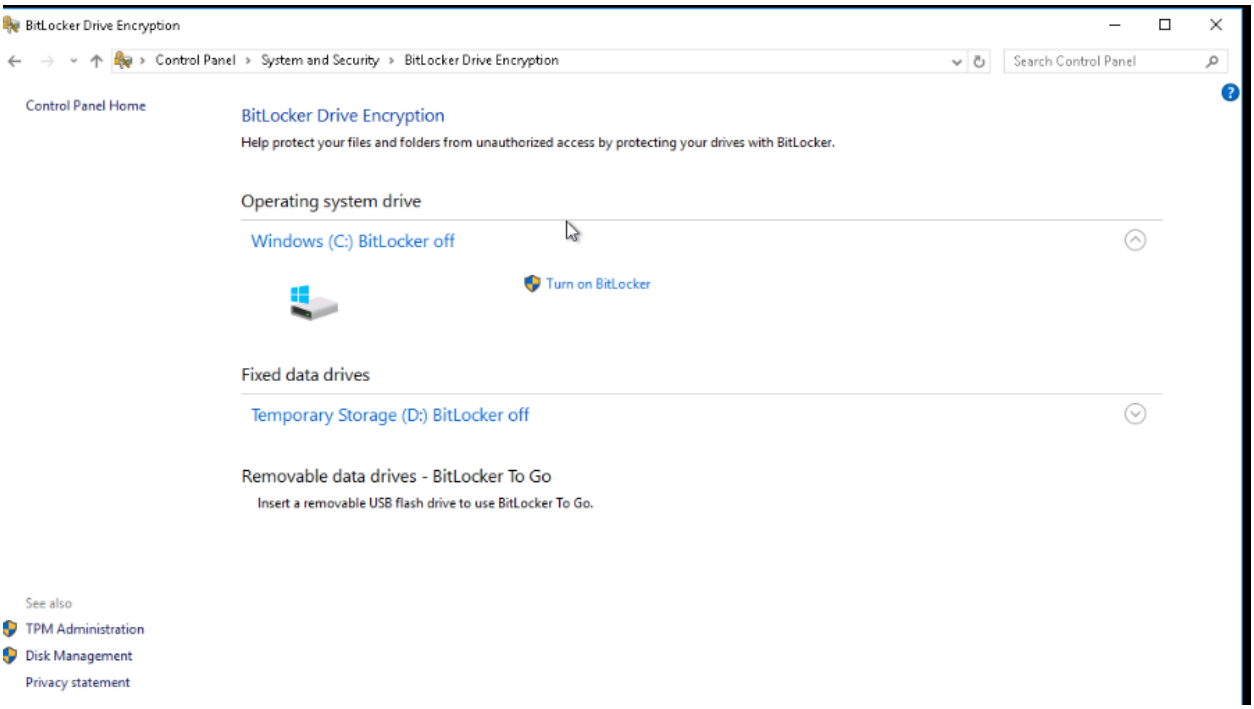
Change settings

Allowed apps and features:

Name	Private	Public
☐ Windows Management Instrumentation (WMI)	☐	☐
☐ Windows Media Player	☐	☐
☑ Windows Remote Management	☑	☑
☐ Windows Remote Management (Compatibility)	☐	☐
☑ Windows Shell Experience	☑	☑
☑ WMS Service	☑	☑
☑ WMS Session Agent	☑	☑
☑ Work or school account	☑	☑
☑ World Wide Web Services (HTTP)	☑	☑
☑ Xbox Game UI	☑	☑
☑ Your account	☑	☑

Details... Remove

Allow another app...



Tip: Do not miss the security permissions on the HR Directory.

The Users account have read modify access to HR folders, where are stored confidential datas, like salary, bank account of employees, etc.

3. **Firewall Rules:**

DFI does not have a dedicated networking department just yet, once again these tasks normally fall under the SysAdmin group. Now that we have you as a security professional, you'll take over the creation of our firewall rules. We recently entered into a new partnership and require new IP connections.
Using Cisco syntax, create the text of a firewall rule allowing a new DFI partner WBC International, access to DFI-File-001 access via port tcp-9082.

The partner's IP is 21.19.241.63, and DFI-File-001's IP is 172.21.30.44.

For this exercise, assume the two IP objects **have not** been created in the firewall. **Note*** Use *DFI-Ingress* as the interface for the rule. For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Place your firewall rules and explanation here.
Name the IP objects and provide the commands necessary to complete the firewall rule.]
Tip: The rule must be exact.

name 21.19.241.63 WBC-001

name 172.21.30.44 DFI-File-001

access-list *DFI-Ingress extended permit tcp host* wbc-001 *host* dfi-file-001 eq 9082

Access-list ->this is the rule that controls traffic

DFI-Ingress – the name of our internal interface

extended permit- gives additional flexibility in matching the traffic and the ability to match based on protocol, sources and destination address.

Tcp – protocol being used

21.19.241.63 – IP that will be allowed to access the server (wbs-001)

172.21.30.44 – Destination IP of the server.(dfi-file-001)

eq 9082 – means "equal to" and is the post required

To explain this syntax to non-technical management on the change control board, it can be described as follows:

This firewall rule is being created to allow a new DFI partner, WBC International, to access DFI-File-001 via port tcp-9082. We are specifying the source IP address of the partner (21.19.241.63) and the destination IP address of DFI-File-001 (172.21.30.44). This rule is being applied to the DFI-Ingress interface to ensure that traffic is properly routed. This rule is being added to the firewall configuration to enable secure access to DFI-File-001 by our new partner.

4. VPN Encryption Recommendation:

DFI is creating a payroll processing partnership with Payroll-USA; this will involve creating a VPN connection between the two. Research, recommend, and justify an encryption solution for the connection that is using the latest available encryption for Cisco. Use the Cisco documentation as a guide.

[Place your VPN Encryption Recommendation here]
Choose one of the appropriate encryption methods from the documentation provided. Provide justification for the method you chose.
Tip: Do not use those encryption methods whose status is marked either as "Avoid" or "Legacy" in the Cisco documentation.

Advanced Encryption Standard (AES) encryption algorithm. AES is recommended by Cisco for VPN connections.

To implement AES encryption, we would need to configure both the DFI and Payroll-USA VPN endpoints to use AES with a key length of 256 bits. This can be done by configuring the IPsec transform set on both endpoints to use AES-256 encryption.

crypto ipsec transform-set my-transform-set esp-aes 256 esp-sha-hmac

It's also important to ensure that the VPN tunnel is version 3 (IKEv3).

For a VPN connection, that requires an authentication process, this provides the best option. It is nor marked as avoid/Legacy. This encryption is necessary because of the payroll documents that contain personal, sensitive information about the bank accounts, IBAN's, employee name, employee social security number, etc.

5. **IDS Rule:**

The System Administrator gave you a heads up that DFI-File-001 with an IP address of 172.21.30.44 has been receiving a high volume of ICMP traffic and is concerned that a DDoS attack is imminent. She has requested an IDS rule for this specific server.

The VoIP Administrator is also concerned that an attacker is attempting to connect to her primary VoIP server, which resides at 172.21.30.55 via TFTP. She has requested an IDS rule for this traffic.

For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Place your System Admin rule and explanation here]

alert icmp any any -> 172.21.30.44 any (msg:"DDos Attack Attempt "; threshold: type both, track by_dst, count 100, seconds 10; sid:1000111;)

[Place your VoIP Admin rule and explanation here]

Alert udp any any -> 172.21.30.55 69 (msg: "VoIP Attack Attempt"; sid:1000222;)

For documentation purposes, provide and explain your commands to non-technical management.

Alert – generate an alert using the selected alert method, and then log the packet with the message we chose.

Icmp/udp – type of a protocol

Any (first) – IP address source

Any (second) – Port nr source.

172.21.30.44/172.21.30.55 – Destination IP address.

Any(third) – Any destination port of the specific IP.

(msg: "DDos Attack Attempt"; sid:1000111;) – Rule option with message "Ddos Attack Attempt"

(msg: "VoIP Attack Attempt"; sid:1000222;) - Rule option with message "VoIP Attack Attempt"

Threshold - type both, track by_dst, count 100, seconds 10;: This sets a threshold for the rule to avoid false positives. The rule will only trigger an alert if 100 or more ICMP packets are received targeting DFI-File-001 within a 10-second window.

Sid sid:1000111 sid:1000222: - number that identify the local snort rule.

Tip: Both the rules should be exact including the parenthesis and classtype. Also, the sid number needs to be 1000000 or higher and can't be the same for both rules.

