ACE Compliance Report

Evidence ID – 1741884584945

Scan Date	13-Mar-2025
Report Date	13-Mar-2025
Kbox No	1980
Target IP address	172.18.36.186
Target Hostname	EC2AMAZ-TG2STE6
Target Operating System	Microsoft Windows Server 2025 Datacenter OS Version: 10.0.26100 N/A Build 26100
Technology	Windows

Table of Contents

Table of Contents

Running Services (Q21)

Status: **Assessor Review Required**

Sub Status: Assessor must review the list of running services and check if system has any unwanted services running other than "telnet","snmp","smtp","pop3","imap","ftp","VNC" or port "5901". If yes, then client to provide justification to Assessor, else remove/uninstall the unwanted services.

Evidence:

These Windows services are started:

Amazon SSM Agent
App Readiness
Application Host Helper Service
Application Information
Application Management
AppX Deployment Service (AppXSVC)
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
Capability Access Manager Service
Certificate Propagation
Clipboard User Service_16076ef
CNG Key Isolation
COM+ Event System
Connected Devices Platform Service
Connected Devices Platform User Service_16076ef
Connected User Experiences and Telemetry
CoreMessaging
Credential Manager
Cryptographic Services
Data Sharing Service
DCOM Server Process Launcher
DHCP Client
Diagnostic Policy Service
Diagnostic System Host
Display Policy Service
DisplayEnhancementService
Distributed Link Tracking Client
Distributed Transaction Coordinator
DNS Client
Geolocation Service
Group Policy Client
IIS Admin Service
Inventory and Compatibility Appraisal service
IP Helper
Local Session Manager
Message Queuing
Microsoft Account Sign-in Assistant
Microsoft Defender Antivirus Network Inspection Service
Microsoft Defender Antivirus Service
Microsoft Store Install Service
Net.Msmq Listener Adapter
Net.Pipe Listener Adapter
Net.Tcp Listener Adapter

```
Net.Tcp Port Sharing Service
Network Connection Broker
Network List Service
Network Store Interface Service
Plug and Play
Power
Print Spooler
Program Compatibility Assistant Service
Radio Management Service
Remote Desktop Configuration
Remote Desktop Services
Remote Desktop Services UserMode Port Redirector
Remote Procedure Call (RPC)
RPC Endpoint Mapper
Security Accounts Manager
Server
Shell Hardware Detection
Smart Card Device Enumeration Service
State Repository Service
Storage Service
Sync Host_16076ef
SysMain
System Event Notification Service
System Events Broker
Task Scheduler
TCP/IP NetBIOS Helper
Text Input Management Service
Themes
Time Broker
Udk User Service_16076ef
Update Orchestrator Service
User Access Logging Service
User Manager
User Profile Service
Web Account Manager
Windows Audio
Windows Audio Endpoint Builder
Windows Connection Manager
Windows Defender Firewall
Windows Event Log
Windows Font Cache Service
Windows License Manager Service
Windows Management Instrumentation
Windows Modules Installer
Windows Process Activation Service
Windows Push Notifications System Service
Windows Push Notifications User Service_16076ef
Windows Remote Management (WS-Management)
Windows Security Service
Windows Time
WinHTTP Web Proxy Auto-Discovery Service
Workstation
World Wide Web Publishing Service

The command completed successfully.
```

Password Length (Q50)

Status: **ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required**

Probable Reason: Minimum password length is either not set or is set to be less than 7

Synopsis: This evidence lists the minimum length of password on Windows, Linux and AIX system scanned and checks if length is more than or equal to 7. If not, then the evidence is marked as Non-Compliant. If you have any other method, service or software implemented to manage password policies, then provide evidence and justification to the assessor.

Evidence:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    10
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        SERVER
The command completed successfully.
```

Latest Patch Date (Q34)

Status: **ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required**

Sub Status: Machine has NOT been patched within last 90 days. Assessor also must check latest microsoft released patch with machine updated patch.

Probable Reason: The latest patch updated date is not within 90 days from the date the scan is run.

Synopsis: This evidence documents list of patches installed on each Windows or Linux system scanned and it checks if the latest patch updated is within 90 days from the date the scan is run. If not, it identifies as non-compliant or otherwise identifies as compliant. ACE scanner collects this information by log on to the system.

You can now check only those IP addresses specific files mentioned in Impacted IPs section and either fix the issue by installing latest patches or provide justification.

Evidence:

```
wmic : The term 'wmic' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:251
+ ... $prevDate -split "-"; $prevYear= "$($prevDateArray[2])"; wmic qfe whe ...
+                                                              ~~~~
+ CategoryInfo          : ObjectNotFound: (wmic:String) [], CommandNotFoundException
```

```
+ FullyQualifiedErrorId : CommandNotFoundException
```

Inactive Users (Q48)

Status: Compliant

Evidence:

```
No inactive user found
```

Audit Policy 1 (Q67)

Status: ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required

Probable Reason: Audit policies required to generate PCI related events are not set on your Linux, Windows or AIX systems.

