

Active Directory Hardening Windows Server 2012

1. Helpful commands:

Common Commands

Command	Explained	Command	Explained
Tasklist	List Process	ping	Ping a machine

Taskkill	Kill a process with PID	del	Delete a file
nslookup	Lookup DNS Record	rmdir	Remove Directory
ipconfig /all	Network Configuration	copy	Copy a files.
tracert	Traceroute	tree	See directory Contents
systeminfo	See Systeminfo	attrib	see
find	Grep equivalent, Find a string	Schtasks	List all scheduled Tasks
hostname	See hostname		

Networking and Firewall

Task	Command
Configure your server to use a proxy server	netsh Winhttp set proxy <servername>:<port number> <i>Note: Server Core installations can't access the Internet through a proxy that requires a password to allow connections.</i>
Configure your server to bypass the proxy for internet addresses	netsh winhttp set proxy <servername>:<port number> bypass-list="<local>"
Display or modify IPSEC configuration	netsh ipsec
Display or modify NAP configuration	netsh nap
Display or modify IP to physical address translation	arp
Display or configure the local routing table	route
View or configure DNS server settings	nslookup
Display protocol statistics and current TCP/IP network connections	netstat
Display TCP/UDP connections	netstat /t Netstat /i
Display protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP (NBT)	nbtstat
Display hops for network connections	pathping
Trace hops for network connections	tracert
Display to configuration of the multicast router	mrinfo
Enable/Disable remote administration of the firewall	netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=yes

Get a new DHCP lease	ipconfig /release ipconfig /renew
----------------------	--------------------------------------

2. Disable SMBv1

<https://learn.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server>

To remove SMBv1 from Windows Server:

1. On the Server Manager Dashboard of the server where you want to remove SMBv1, under **Configure this local server**, select **Add roles and features**.
2. On the **Before you begin** page, select **Start the Remove Roles and Features Wizard**, and then on the following page, select **Next**.
3. On the **Select destination server** page under **Server Pool**, ensure that the server you want to remove the feature from is selected, and then select **Next**.
4. On the **Remove server roles** page, select **Next**.
5. On the **Remove features** page, clear the check box for **SMB 1.0/CIFS File Sharing Support** and select **Next**.
6. On the **Confirm removal selections** page, confirm that the feature is listed, and then select **Remove**.


You can detect SMBv1 status, without elevation, by running: `Get-SmbServerConfiguration | Format-List EnableSMB1Protocol`.

Windows 8 and Windows Server 2012 introduced the new **Set-SMBServerConfiguration** Windows PowerShell cmdlet. The cmdlet enables you to enable or disable the SMBv1, SMBv2, and SMBv3 protocols on the server component.

You don't have to restart the computer after you run the **Set-SMBServerConfiguration** cmdlet.


SMBv1

- Detect:

PowerShell  Copy


```
Get-SmbServerConfiguration | Select EnableSMB1Protocol
```

- Disable:

PowerShell  Copy

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```


- Enable:

PowerShell  Copy

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```


SMB v2/v3

- Detect:

PowerShell  Copy


```
Get-SmbServerConfiguration | Select EnableSMB2Protocol
```

- Disable:

PowerShell  Copy

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

- Enable:

PowerShell  Copy

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

3. Enable Audit Policy Settings with Group Policy

Ensure the following Audit Policy settings are configured in group policy and applied to all computers and servers.

Computer Configuration -> Policies -Windows Settings -> Security Settings -> Advanced Audit Policy Configuration

System

Audit 'IPsec Driver' is set to 'Success and Failure'

Audit 'Other System Events' is set to 'Success and Failure'

Audit 'Security State Change' is set to 'Success'

Audit 'Security System Extension' is set to 'Success and Failure'

Audit 'System Integrity' is set to 'Success and Failure'

Malicious activity often starts on workstations, if you're not monitoring all systems you could be missing early signs of an attack.