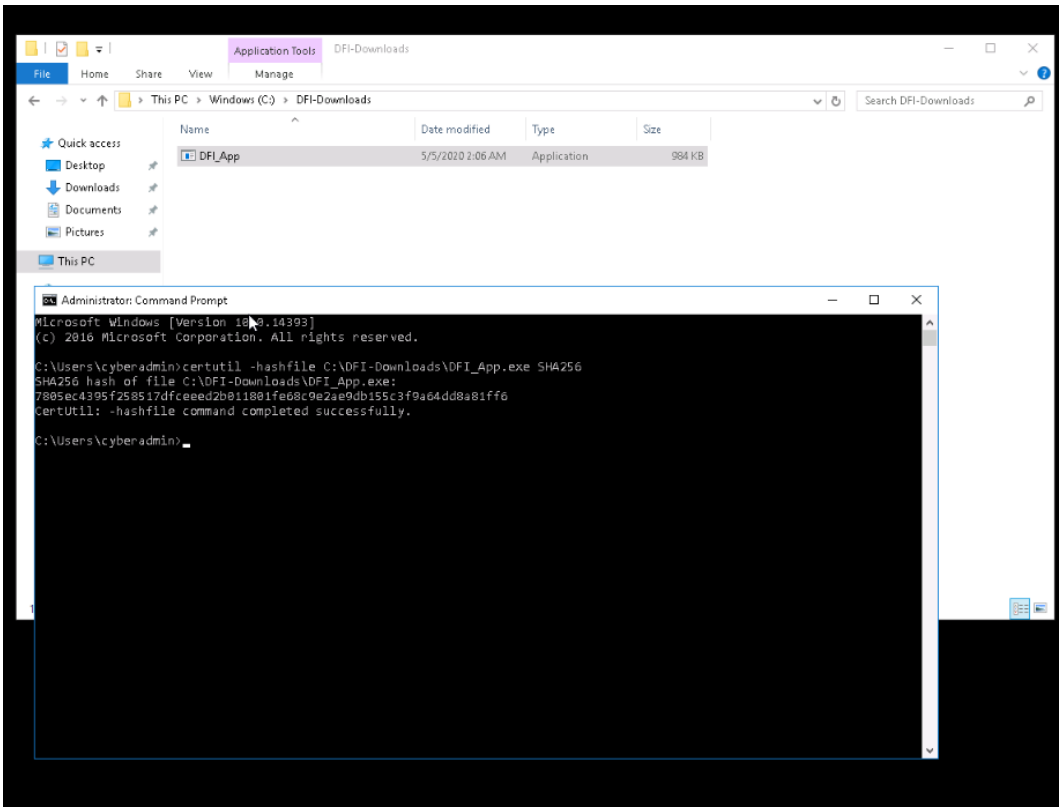
6. **File Hash verification:**

A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

Hash: 7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6

Perform a file hash verification and submit a screenshot of your command and output.
The File is stored on the Windows 2016 Server in C Drive under DFI-Download.

[Place your screenshot that displays the command that was run as well as the file hash.]



Week Two:

Now that you've performed a light audit and crafted Firewall and IDS Signatures we're ready for you to make some additional recommendations to tighten up our security.

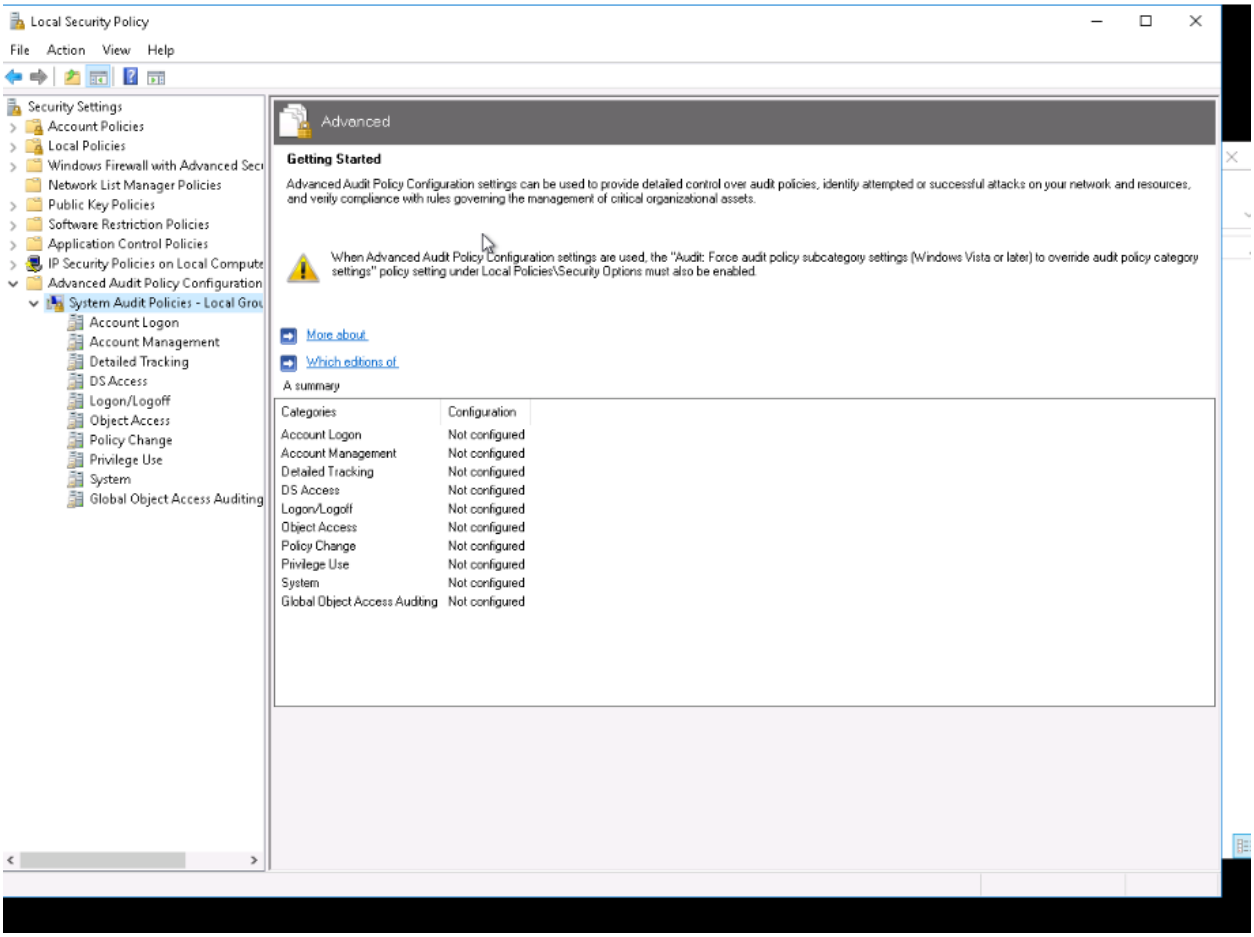
7. **Automation:**

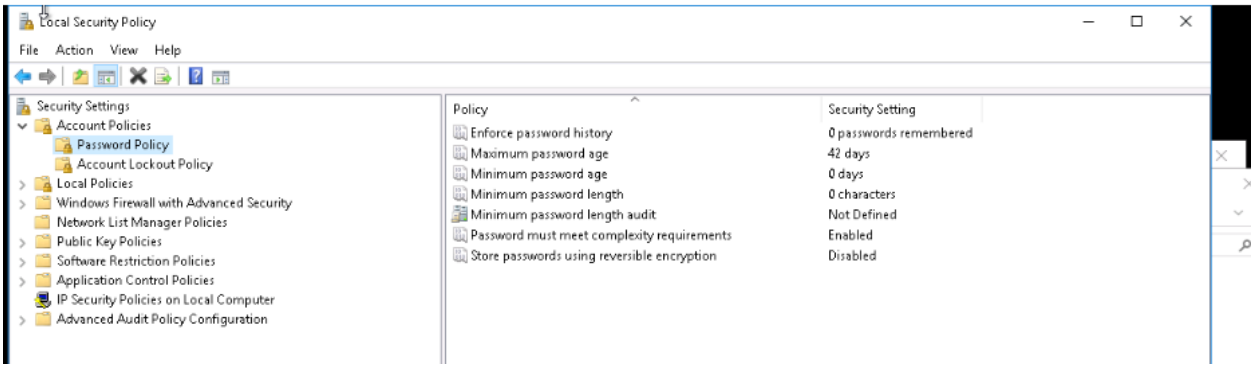
The IT Manager has tasked you with some introductory research on areas that could be improved via automation.

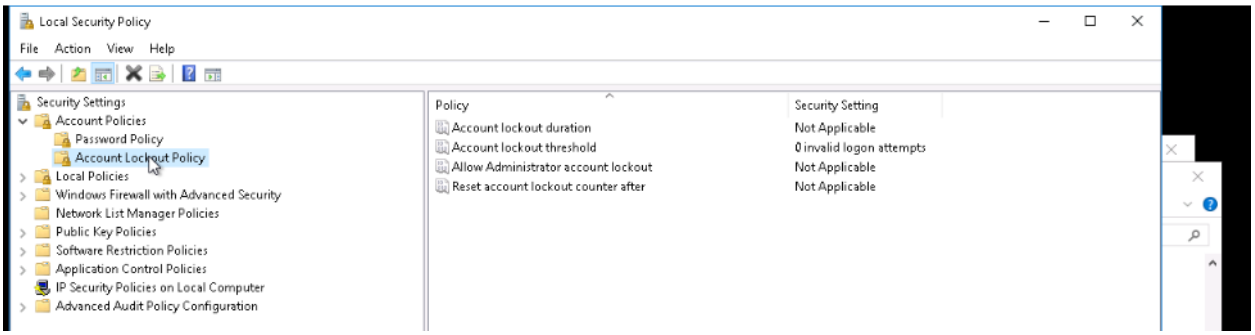
Research and recommend products, technologies and areas within DFI that could be improved via automation.