Synopsis: This evidence lists the audit policies set in your Linux, Windows or AIX systems. The application checks Auditd or syslog for Linux, GPO policies for Windows.

Audit policies should be set to generate events under following categories, "Access to audit trails", "Add-Delete-Change to Accounts", "Creation Deletion of System Objects", "Failed Login", "Identification Mechanism", "Initialization of Audit Logging", "Privilege Elevation", "Root Action", "Stop or Pause of Audit Logging".

Please ensure that audit policies are set for above events. If you are using any other software or package other than Auditd, GPO, then provide evidence and justification to assessor.

Evidence:

```
System audit policy
Category/Subcategory                    Setting
System
Security System Extension               No Auditing
System Integrity                        Success and Failure
IPsec Driver                            No Auditing
Other System Events                     Success and Failure
Security State Change                   Success
Logon/Logoff
Logon                                   Success and Failure
Logoff                                  Success
Account Lockout                         Success
IPsec Main Mode                         No Auditing
IPsec Quick Mode                        No Auditing
IPsec Extended Mode                     No Auditing
Special Logon                           Success
Other Logon/Logoff Events               No Auditing
Network Policy Server                   Success and Failure
```

```
User / Device Claims                No Auditing
Group Membership                    No Auditing
Object Access
File System                         No Auditing
Registry                            No Auditing
Kernel Object                       No Auditing
SAM                                 No Auditing
Certification Services              No Auditing
Application Generated               No Auditing
Handle Manipulation                 No Auditing
File Share                          No Auditing
Filtering Platform Packet Drop      No Auditing
Filtering Platform Connection       No Auditing
Other Object Access Events          No Auditing
Detailed File Share                 No Auditing
Removable Storage                   No Auditing
Central Policy Staging              No Auditing
Privilege Use
Non Sensitive Privilege Use         No Auditing
Other Privilege Use Events          No Auditing
Sensitive Privilege Use             No Auditing
```

List Patch Level (Q34)

Status: Compliant

Evidence:

```
wmic : The term 'wmic' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:251
+ ... $prevDate -split "-"; $prevYear= "$($prevDateArray[2])"; wmic qfe whe ...
+                                                              ~~~~
+ CategoryInfo          : ObjectNotFound: (wmic:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

Network Connections (Q21)

Status: Assessor Review Required

Sub Status: Assessor must review the processes, services, connections that are open/running in background and check if system has any unwanted processes, services, connections open/running in background other than "telnet","snmp","smtp","pop3","imap","ftp","VNC" or port "5901". Client to provide justification to Assessor, else remove/uninstall the unwanted processes, services, connections.