Policy Change

Audit 'Audit Policy Change' is set to 'Success and Failure'

Audit 'Authentication Policy Change' is set to 'Success'

Audit 'Authorization Policy Change' is set to 'Success'

Privilege Use

Audit 'Sensitive Privilege Use' is set to 'Success and Failure'

Object Access

Audit 'Removable Storage' is set to 'Success and Failure'

Logon/Logoff

Audit 'Account Lockout' is set to 'Success and Failure'

Audit 'Group Membership' is set to 'Success'

Audit 'Logoff' is set to 'Success'

Audit 'Logon' is set to 'Success and Failure'

Audit 'Other Logon/Logoff Events' is set to 'Success and Failure'

Audit 'Special Logon' is set to 'Success'

Detailed Tracking

Audit 'PNP Activity' is set to 'Success'

Audit 'Process Creation' is set to 'Success'

Account Management

Audit 'Application Group Management' is set to 'Success and Failure'

Audit 'Computer Account Management' is set to 'Success and Failure'

Audit 'Other Account Management Events' is set to 'Success and Failure'

Audit 'Security Group Management' is set to 'Success and Failure'

Audit 'User Account Management' is set to 'Success and Failure'

Account Logon

Ensure 'Audit Credential Validation' is set to 'Success and Failure'

4. Use Local Administrator Password Solutions LDAPS

5. Scripts:

- # Cceld: CCE-36326-7

DataSource: Registry Policy

Network security: Do not store LAN Manager hash value on next password change

Network_security_Do_not_store_LAN_Manager_hash_value_on_next_password_change
= 'Enabled'

pause

- # Cceld: CCE-36858-9

DataSource: Registry Policy

Network security: LDAP client signing requirements

Network_security_LDAP_client_signing_requirements = 'Negotiate Signing'

- Node \$ComputerName {

- AccountPolicy AccountPolicies

- {

- Name = 'PasswordPolicies'

-

- # Cceld: CCE-37166-6

- # DataSource: Security Policy

- # Ensure 'Enforce password history' is set to '24 or more password'

- Enforce_password_history = 24

-

- # Cceld: CCE-37167-4

- # DataSource: Security Policy

- # Ensure 'Maximum password age' is set to '70 or fewer days, but not 0'

- Maximum_Password_Age = 70

-

- # Cceld: CCE-37073-4

- # DataSource: Security Policy

- # Ensure 'Minimum password age' is set to '1 or more day'

- Minimum_Password_Age = 1

-

- # Cceld: CCE-36534-6

- # DataSource: Security Policy

- # Ensure 'Minimum password length' is set to '14 or more character'

- Minimum_Password_Length = 14

-

- # Cceld: CCE-37063-5

- # DataSource: Security Policy

- # Ensure 'Password must meet complexity requirements' is set to 'Enabled'

- Password_must_meet_complexity_requirements = 'Enabled'

-


```

-      # Cceld: CCE-36286-3
-      # DataSource: Security Policy
-      # Ensure 'Store passwords using reversible encryption' is set to 'Disabled'
-      Store_passwords_using_reversible_encryption = 'Disabled'
-    }
-  pause

-  # Cceld: CCE-35818-4
-  # DataSource: Security Policy
-  # Configure 'Access this computer from the network'
-  UserRightsAssignment Accessthiscomputerfromthenetwork {
-    Policy    = 'Access_this_computer_from_the_network'
-    Identity   = 'Administrators, Authenticated Users, Backup Operators'
-  }
-  pause

-  # Cceld: CCE-37072-6
-  # DataSource: Security Policy
-  # Configure 'Allow log on through Remote Desktop Services'
-  UserRightsAssignment AllowlogonthroughRemoteDesktopServices {
-    Policy    = 'Allow_log_on_through_Remote_Desktop_Services'
-    Identity   = 'Administrators, Remote Desktop Users'
-  }
-  Pause

-  # Cceld: CCE-37659-0
-  # DataSource: Security Policy
-  # Ensure 'Allow log on locally' is set to 'Administrators'
-  UserRightsAssignment Allowlogonlocally {
-    Policy    = 'Allow_log_on_locally'
-    Identity   = 'Administrators'
-  }
-  pause

-  # Cceld: CCE-37954-5
-  # DataSource: Security Policy
-  # Configure 'Deny access to this computer from the network'
-  UserRightsAssignment Denyaccesstothiscomputerfromthenetwork {
-    Policy    = 'Deny_access_to_this_computer_from_the_network'
-    Identity   = 'Guests'
-  }
-  pause

-  # Cceld: CCE-36860-5