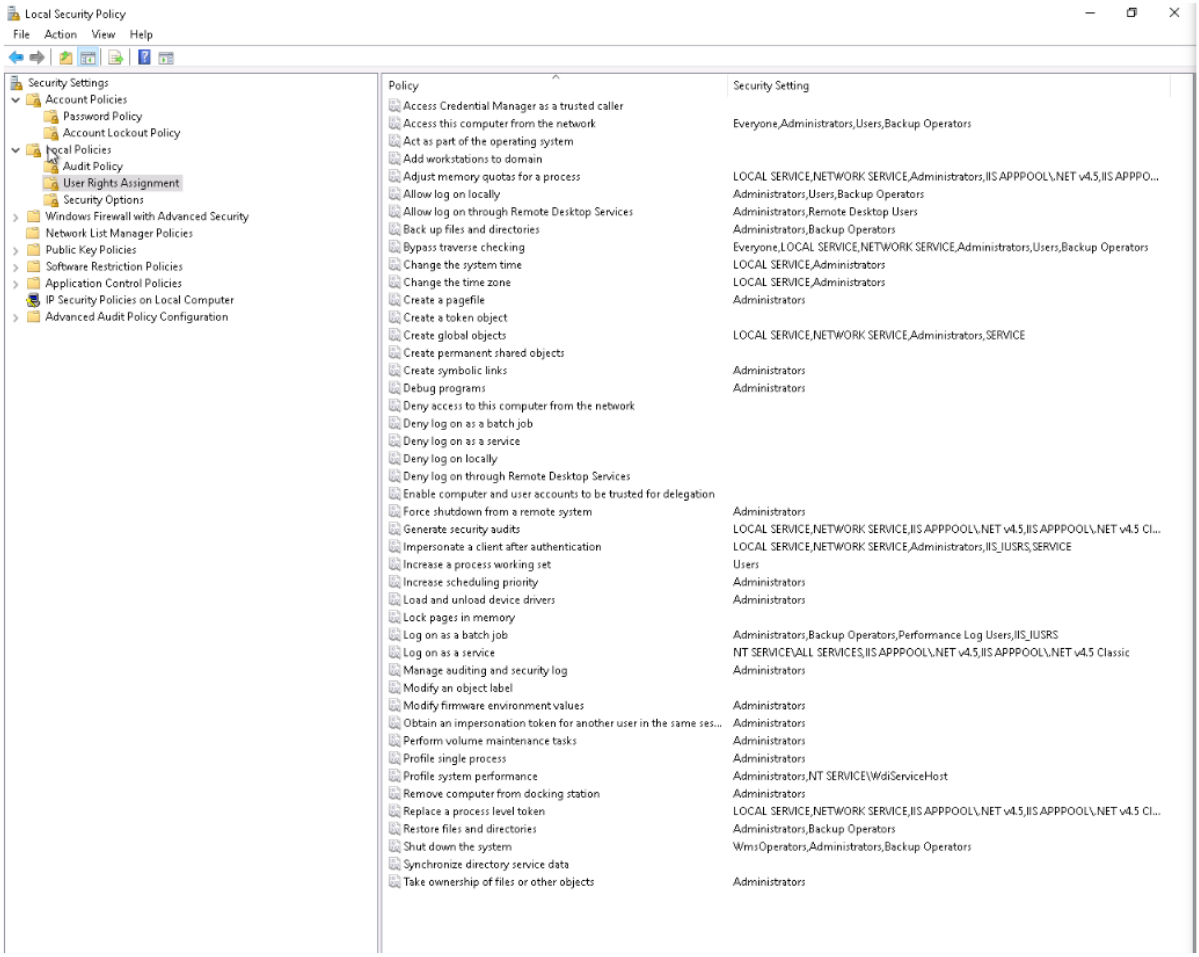
Recommended areas are:

- SOAR products and specifically what could be done with them
- Automation of mitigation actions for IDS and firewall alerts.
- Feel free to elaborate on other areas that could be improved.