Evidence:

```
Active Connections

Proto  Local Address          Foreign Address        State
```

```
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING
TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
TCP    172.18.36.186:139      0.0.0.0:0              LISTENING
TCP    172.18.36.186:3389     172.18.2.242:65232     ESTABLISHED
TCP    172.18.36.186:49738    20.7.2.167:443         ESTABLISHED
TCP    172.18.36.186:50672    20.190.151.134:443     TIME_WAIT
TCP    172.18.36.186:50686    4.152.133.8:443        ESTABLISHED
TCP    172.18.36.186:50687    13.91.96.185:443       ESTABLISHED
TCP    172.18.36.186:50690    172.178.160.22:443     ESTABLISHED
TCP    172.18.36.186:50691    64.233.180.94:443      ESTABLISHED
TCP    172.18.36.186:50693    13.107.21.239:443      ESTABLISHED
TCP    172.18.36.186:50698    20.42.65.88:443        ESTABLISHED
TCP    172.18.36.186:50699    150.171.28.10:443      ESTABLISHED
TCP    [::]:80                [::]:0                 LISTENING
TCP    [::]:135               [::]:0                 LISTENING
TCP    [::]:445               [::]:0                 LISTENING
TCP    [::]:1801              [::]:0                 LISTENING
TCP    [::]:2103              [::]:0                 LISTENING
TCP    [::]:2105              [::]:0                 LISTENING
TCP    [::]:2107              [::]:0                 LISTENING
TCP    [::]:3389              [::]:0                 LISTENING
TCP    [::]:5985              [::]:0                 LISTENING
TCP    [::]:47001             [::]:0                 LISTENING
TCP    [::]:49664             [::]:0                 LISTENING
TCP    [::]:49665             [::]:0                 LISTENING
TCP    [::]:49666             [::]:0                 LISTENING
TCP    [::]:49667             [::]:0                 LISTENING
TCP    [::]:49668             [::]:0                 LISTENING
TCP    [::]:49669             [::]:0                 LISTENING
TCP    [::]:49671             [::]:0                 LISTENING
TCP    [::]:49672             [::]:0                 LISTENING
TCP    [::1]:50694            [::1]:5985             TIME_WAIT
TCP    [::1]:50695            [::1]:5985             TIME_WAIT
UDP    0.0.0.0:123            *:*
UDP    0.0.0.0:3389           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
UDP    0.0.0.0:57322          *:*
UDP    0.0.0.0:58539          *:*
```

```
UDP    0.0.0.0:59649          64.233.180.94:443
UDP    127.0.0.1:53010        127.0.0.1:53010
UDP    172.18.36.186:137      *:*
UDP    172.18.36.186:138      *:*
UDP    [::]:123               *:*
UDP    [::]:3389              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5355              *:*
UDP    [::]:57322             *:*
UDP    [::]:58539             *:*
```

List of Users and Groups (Q45)

Status: Compliant

Evidence:

```
User accounts for \\EC2AMAZ-TG2STE6

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
WDAGUtilityAccount
The command completed successfully.


Aliases for \\EC2AMAZ-TG2STE6

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*OpenSSH Users
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Storage Replica Administrators
*System Managed Accounts Group
```

```
*User Mode Hardware Operators
*Users
The command completed successfully.

Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.
```

Password Complexity (Q50)

Status: Compliant

Evidence:

```
The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
PasswordComplexity = 1
```

Password Expiry (Q50)

Status: Compliant

Evidence:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    10
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        SERVER
The command completed successfully.
```

Password History (Q50)

Status: **ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required**

Probable Reason: Password history maintenance is either not set or is set for less than 4.

Synopsis: This evidence lists the password history on Windows, Linux and AIX system scanned and checks if history is maintained for password, if yes, then history maintained should be for at least last 4 passwords. If not, then the evidence is marked as Non-Compliant. If you have any other method, service or software implemented to manage password policies, then provide evidence and justification to the assessor.

Evidence:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    10
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        SERVER
The command completed successfully.
```

Account Lockout Threshold (Q50)

Status: **Compliant**

Evidence:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    10
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        SERVER
The command completed successfully.
```

Account Lockout Duration (Q50)

Status: **ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required**

Probable Reason: Account Lockout duration is either not set or is set as less than 30 mins

Synopsis: This evidence lists the account lockout policy for Account Lockout Duration on Windows, Linux and AIX system scanned and checks if the account lockout policy is set. If the duration set is not more than or equal to 30 mins, then it marks evidence as Non-Compliant.

If you have any other method, service or software implemented to manage account policies, then provide evidence and justification to the assessor.

Evidence:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    10
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        SERVER
The command completed successfully.
```

Session Timeout (Q50)

Status: **ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required**

Probable Reason: User account login session timeout is either not set or is set for more than 15 mins in Windows, or 900 seconds in Linux/AIX based system

Synopsis: This evidence outlines the required session timeout periods for user account logins. For Windows systems, the timeout must be set to less than or equal to 15 minutes. On Linux/AIX-based systems, the timeout must be set to 900 seconds or less. In Windows, if Remote Desktop Protocol (RDP) is enabled, either the RDP session timeout or interactive logon session timeout must be configured accordingly. If RDP is disabled, the interactive logon session timeout must be set to less than or equal to 15 minutes. Failure to meet these requirements results in the evidence being marked as Non-Compliant. If alternative methods, services, or software are utilized to manage session timeout, evidence and justification should be provided to the assessor.