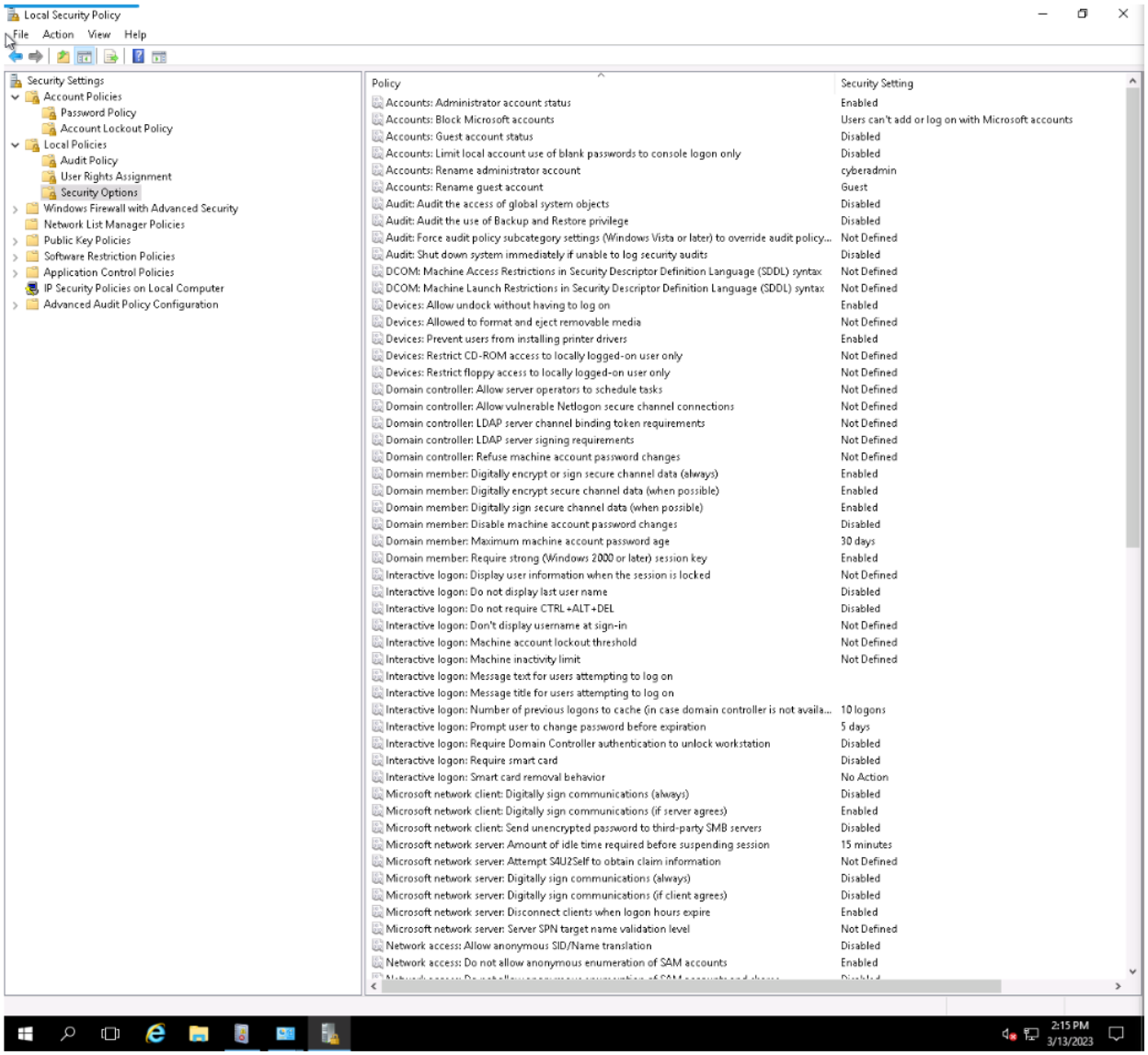


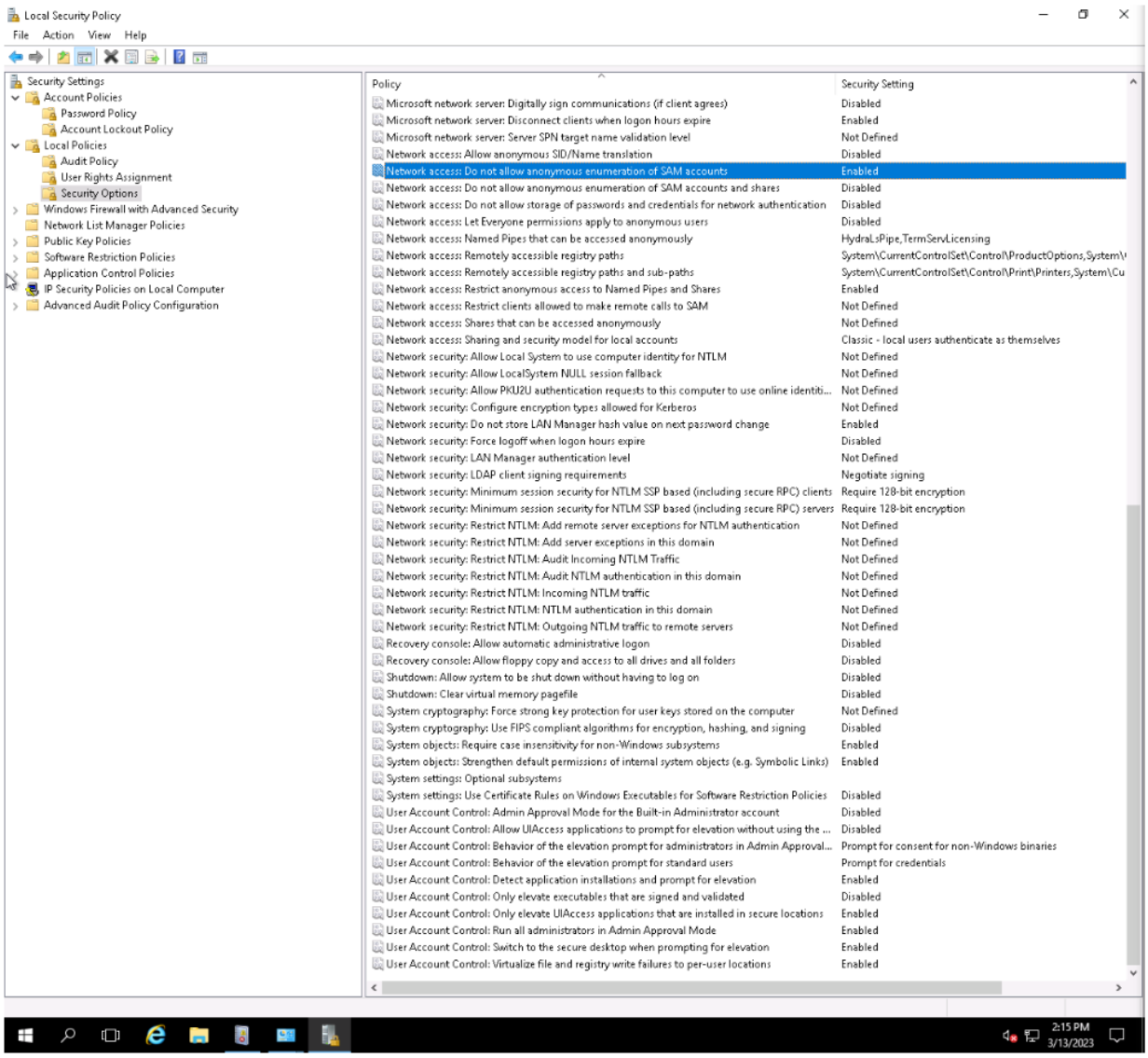




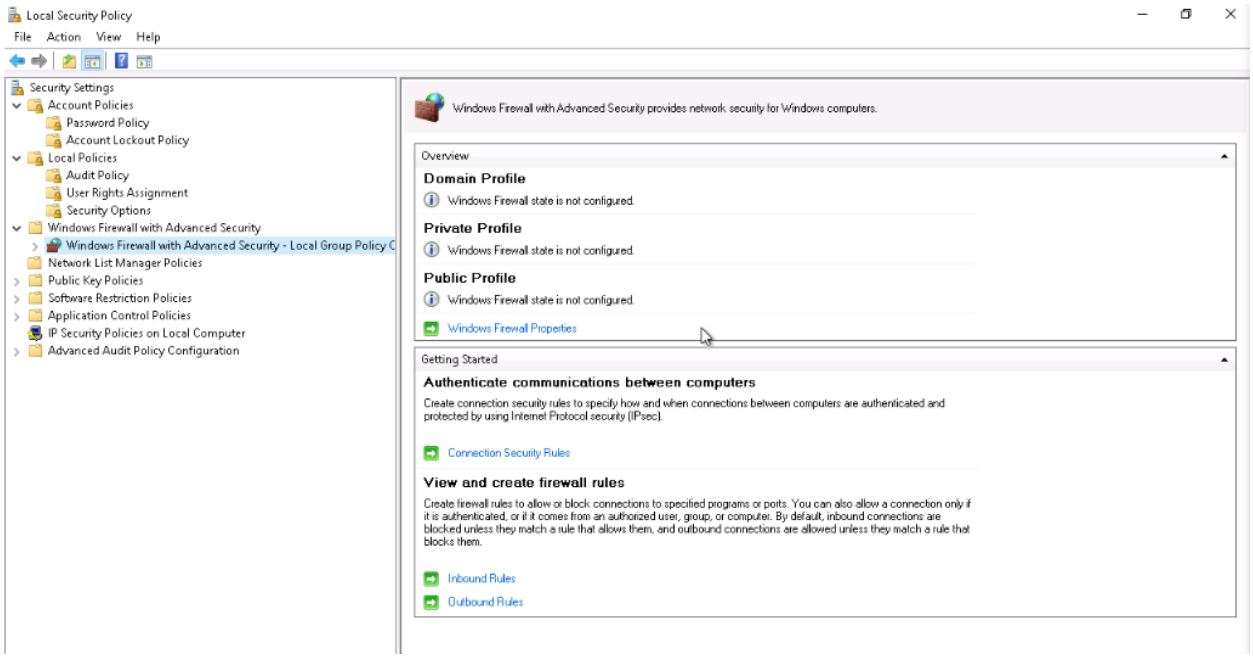
CYBERND0201

Security

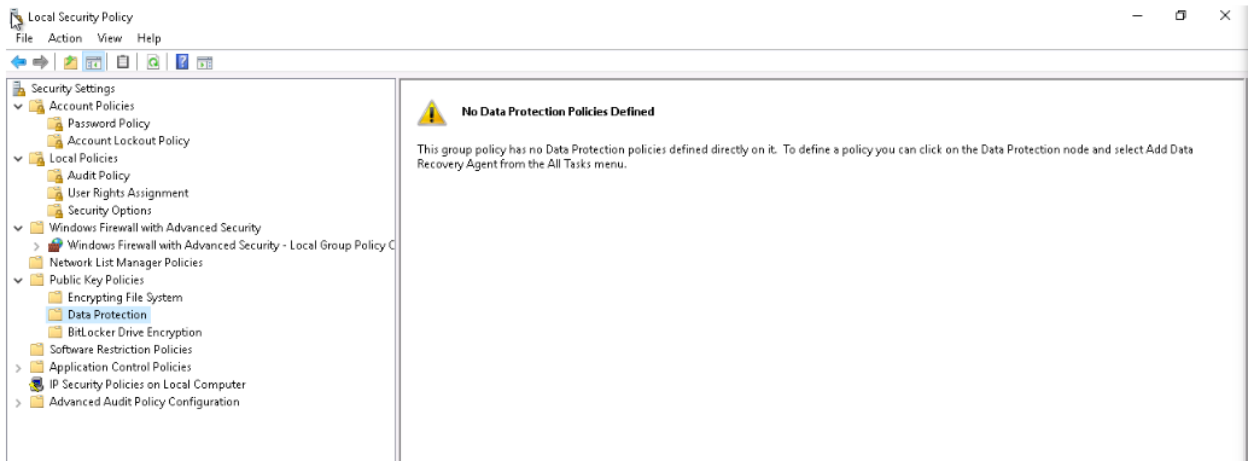

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Accounts: Administrator account status
Enabled
Accounts: Block Microsoft accounts
Users can't add or log on with Microsoft accounts
Accounts: Guest account status
Disabled
Accounts: Limit local account use of blank passwords to console logon only
Disabled
Accounts: Rename administrator account
cyberadmin
Accounts: Rename guest account
Guest
Audit: Audit the access of global system objects
Disabled
Audit: Audit the use of Backup and Restore privilege
Disabled
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy...
Not Defined
Audit: Shut down system immediately if unable to log security audits
Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
Not Defined
Devices: Allow undock without having to log on
Enabled
Devices: Allowed to format and eject removable media
Not Defined
Devices: Prevent users from installing printer drivers
Enabled
Devices: Restrict CD-ROM access to locally logged-on user only
Not Defined
Devices: Restrict floppy access to locally logged-on user only
Not Defined
Domain controller: Allow server operators to schedule tasks
Not Defined
Domain controller: Allow vulnerable Netlogon secure channel connections
Not Defined
Domain controller: LDAP server channel binding token requirements
Not Defined
Domain controller: LDAP server signing requirements
Not Defined
Domain controller: Refuse machine account password changes
Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)
Enabled
Domain member: Digitally encrypt secure channel data (when possible)
Enabled
Domain member: Digitally sign secure channel data (when possible)
Enabled
Domain member: Disable machine account password changes
Disabled
Domain member: Maximum machine account password age
30 days
Domain member: Require strong (Windows 2000 or later) session key
Enabled
Interactive logon: Display user information when the session is locked
Not Defined
Interactive logon: Do not display last user name
Disabled
Interactive logon: Do not require CTRL+ALT+DEL
Disabled
Interactive logon: Don't display username at sign-in
Not Defined
Interactive logon: Machine account lockout threshold
Not Defined
Interactive logon: Machine inactivity limit
Not Defined
Interactive logon: Message text for users attempting to log on
Interactive logon: Message title for users attempting to log on
Interactive logon: Number of previous logons to cache (in case domain controller is not availa...
10 logons
Interactive logon: Prompt user to change password before expiration
5 days
Interactive logon: Require Domain Controller authentication to unlock workstation
Disabled
Interactive logon: Require smart card
Disabled
Interactive logon: Smart card removal behavior
No Action
Microsoft network client: Digitally sign communications (always)
Disabled
Microsoft network client: Digitally sign communications (if server agrees)
Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers
Disabled
Microsoft network server: Amount of idle time required before suspending session
15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information
Not Defined
Microsoft network server: Digitally sign communications (always)
Disabled
Microsoft network server: Digitally sign communications (if client agrees)
Disabled
Microsoft network server: Disconnect clients when logon hours expire
Enabled
Microsoft network server: Server SPN target name validation level
Not Defined
Network access: Allow anonymous SID/Name translation
Disabled
Network access: Do not allow anonymous enumeration of SAM accounts
Enabled
2:15 PM
3/13/2023