Evidence:

```
**********RDP SETTING**********
```

```
Hive: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control


Name                           Property
----                           --------
Terminal Server                AllowRemoteRPC               : 1
DelayConMgrTimeout             : 0
DeleteTempDirsOnExit           : 1
fDenyTSConnections             : 0
fSingleSessionPerUser          : 1
NotificationTimeOut            : 0
PerSessionTempDir              : 1
ProductVersion                 : 5.1
RCDependentServices            : {CertPropSvc, SessionEnv}
SessionDirectoryActive         : 0
SessionDirectoryCLSID          : {005a9c68-e216-4b27-8f59-b336829b3868}
SessionDirectoryExCLSID        : {ec98d957-48ad-436d-90be-bc291f42709c}
SessionDirectoryExposeServerIP : 1
SnapshotMonitors               : 1
StartRCM                       : 0
TSUserEnabled                  : 0
InstanceID                     : 4964350e-0cdb-46d6-a597-616b88e
GlassSessionId                 : 1
LastRemoteLogonTime            : 2025-03-13T16:38:48.729Z


*************RDP SESSION TIMEOUT*************



Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT


Name                           Property
----                           --------
Terminal Services


*************INTERACTIVE LOGON SESSION TIMEOUT*************



Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies


Name                           Property
----                           --------
System                         ConsentPromptBehaviorAdmin        : 5
ConsentPromptBehaviorEnhancedAdmin : 1
ConsentPromptBehaviorUser          : 3
DelayedDesktopSwitchTimeout        : 0
DisableAutomaticRestartSignOn      : 1
DSCAutomationHostEnabled           : 2
EnableInstallerDetection           : 1
```

```
EnableLUA                    : 1
EnableSecureUIAPaths         : 1
EnableUIADesktopToggle       : 0
EnableVirtualization         : 1
PromptOnSecureDesktop        : 1
TypeOfAdminApprovalMode      : 1
ValidateAdminCodeSignatures  : 0
EnableCursorSuppression      : 1
EnableFullTrustStartupTasks  : 2
EnableUwpStartupTasks        : 2
SupportFullTrustStartupTasks : 1
SupportUwpStartupTasks       : 1
disablecad                   : 0
dontdisplaylastusername      : 0
legalnoticecaption           :
legalnoticetext              : □
scforceoption                : 0
shutdownwithoutlogon         : 0
undockwithoutlogon           : 1
```

RDP/SSH Configuration (Q24)

Status: **ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required**

Probable Reason: RDP for Windows based system is enabled with insecure encryption level

Synopsis: This evidence list the RDP configuration information on scanned systems and checks if remote terminal connection is enabled. If remote terminal connection is enabled and encryption level is set to less than 3, then application marks the evidence as Non-Compliant. If the connection is required to be enabled with insecure encryption level, please provide evidence and justification to the assessor.

Evidence:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
AllowRemoteRPC    REG_DWORD    0x1
DelayConMgrTimeout    REG_DWORD    0x0
DeleteTempDirsOnExit    REG_DWORD    0x1
fDenyTSConnections    REG_DWORD    0x0
fSingleSessionPerUser    REG_DWORD    0x1
NotificationTimeOut    REG_DWORD    0x0
PerSessionTempDir    REG_DWORD    0x1
ProductVersion    REG_SZ    5.1
RCDependentServices    REG_MULTI_SZ    CertPropSvc\0SessionEnv
SessionDirectoryActive    REG_DWORD    0x0
SessionDirectoryCLSID    REG_SZ    {005a9c68-e216-4b27-8f59-b336829b3868}
SessionDirectoryExCLSID    REG_SZ    {ec98d957-48ad-436d-90be-bc291f42709c}
SessionDirectoryExposeServerIP    REG_DWORD    0x1
SnapshotMonitors    REG_SZ    1
StartRCM    REG_DWORD    0x0
TSUserEnabled    REG_DWORD    0x0
InstanceID    REG_SZ    4964350e-0cdb-46d6-a597-616b88e
GlassSessionId    REG_DWORD    0x1
```

```
LastRemoteLogonTime    REG_SZ    2025-03-13T16:38:48.729Z

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\AddIns
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ClusterSettings
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ConnectionHandler
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\KeyboardType Mapping
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\SessionArbitrationHelper
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\SysProcs
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TerminalTypes
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Utilities
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\VIDEO
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
AudioEnumeratorDll    REG_SZ    rdpendp.dll
Callback    REG_DWORD    0x0
CallbackNumber    REG_SZ
CdClass    REG_DWORD    0x0
CdDLL    REG_SZ
CdFlag    REG_DWORD    0x0
CdName    REG_SZ
CfgDll    REG_SZ    RDPCFGEX.DLL
ColorDepth    REG_DWORD    0x3
Comment    REG_SZ
Domain    REG_SZ
DrawGdiplusSupportLevel    REG_DWORD    0x1
EncoderDllName    REG_SZ    RdpAvenc.dll
fAllowSecProtocolNegotiation    REG_DWORD    0x1
fAutoClientDrives    REG_DWORD    0x1
fAutoClientLpts    REG_DWORD    0x1
fDisableAudioCapture    REG_DWORD    0x0
fDisableCam    REG_DWORD    0x0
fDisableCcm    REG_DWORD    0x0
fDisableCdm    REG_DWORD    0x0
fDisableClip    REG_DWORD    0x0
fDisableCpm    REG_DWORD    0x0
fDisableEncryption    REG_DWORD    0x1
fDisableExe    REG_DWORD    0x0
fDisableLPT    REG_DWORD    0x0
fEnableWinStation    REG_DWORD    0x1
fForceClientLptDef    REG_DWORD    0x1
fHomeDirectoryMapRoot    REG_DWORD    0x0
fInheritAutoClient    REG_DWORD    0x1
fInheritAutoLogon    REG_DWORD    0x1
fInheritCallback    REG_DWORD    0x0
fInheritCallbackNumber    REG_DWORD    0x1
fInheritColorDepth    REG_DWORD    0x0
fInheritInitialProgram    REG_DWORD    0x1
fInheritMaxDisconnectionTime    REG_DWORD    0x1
fInheritMaxIdleTime    REG_DWORD    0x1
fInheritMaxSessionTime    REG_DWORD    0x1
fInheritReconnectSame    REG_DWORD    0x1
fInheritResetBroken    REG_DWORD    0x1
fInheritSecurity    REG_DWORD    0x0
```

```
fInheritShadow    REG_DWORD    0x1
fLogonDisabled    REG_DWORD    0x0
fPromptForPassword    REG_DWORD    0x0
fReconnectSame    REG_DWORD    0x0
fResetBroken    REG_DWORD    0x0
fUseDefaultGina    REG_DWORD    0x0
InitialProgram    REG_SZ
InputBufferLength    REG_DWORD    0x800
InteractiveDelay    REG_DWORD    0x32
KeepAliveTimeout    REG_DWORD    0x0
KeyboardLayout    REG_DWORD    0x0
LanAdapter    REG_DWORD    0x0
LoadableProtocol_Object    REG_SZ    {5828227c-20cf-4408-b73f-73ab70b8849f}
MaxConnectionTime    REG_DWORD    0x0
MaxDisconnectionTime    REG_DWORD    0x0
MaxIdleTime    REG_DWORD    0x0
MaxInstanceCount    REG_DWORD    0xffffffff
MinEncryptionLevel    REG_DWORD    0x2
NWLogonServer    REG_SZ
OutBufCount    REG_DWORD    0x6
OutBufDelay    REG_DWORD    0x64
OutBufLength    REG_DWORD    0x212
Password    REG_SZ
PdClass    REG_DWORD    0x2
PdClass1    REG_DWORD    0xb
PdDLL    REG_SZ    tdtcp
PdDLL1    REG_SZ    tssecsrv
PdFlag    REG_DWORD    0x4e
PdFlag1    REG_DWORD    0x0
PdName    REG_SZ    tcp
PdName1    REG_SZ    tssecsrv
PortNumber    REG_DWORD    0xd3d
SecurityLayer    REG_DWORD    0x2
SelectNetworkDetect    REG_DWORD    0x1
SelectTransport    REG_DWORD    0x2
Shadow    REG_DWORD    0x1
UserAuthentication    REG_DWORD    0x1
Username    REG_SZ
WdFlag    REG_DWORD    0x36
WdName    REG_SZ    Microsoft RDP 8.0
WdPrefix    REG_SZ    RDP
WebSocketListenerPort    REG_DWORD    0xd3b
WebSocketTlsListenerPort    REG_DWORD    0xd40
WFProfilePath    REG_SZ
WorkDirectory    REG_SZ

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
Tcp\TSMMRemotingAllowedApps
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
Tcp\VideoRemotingWindowNames
```

Audit Service (Q67)

Status: Compliant

Evidence:

```
Status   Name            DisplayName
------   ----            -----------
Running  EventLog        Windows Event Log
```

Vendor Accounts (Q49)

Status: Assessor Review Required

Evidence:

```
User accounts for \\EC2AMAZ-TG2STE6

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
WDAGUtilityAccount
The command completed successfully.