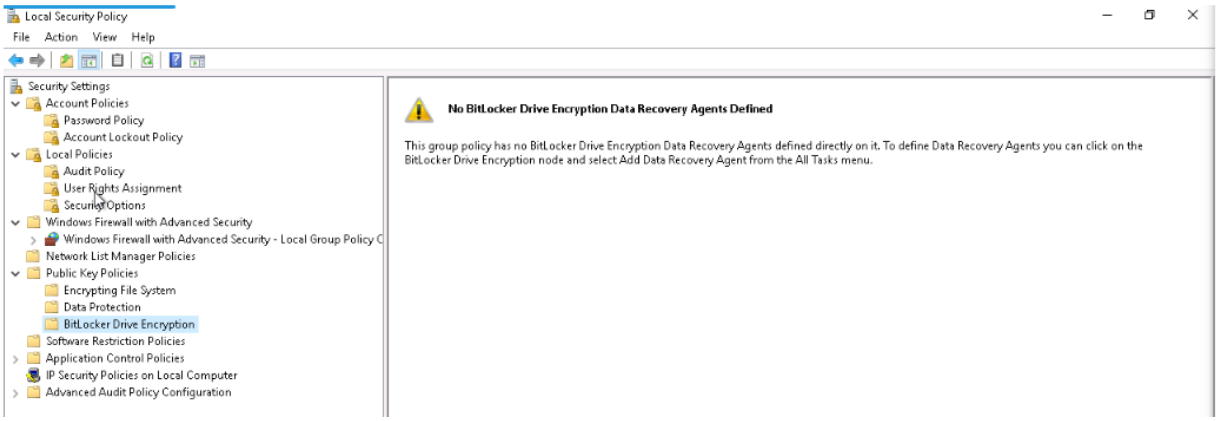

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Microsoft network server: Digitally sign communications (if client agrees) Disabled
Microsoft network server: Disconnect clients when logon hours expire Enabled
Microsoft network server: Server SPN target name validation level Not Defined
Network access: Allow anonymous SID/Name translation Disabled
Network access: Do not allow anonymous enumeration of SAM accounts Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares Disabled
Network access: Do not allow storage of passwords and credentials for network authentication Disabled
Network access: Let Everyone permissions apply to anonymous users Disabled
Network access: Named Pipes that can be accessed anonymously HydraLsPipe,TermServLicensing
Network access: Remotely accessible registry paths System\CurrentControlSet\Control\ProductOptions,System\
Network access: Remotely accessible registry paths and sub-paths System\CurrentControlSet\Control\Print\Printers,System\Cu
Network access: Restrict anonymous access to Named Pipes and Shares Enabled
Network access: Restrict clients allowed to make remote calls to SAM Not Defined
Network access: Shares that can be accessed anonymously Not Defined
Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves
Network security: Allow Local System to use computer identity for NTLM Not Defined
Network security: Allow LocalSystem NULL session fallback Not Defined
Network security: Allow PKU2U authentication requests to this computer to use online identiti... Not Defined
Network security: Configure encryption types allowed for Kerberos Not Defined
Network security: Do not store LAN Manager hash value on next password change Enabled
Network security: Force logoff when logon hours expire Disabled
Network security: LAN Manager authentication level Not Defined
Network security: LDAP client signing requirements Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers Require 128-bit encryption
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers Not Defined
Recovery console: Allow automatic administrative logon Disabled
Recovery console: Allow floppy copy and access to all drives and all folders Disabled
Shutdown: Allow system to be shut down without having to log on Disabled
Shutdown: Clear virtual memory pagefile Disabled
System cryptography: Force strong key protection for user keys stored on the computer Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing Disabled
System objects: Require case insensitivity for non-Windows subsystems Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) Enabled
System settings: Optional subsystems
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the ... Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval... Prompt for consent for non-Windows binaries
User Account Control: Behavior of the elevation prompt for standard users Prompt for credentials
User Account Control: Detect application installations and prompt for elevation Enabled
User Account Control: Only elevate executables that are signed and validated Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations Enabled
User Account Control: Run all administrators in Admin Approval Mode Enabled
User Account Control: Switch to the secure desktop when prompting for elevation Enabled
User Account Control: Virtualize file and registry write failures to per-user locations Enabled
2:15 PM
3/13/2023

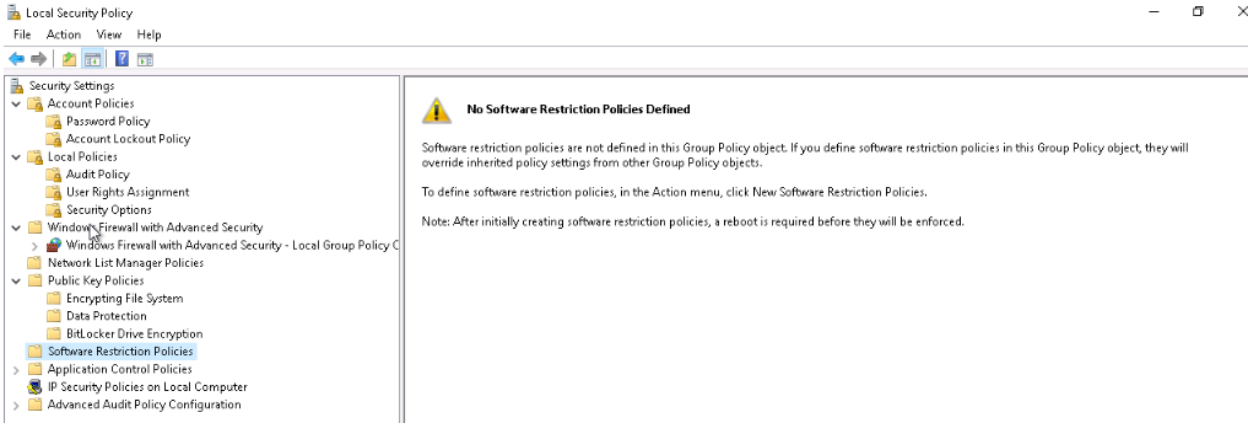
Firewall

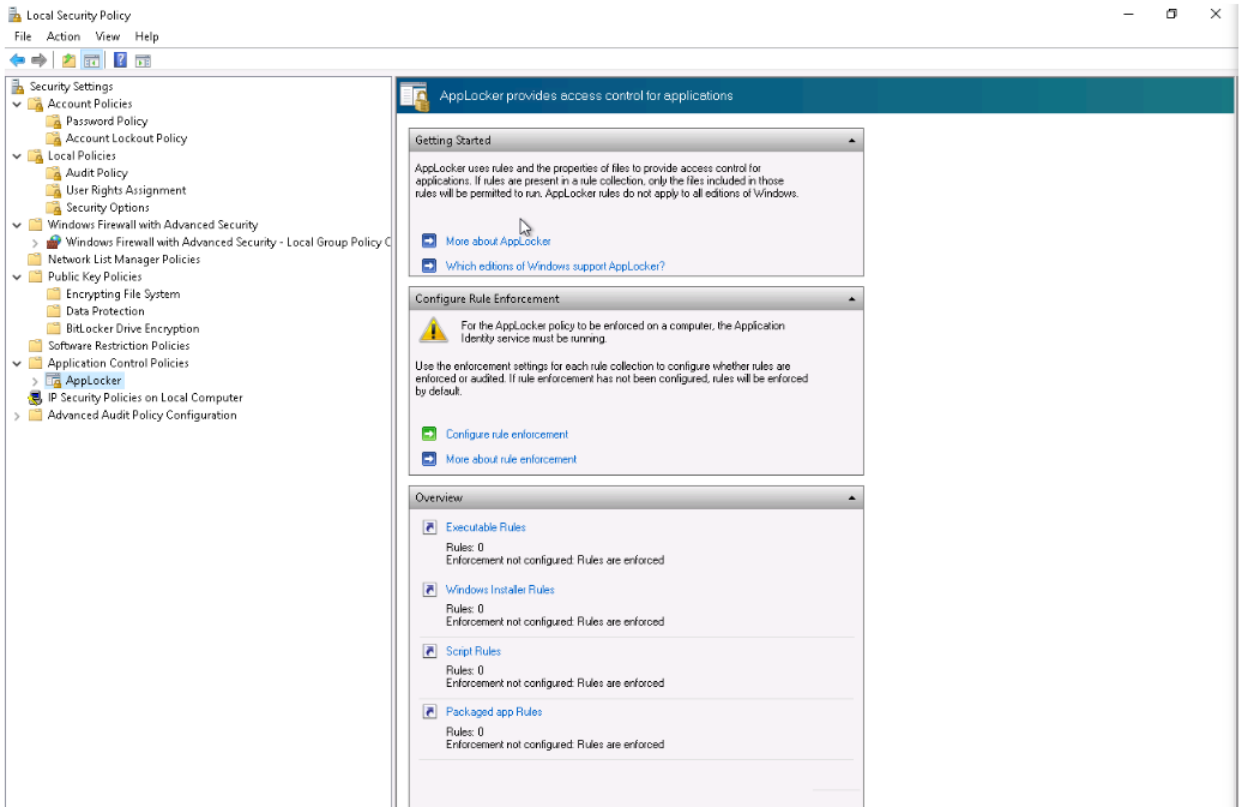

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - Local Group Policy C
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall state is not configured.
Private Profile
Windows Firewall state is not configured.
Public Profile
Windows Firewall state is not configured.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.
Inbound Rules
Outbound Rules


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - Local Group Policy C
Network List Manager Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
No Encrypting File System Policies Defined
This group policy has no Encrypting File System policies defined directly on it. To define a policy you can click on the Encrypting File System node and select Add Data Recovery Agent from the All Tasks menu.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - Local Group Policy C
Network List Manager Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
No Data Protection Policies Defined
This group policy has no Data Protection policies defined directly on it. To define a policy you can click on the Data Protection node and select Add Data Recovery Agent from the All Tasks menu.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - Local Group Policy C
Network List Manager Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
No BitLocker Drive Encryption Data Recovery Agents Defined
This group policy has no BitLocker Drive Encryption Data Recovery Agents defined directly on it. To define Data Recovery Agents you can click on the BitLocker Drive Encryption node and select Add Data Recovery Agent from the All Tasks menu.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - Local Group Policy C
Network List Manager Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
No Software Restriction Policies Defined
Software restriction policies are not defined in this Group Policy object. If you define software restriction policies in this Group Policy object, they will override inherited policy settings from other Group Policy objects.
To define software restriction policies, in the Action menu, click New Software Restriction Policies.
Note: After initially creating software restriction policies, a reboot is required before they will be enforced.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - Local Group Policy C
Network List Manager Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
Software Restriction Policies
Application Control Policies
AppLocker
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
AppLocker provides access control for applications
Getting Started
AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.
More about AppLocker
Which editions of Windows support AppLocker?
Configure Rule Enforcement
For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.
Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.
Configure rule enforcement
More about rule enforcement
Overview
Executable Rules
Rules: 0
Enforcement not configured: Rules are enforced
Windows Installer Rules
Rules: 0
Enforcement not configured: Rules are enforced
Script Rules
Rules: 0
Enforcement not configured: Rules are enforced
Packaged app Rules
Rules: 0
Enforcement not configured: Rules are enforced

Complete the chart below, including the area/technology within DFI and a proposed solution, with a minimum of 3 areas. Example:

- Area: Active Directory.
- Solution: The item for automation - Automatic account lockout if login from 2 geographically distant IPs
- Justification: Provide a brief explanation for your choices.

DFI Area/Technology	Solution	Justification for Recommendation
Network Security(Automated Firewall Configuration Management)	**Tufin SecureTrack**	Part of the Tufin Orchestration Suite, SecureTrack offers real-time insight into firewall and security changes. Not only that, but it provides alerts for potential security risks and keeps you up-to-date on the state of your network. What's also remarkable about SecureTrack is that it lets you keep track of security policy changes and violations, which is really nice in enterprise settings. SecureTrack also lets you generate automated audit reports that are compliant with GDPR, SOX, PCI-DSS, NERC-CIP, HIPAA, and not only. SecureTrack also lets you control all your firewall rules across the entire network from a single location. Thanks to the advanced troubleshooting, path analysis, and topology modeling features, SecureTrack lets you quickly fix issues and deploy changes in the network too.

		All in all, Tufin SecureTrack is an excellent choice for large-scale and multi-vendor enterprise networks. It integrates seamlessly with technologies from various manufacturers, and it lets you control and monitor everything from a single location.
Endpoint Security(Automated Endpoint Protection)	CrowdStrike Falcon	Prevents all kinds of Attacks It prevents both basic and sophisticated attacks, whether they use malware or not, or whether their endpoints are connected to the network or not. U Accelerated Identification It proactively identifies advanced threat activities with unprecedented speed and effectiveness. Real-time visibility Provides complete visibility into running endpoints, applications, and processes so you can view and analyze both current and historical activity in seconds. Nothing is overlooked. Multiplatform CrowdStrike Falcon is tailored to protect all major platforms: Windows, OS X, Linux, data center servers, virtual systems, and cloud platforms like AWS, Azure, and Google. Threat Hunting Provides an additional layer of

		monitoring and analysis to detect any threats. This service is made up of a team of cybersecurity experts specialized in proactive threat search that hunt, investigate, and advise on the threat activity in the environment.
Data Protection(Automated Data Backup and Recovery)	**Rubrik**	Rubrik is cloud data management and enterprise backup software provided by Palo Alto-based Rubrik, Inc. It is a software platform that provides backup, instant recovery, archival, search, analytics, compliance, and copy data management in one secure fabric across data centers and clouds. Its software is also designed to be vendor-agnostic, and supports the most commonly used operating systems, databases, hypervisors, clouds, and SaaS applications. And while you can utilize Rubrik's software completely on the cloud, Rubrik also integrates with on-premises hardware, and even provides their own proprietary Rubrik appliances. Key Features Policy-driven Rubrik functions through a single policy engine that orchestrates service level agreements (SLAs) across the data lifecycle. Management is automated across hybrid and multi-cloud environments with

		one programmatic interface. Analytics & Reporting Rubrik's software creates customized reports and data visualizations for user's platforms on operational efficiency, compliance, and capacity utilization. Security & Compliance Data stored and backed up through Rubrik is secured in-transit and at-rest throughout its lifecycle, regardless of location. Rubrik delivers granular role-based access control while automating compliance reporting to complete various industry and internal audits. Users can quickly recover from ransomware through immutable backups native to the platform.

8. **Logging RDP Attempts:**

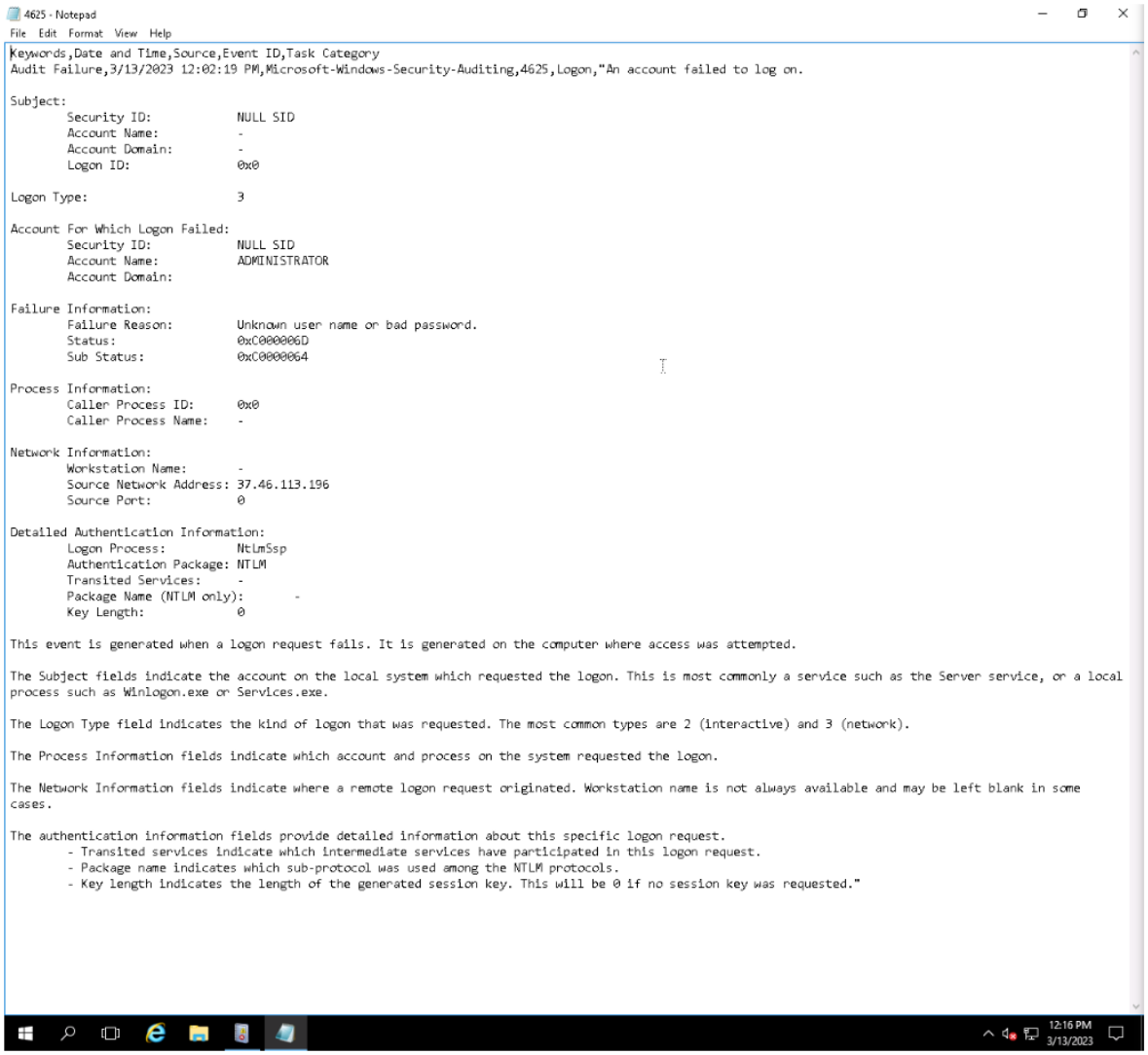
The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

Prepare a report that lists unsuccessful attempts in connecting over the last 24-hours. Using Powershell or Eventviewer, search the Windows Security Log for Event 4625. Export to CSV.