Aliases for \\EC2AMAZ-TG2STE6

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*OpenSSH Users
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Storage Replica Administrators
*System Managed Accounts Group
*User Mode Hardware Operators
```

*Users
The command completed successfully.

Alias name Administrators
Comment Administrators have complete and unrestricted access to the computer/domain

Members

Administrator
The command completed successfully.

Password Encryption during Storage (Q51)

Status: Compliant

Evidence:

Windows handles this requirement by default. Refer: https://docs.microsoft.com/en-us/windows/win32/secauthn/microsoft-ntlm

OS Name and Version (Q34)

Status: Compliant

Evidence:

OS Name: Microsoft Windows Server 2025 Datacenter
OS Version: 10.0.26100 N/A Build 26100
'wmic' is not recognized as an internal or external command,
operable program or batch file.

NTP (Q69)

Status: Assessor Review Required

Evidence:

.
----------NTP Registry Information----------

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
NTPServer REG_SZ 169.254.169.123,0x9
ServiceDll REG_EXPAND_SZ %systemroot%\system32\w32time.dll
ServiceDllUnloadOnStop REG_DWORD 0x1
ServiceMain REG_SZ SvchostEntry_W32Time
Type REG_SZ NTP

----------NTP Configuration----------
[Configuration]

EventLogFlags: 2 (Local)
AnnounceFlags: 10 (Local)
TimeJumpAuditOffset: 28800 (Local)
MinPollInterval: 6 (Local)
MaxPollInterval: 10 (Local)
MaxNegPhaseCorrection: 54000 (Local)
MaxPosPhaseCorrection: 54000 (Local)
MaxAllowedPhaseOffset: 1 (Local)

FrequencyCorrectRate: 4 (Local)
PollAdjustFactor: 5 (Local)
LargePhaseOffset: 50000000 (Local)
SpikeWatchPeriod: 900 (Local)
LocalClockDispersion: 10 (Local)
HoldPeriod: 5 (Local)
PhaseCorrectRate: 1 (Local)
UpdateInterval: 100 (Local)

FileLogName: (Local)
FileLogEntries: (Local)
FileLogSize: 0 (Local)

[TimeProviders]

NtpClient (Local)
DllName: C:\Windows\system32\w32time.dll (Local)
Enabled: 1 (Local)
InputProvider: 1 (Local)
AllowNonstandardModeCombinations: 1 (Local)
ResolvePeerBackoffMinutes: 15 (Local)
ResolvePeerBackoffMaxTimes: 7 (Local)
CompatibilityFlags: 2147483648 (Local)
EventLogFlags: 1 (Local)
LargeSampleSkew: 3 (Local)
SpecialPollInterval: 1024 (Local)
Type: NTP (Local)
NTPServer: 169.254.169.123,0x9 (Local)

VMICTimeProvider (Local)
DllName: C:\Windows\System32\vmictimeprovider.dll (Local)
Enabled: 1 (Local)
InputProvider: 1 (Local)

NTPServer (Local)
DllName: C:\Windows\system32\w32time.dll (Local)
Enabled: 0 (Local)
InputProvider: 0 (Local)

----------NTP Status----------
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0006664s