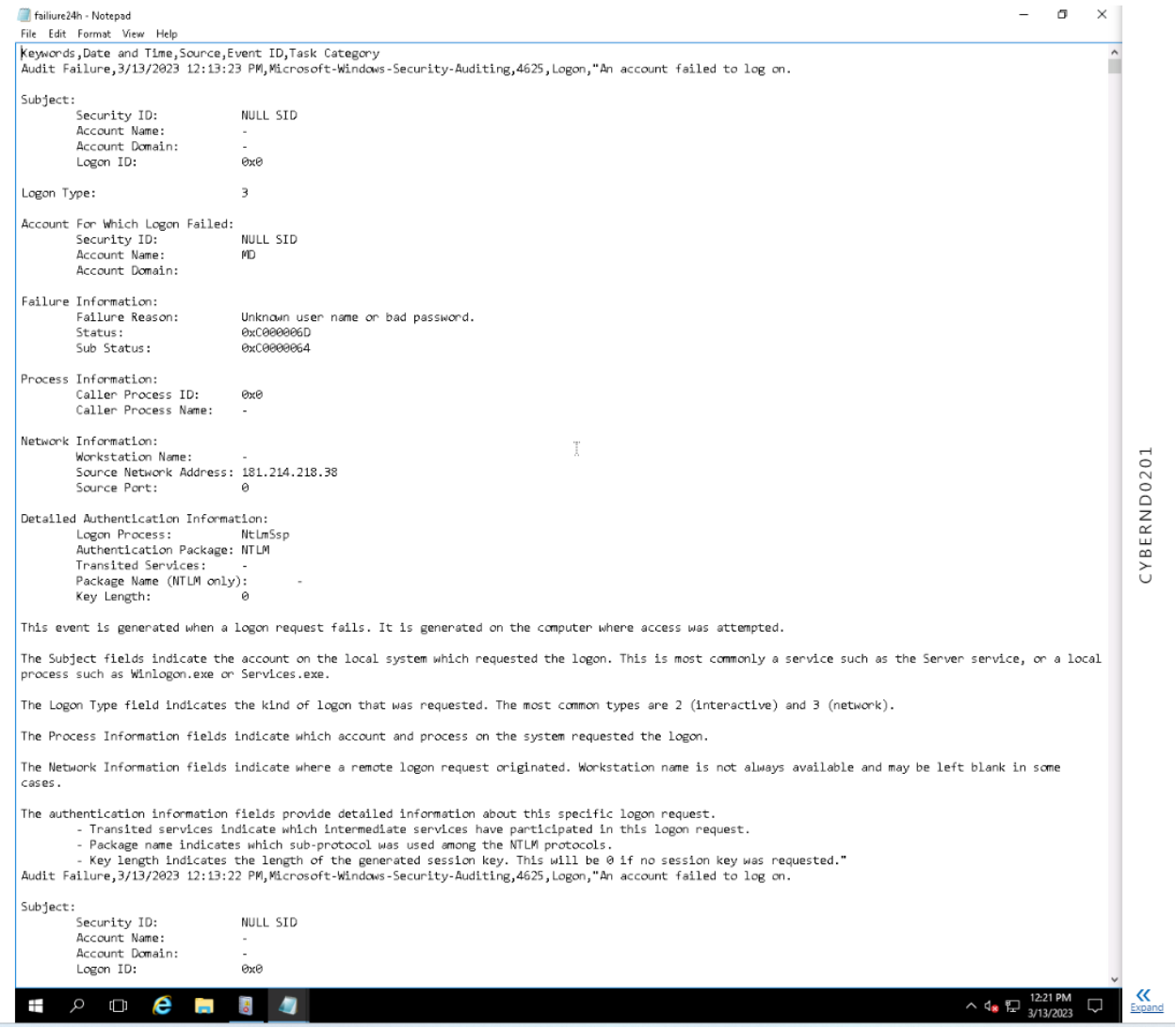
For your deliverable, open the CSV with a notepad and take a screenshot from your personal computer for your explanation. Please also include this file in your submission. Then in your report below, explain your findings, recommendations, and justifications to the IT Manager.

[Place IT Manager Report Here]

- Export the results to CSV on the server provided.
- Open the CSV with notepad. It must have the Event 4625 present.
- Provide a screenshot of the results



Cloud Lab - CYBERND0201 - Windows Server 2016



9. **Windows Updates:**

Using NIST 800-40r3 and Microsoft Security Update Guide, analyze the windows servers and provide your answers in the table below of available updates (KB and CVE) that should be installed as well as any updates that can be safely ignored for DFI's purpose. To assist, be aware that DFI is concerned with stability and security, any update that is not labeled as 'critical' or 'security' can be left off.

Provide a table that lists at least 3 updates that should be installed and 3 updates that are not necessary. Justify your recommendations as to why you are making your choices.

Tip: The severity of the updates can also help you decide the updates you'd like to install or ignore.

Add as many rows or additional columns as you need to the table.

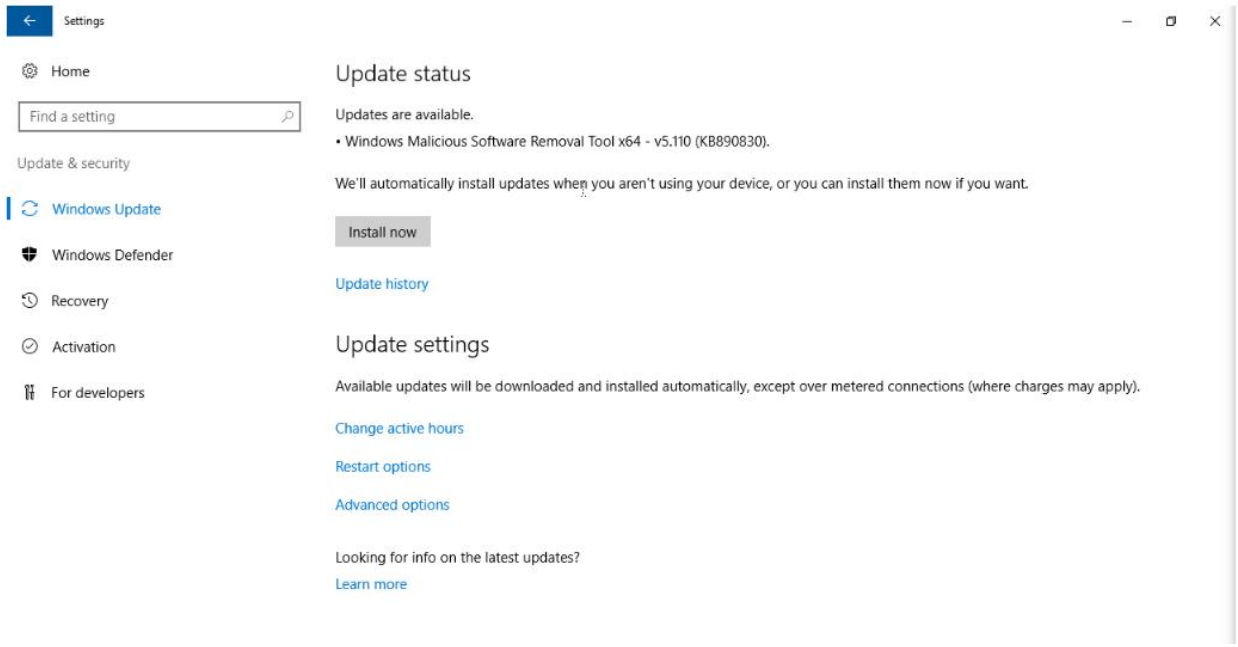
Taking into account the DFI request and concern for stability and security, those updates are regarded with priority that fulfill those requirements.

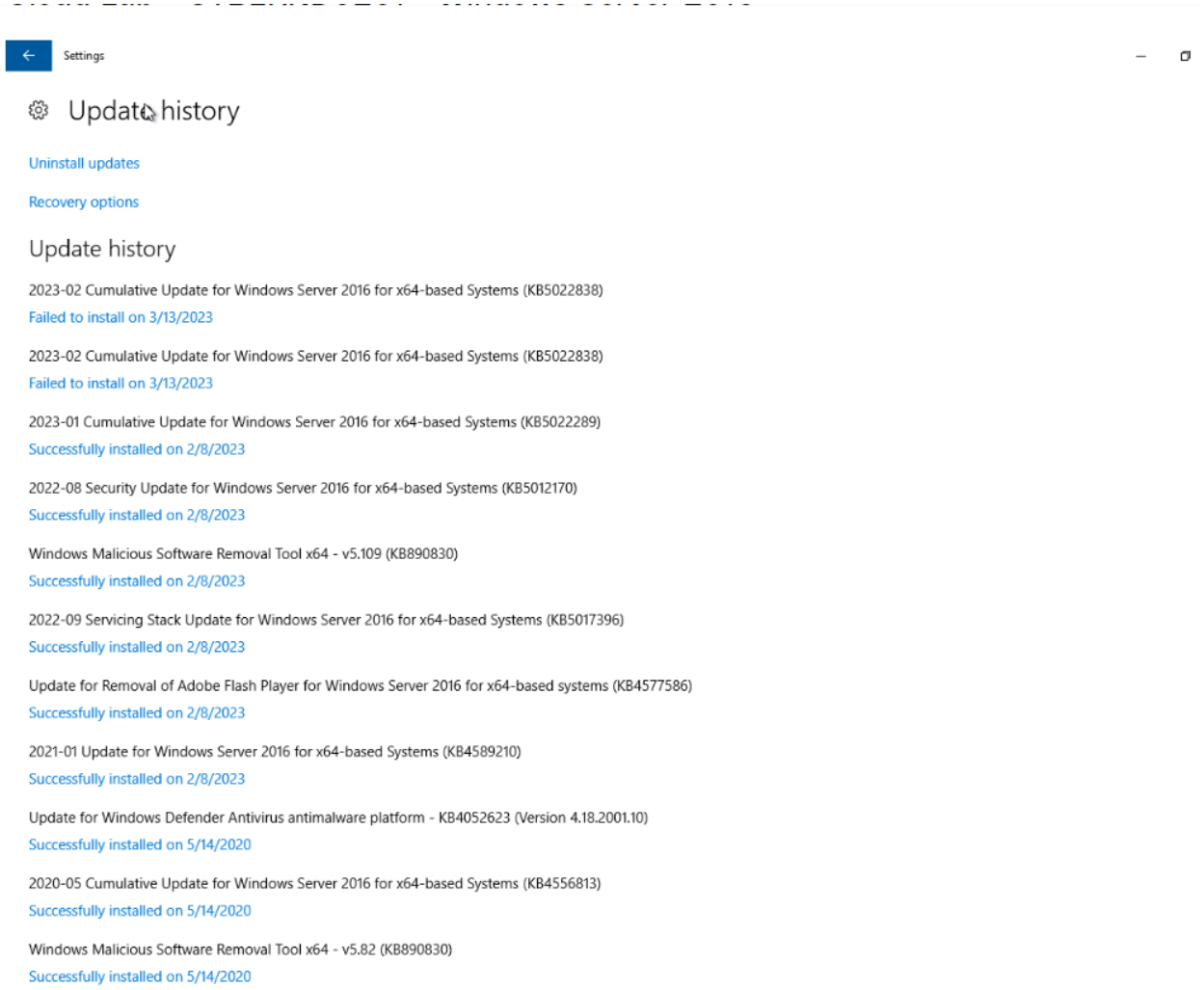
Available Updates	Update/Ignore	Justification
KB890830	Update	(MSRT) helps **remove malware from computers** running Windows Server 2016,
Kb5017396	Update	This update makes quality improvements to the servicing stack, which is the component that installs **Windows updates.** Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates
Kb4577586 Update for the removal of Adobe Flash Player	Ignore	This update **removes Adobe Flash Player** that is installed on any of the Windows operating systems that are listed in the "Applies to" section. After you apply this update, it cannot be uninstalled.
KB5022838	Update	This security update includes quality improvements. When you install this KB: This update addresses an issue that puts domain controllers (DC) in a restart loop. This occurs because the Local Security Authority Subsystem Service (LSASS) stops responding. The error is 0xc0000374. LSASS stops responding if you populate KrbTGT with the AltsecID on accounts that read-write and read-only DCs use. This update addresses an issue

		that affects AppV. It stops file names from having the correct letter case (uppercase or lowercase). This update addresses an issue that affects certain Internet of Things (IoT) devices. They lose audio. This update addresses an issue that affects searchindexer.exe. It randomly stops you from signing in or signing out.
KB5022289	Ignore	This security update includes quality improvements. When you install this KB: New! This update provides the Quick Assist application for your client device. This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain. This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails. The error message is, "There was an error resetting the AD password... // 0x80070005". This update introduces a Group Policy that enables and disables HTML Application (HTA) files. If you enable this policy, it stops

		you from running HTA files. If you disable or do not configure this policy, you can run HTA file. This update addresses a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.
KB4556813	Ignore	Highlights Updates to improve security when using Internet Explorer and Microsoft Edge. Updates to improve security when using input devices such as a mouse, keyboard, or stylus. Updates to improve security when Windows performs basic operations. Updates for storing and managing files. Improvements and fixes This security update includes quality improvements. Key changes include: Updates the 2020 start date for daylight saving time (DST) in the Kingdom of Morocco. Security updates to Internet Explorer, the Microsoft Scripting Engine, Windows App Platform

		and Frameworks, Windows Input and Composition, Windows Media, Windows Shell, Microsoft Edge, Windows Fundamentals, Windows Kernel, Windows Core Networking, Internet Information Services, Windows Network Security and Containers, Windows Active Directory, Windows Storage and Filesystems, and the Microsoft JET Database Engine.
KB5017396/Servicing stack update for Windows 10, version 1607 and Server 2016: September 13, 2022	Update	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.





10. **Linux Data Directories:**

The IT Manager has requested your help with creating directories on the CentOS server DFI-App-001 (reachable by ssh from the Windows 10 machine. in the DFI subnet.)

- The root directory should be 'Home'
- The first subdirectory should be "Departments" with subdirectories: HR, Accounting, Public, IT and Operations.
- Set owner permissions for the groups IT, HR, Operations and Accounting
- Create the users AmyIT, PamOps, MandyAcct and TimHR in the appropriate groups so that they can read/write/execute in their respective departmental folders.

For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Provide a screenshot(s) of completed tasks and the correctly set permissions here]
[Provide your non-technical syntax explanation for management here]

- Create the directories listed in the request.
- Create the groups listed in the request.
- Create the users listed and place them in the appropriate groups.
- Set the directory permissions where the groups are the owners of their respective directories. Tip: Appropriate groups should be the owners of the respective directories.
- Explain the syntax used for setting the permissions.

To fulfill the IT Manager's request, we need to perform the following steps:

Create the 'Home' directory:
mkdir /Home

Create the 'Departments' directory and its subdirectories:
mkdir /Home/Departments
mkdir /Home/Departments/HR
mkdir /Home/Departments/Accounting
mkdir /Home/Departments/Public
mkdir /Home/Departments/IT
mkdir /Home/Departments/Operations

Create the groups and users:
groupadd IT
groupadd HR
groupadd Operations
groupadd Accounting

useradd -G IT AmyIT
useradd -G Operations PamOps
useradd -G Accounting MandyAcct
useradd -G HR TimHR

Set directory permissions for the groups:
chown -R root:IT /Home/Departments/IT
chmod -R 770 /Home/Departments/IT

chown -R root:HR /Home/Departments/HR
chmod -R 770 /Home/Departments/HR

chown -R root:Operations /Home/Departments/Operations
chmod -R 770 /Home/Departments/Operations

chown -R root:Accounting /Home/Departments/Accounting
chmod -R 770 /Home/Departments/Accounting

The syntax used to set the permissions is as follows:

1. **mkdir**: create directories in the specified path.
2. **groupadd**: create a new group.
3. **useradd**: create a new user.
4. **chown**: change the owner and group ownership of files and directories.
5. **chmod**: change the permissions of files and directories.

-R perform the operation recursively for all files and subdirectories within the specified directory.
chown sets the owner and group,
chmod command sets the permissions to read (4), write (2), and execute (1) for the owner, group, and others (770).

11. **Firewall Alert Response:**

The IT Manager took a look at firewall alerts and was concerned with some traffic she saw, please take a look and provide a mitigation response to the below firewall report. Remember to justify your mitigation strategy.
This file is available from the project resources title: **DFI_FW_Report.xlsx**. Please download and use this file to complete this task.

[Firewall mitigation response and justification goes here]
Provide mitigation recommendations based on your analysis of the report with a focus on friend/foe of the source IP as well as an additional layer of protection for the destination IP.

The firewall report shows that there is an ongoing SSH User Authentication Brute Force Attack from several source IP addresses to a single destination IP address. This type of attack is commonly used by cybercriminals access a system by systematically trying different username and password to login.

1. For IP's (213.91.162.133, 139.199.170.238, 198.12.32.123) that the Repeat count is on the higher end it must be added to the block list. Automatically blocking malicious IP addresses when an IDS or firewall alert detects a malicious IP address at the network perimeter, reducing the risk of an attack. The reason for this choice is that the this IP's remains the same so it is easy to block them. This is also the NIST Publication800-41 recommendations, to always block an IP address that tries to attack an organization.

2. Change the SSH Port: Changing the default SSH port from port 22 to another port make's it difficult for hackers to find the correct port to gain access. This can be done by modifying the configuration file of the SSH service.
3. Implement Rate Limiting: Rate limiting can be implemented to restrict the number of authentication attempts per minute per IP address. This can slow down the attackers' ability to launch a successful attack
4. Continue the monitor and analyze of the logs on a regular basis, this will make it to find IP's that are have an increased nr of attempts and block them.

Tips: Edge case - Think about what should you do with IPs from non-trusted source.

1. With all IP from non-trusted an firewall analyzer must be set in place, and a risk rule must be created, using a software from a hardware/software provider.

12. **Status Report and where to go from here:**

As your first two weeks wind down, the IT Manager, HR Manager as well as other management are interested in your experience. With your position being the first dedicated Information Security role, they would like a 'big picture' view of what you've done as well as the security posture of DFI.

Similar to Defense-in-Depth, an organization has multiple layers of security from the edge of their web presence all the way to permissions on a file.

In your own words, explain the work you've done, the recommendations made, and how DFI should proceed from a security standpoint. This is your opportunity to provide a thoughtful analysis that shows your understanding of Cyber Security and how all of the tasks you've performed contribute to the security of DFI. As this will be reviewed by non-technical management, please keep the technical jargon to a minimum.

[Provide your Status Report Here]

- Explain all of the tasks performed in the first two weeks.
- Explain any recommendations for changes in permissions.
- Tie all of the work done together in a big picture narrative.
- Recommend the way forward for DFI in terms of security products (at least 2) and policies (also at least 2.)
-

During the first 2 very hard weeks, the tasks involved a system evaluation from a security point of view. My priority was to get familiar with Windows settings for updates, Firewall setting, Folder and Accounts Permissions, Services that run on the server. The next step was to Set up a firewall rules, to recommend an VPN encryption method suitable to DFI. Then an IDS rule was needed, and some HASH file verification was requested. Then, Automation for the network security, where I recommended Tufin Secure track, automation for Endpoint security with CrowdStrike Falcon and Data protection with Rubik. A report was prepared for Login RDP attempts. An analysis for Windows Updates was prepared, with focus on stability

and security. For Linux, directories, set owner permissions, and users was needed. A report for firewall Alert Response was provided to the management, considering various IP addresses that tried to penetrate the network.

13. **File Encryption:**

As your final task, assemble all the deliverables you have created in Steps 1-12 and encrypt them using 7zip with a strong password, 15 or more characters.

When you submit the file you must also include your password as a note to the reviewer at Udacity or they will not be able to review your project. See the classroom instructions for the submission.