```
Root Dispersion: 0.0223355s
ReferenceId: 0xA9FEA97B (source IP:  169.254.169.123)
Last Successful Sync Time: 3/13/2025 4:35:00 PM
Source: 169.254.169.123,0x9
Poll Interval: 10 (1024s)
```

Password Encryption during Transmission (Q51)

Status: Compliant

Evidence:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
AllowRemoteRPC    REG_DWORD    0x1
DelayConMgrTimeout    REG_DWORD    0x0
DeleteTempDirsOnExit    REG_DWORD    0x1
fDenyTSConnections    REG_DWORD    0x0
fSingleSessionPerUser    REG_DWORD    0x1
NotificationTimeOut    REG_DWORD    0x0
PerSessionTempDir    REG_DWORD    0x1
ProductVersion    REG_SZ    5.1
RCDependentServices    REG_MULTI_SZ    CertPropSvc\0SessionEnv
SessionDirectoryActive    REG_DWORD    0x0
SessionDirectoryCLSID    REG_SZ    {005a9c68-e216-4b27-8f59-b336829b3868}
SessionDirectoryExCLSID    REG_SZ    {ec98d957-48ad-436d-90be-bc291f42709c}
SessionDirectoryExposeServerIP    REG_DWORD    0x1
SnapshotMonitors    REG_SZ    1
StartRCM    REG_DWORD    0x0
TSUserEnabled    REG_DWORD    0x0
InstanceID    REG_SZ    4964350e-0cdb-46d6-a597-616b88e
GlassSessionId    REG_DWORD    0x1
LastRemoteLogonTime    REG_SZ    2025-03-13T16:38:48.729Z

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\AddIns
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ClusterSettings
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ConnectionHandler
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\KeyboardType Mapping
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\SessionArbitrationHelper
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\SysProcs
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TerminalTypes
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Utilities
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\VIDEO
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations
```

Admin Accounts (Q20)

Status: **ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required**

Probable Reason: "Administrator" or "Admin" accounts in Windows are not renamed

Synopsis: This evidence identifies if the "Administrator" or "Admin" accounts in Windows are renamed. If not, then the evidence is marked as Non-Compliant. If you have "Administrator" or "Admin" accounts not renamed, then kindly provide justification to assessor.

Evidence:

```
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/11/2025 1:08:00 PM
Password expires             4/22/2025 1:08:00 PM
Password changeable          3/11/2025 1:08:00 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/13/2025 4:38:48 PM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.

The user name could not be found.

More help is available by typing NET HELPMSG 2221.
```

Guest Accounts (Q20)

Status: Compliant

Evidence:

```
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            3/13/2025 4:46:22 PM
Password expires             Never
Password changeable          3/13/2025 4:46:22 PM
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Guests
Global Group memberships     *None
The command completed successfully.
```

Audit Policy 2 (Q67)

Status: ACE decision: Non-Compliant, Customer to remediate the issue or provide justification and then Assessor review required

Probable Reason: Audit policies required to generate PCI related events are not set on your Linux, Windows or AIX systems.

Synopsis: This evidence lists the audit policies set in your Linux, Windows or AIX systems. The application checks Auditd or syslog for Linux, GPO policies for Windows.

Audit policies should be set to generate events under following categories, "Access to audit trails", "Add-Delete-Change to Accounts", "Creation Deletion of System Objects", "Failed Login", "Identification Mechanism", "Initialization of Audit Logging", "Privilege Elevation", "Root Action", "Stop or Pause of Audit

Logging".

Please ensure that audit policies are set for above events. If you are using any other software or package other than Auditd, GPO, then provide evidence and justification to assessor.

Evidence:

```
System audit policy
Category/Subcategory                    Setting
Detailed Tracking
Process Termination                     No Auditing
DPAPI Activity                          No Auditing
RPC Events                              No Auditing
Plug and Play Events                    No Auditing
Token Right Adjusted Events             No Auditing
Process Creation                        No Auditing
Policy Change
Audit Policy Change                     Success
Authentication Policy Change            Success
Authorization Policy Change             No Auditing
MPSSVC Rule-Level Policy Change         No Auditing
Filtering Platform Policy Change        No Auditing
Other Policy Change Events              No Auditing
Account Management
User Account Management                 Success
Computer Account Management             Success
Security Group Management               Success
Distribution Group Management           No Auditing
Application Group Management            No Auditing
Other Account Management Events         No Auditing
DS Access
Directory Service Changes               No Auditing
Directory Service Replication           No Auditing
Detailed Directory Service Replication  No Auditing
Directory Service Access                Success
Account Logon
Kerberos Service Ticket Operations      Success
Other Account Logon Events              No Auditing
Kerberos Authentication Service         Success
Credential Validation                   Success
```

Service Accounts (Q45)

Status: **Assessor Review Required**

Evidence:

```
'WMIC' is not recognized as an internal or external command,
operable program or batch file.
```

Users Last Login (Q48)

Status: **Assessor Review Required**

Evidence:

```
Username      LastLogin
--------      ---------
Administrator 3/13/2025 4:38:48 PM
```

Antimalware And Version (Q31)

Status: **Assessor Review Required**

Evidence:

```
DisplayName                                          DisplayVersion
-----------                                          --------------
Microsoft Edge WebView2 Runtime                      133.0.3065.92
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.42.34433 14.42.34433.0
Microsoft Edge                                       134.0.3124.66
Amazon SSM Agent                                     3.3.1611.0
aws-cfn-bootstrap                                    2.0.32
```

FIM Agent And Version (Q81)

Status: **Assessor Review Required**

Evidence:

```
DisplayName                                          DisplayVersion
-----------                                          --------------
Microsoft Edge WebView2 Runtime                      133.0.3065.92
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.42.34433 14.42.34433.0
Microsoft Edge                                       134.0.3124.66
Amazon SSM Agent                                     3.3.1611.0
aws-cfn-bootstrap                                    2.0.32
```

Domain Controller Information

Evidence:

```
'wmic' is not recognized as an internal or external command,
operable program or batch file.
```

User and Domain Details

Evidence:

```
'wmic' is not recognized as an internal or external command,
operable program or batch file.
```

NIC Details

Evidence:

```
'wmic' is not recognized as an internal or external command,
operable program or batch file.
```

Logon Server

Evidence:

```
\\EC2AMAZ-TG2STE6
```

GPO and Active Directory Policy

Evidence:

```
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
c Microsoft Corporation. All rights reserved.

Created on ?3/?13/?2025 at 4:46:31 PM


RSOP data for EC2AMAZ-TG2STE6\Administrator on EC2AMAZ-TG2STE6 : Logging Mode
-------------------------------------------------------------------------------

OS Configuration:          Standalone Server
OS Version:                10.0.26100
Site Name:                 N/A
Roaming Profile:           N/A
```

Local Profile: C:\Users\Administrator
Connected over a slow link?: No

COMPUTER SETTINGS

Last time Group Policy was applied: 3/12/2025 at 1:33:32 PM
Group Policy was applied from: N/A
Group Policy slow link threshold: 500 kbps
Domain Name: WINAMAZ-51QCEN9
Domain Type: WindowsNT 4

Applied Group Policy Objects

N/A

The following GPOs were not applied because they were filtered out
---
Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups

System Mandatory Level
Everyone
BUILTIN\Users
NT AUTHORITY\SERVICE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
gpsvc
LOCAL
BUILTIN\Administrators

Resultant Set Of Policies for Computer

Software Installations

N/A

Startup Scripts

N/A

Shutdown Scripts

N/A

Account Policies

N/A

Audit Policy

N/A

User Rights

N/A

Security Options

N/A

N/A

Event Log Settings

N/A

Restricted Groups

N/A

System Services

N/A

Registry Settings

N/A

File System Settings

N/A

Public Key Policies

N/A

Administrative Templates

N/A

USER SETTINGS

Last time Group Policy was applied: 3/13/2025 at 4:38:48 PM
Group Policy was applied from: N/A
Group Policy slow link threshold: 500 kbps
Domain Name: EC2AMAZ-TG2STE6
Domain Type: <Local Computer>

Applied Group Policy Objects

N/A

The following GPOs were not applied because they were filtered out
---
Local Group Policy
Filtering: Not Applied (Empty)

```
The user is a part of the following security groups
---------------------------------------------------
None
Everyone
Local account and member of Administrators group
BUILTIN\Administrators
BUILTIN\Users
REMOTE INTERACTIVE LOGON
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
This Organization
Local account
LOCAL
NTLM Authentication
High Mandatory Level

The user has the following security privileges
----------------------------------------------

Bypass traverse checking
Manage auditing and security log
Back up files and directories
Restore files and directories
Change the system time
Shut down the system
Force shutdown from a remote system
Take ownership of files or other objects
Debug programs
Modify firmware environment values
Profile system performance
Profile single process
Increase scheduling priority
Load and unload device drivers
Create a pagefile
Adjust memory quotas for a process
Remove computer from docking station
Perform volume maintenance tasks
Impersonate a client after authentication
Create global objects
Change the time zone
Create symbolic links
Obtain an impersonation token for another user in the same session
Increase a process working set

Resultant Set Of Policies for User
----------------------------------

Software Installations
----------------------
N/A

Logon Scripts
-------------
N/A

Logoff Scripts
```

N/A

Public Key Policies

N/A

Administrative Templates

N/A

Folder Redirection

N/A

Internet Explorer Browser User Interface

N/A

Internet Explorer Connection

N/A

Internet Explorer URLs

N/A

Internet Explorer Security

N/A

Internet Explorer Programs

N/A