```

```

-      # DataSource: Security Policy
-      # Configure 'Enable computer and user accounts to be trusted for delegation'
-      UserRightsAssignment
Enablecomputeranduseraccountstobetrustedfordelegation {
-      Policy      =
'Enable_computer_and_user_accounts_to_be_trusted_for_delegation'
-      Identity    = ""
-      }
-      pause

-      # Cceld: CCE-35906-7
-      # DataSource: Security Policy
-      # Configure 'Manage auditing and security log'
-      UserRightsAssignment Manageauditingandsecuritylog {
-      Policy      = 'Manage_auditing_and_security_log'
-      Identity    = 'Administrators'
-      }
-      pause

-      # Cceld: CCE-37056-9
-      # DataSource: Security Policy
-      # Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'
-      UserRightsAssignment AccessCredentialManerasatrustedcaller {
-      Policy      = 'Access_Credential_Manager_as_a_trusted_caller'
-      Identity    = ""
-      }
-      pause

-      # Cceld: CCE-35912-5
-      # DataSource: Security Policy
-      # Ensure 'Back up files and directories' is set to 'Administrators'
-      UserRightsAssignment Backupfilesanddirectories {
-      Policy      = 'Back_up_files_and_directories'
-      Identity    = 'Administrators,Backup Operators'
-      }
-      pause

-      # Cceld: CCE-37452-0
-      # DataSource: Security Policy
-      # Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'
-      UserRightsAssignment Changethesystemtime {
-      Policy      = 'Change_the_system_time'
-      Identity    = 'Administrators, LOCAL SERVICE'
-      }

```

- pause
- # Cceld: CCE-37700-2
 - # DataSource: Security Policy
 - # Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'
 - UserRightsAssignment Changethetimezone {
 - Policy = 'Change_the_time_zone'
 - Identity = 'Administrators, LOCAL SERVICE'
 - }
 - pause
- # Cceld: CCE-35821-8
 - # DataSource: Security Policy
 - # Ensure 'Create a pagefile' is set to 'Administrators'
 - UserRightsAssignment Createapagefile {
 - Policy = 'Create_a_pagefile'
 - Identity = 'Administrators'
 - }
 - pause
- # Cceld: CCE-36861-3
 - # DataSource: Security Policy
 - # Ensure 'Create a token object' is set to 'No One'
 - UserRightsAssignment Createatokenobject {
 - Policy = 'Create_a_token_object'
 - Identity = ''
 - }
 - pause
- # Cceld: CCE-37453-8
 - # DataSource: Security Policy
 - # Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'
 - UserRightsAssignment Createglobalobjects {
 - Policy = 'Create_global_objects'
 - Identity = 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'
 - }
 - pause
- # Cceld: CCE-36532-0
 - # DataSource: Security Policy
 - # Ensure 'Create permanent shared objects' is set to 'No One'
 - UserRightsAssignment Createpermanentsharedobjects {

```

-         Policy    = 'Create_permanent_shared_objects'
-         Identity   = ""
-     }
- pause

- # Cceld: CCE-36923-1
-     # DataSource: Security Policy
-     # Ensure 'Deny log on as a batch job' to include 'Guests'
-     UserRightsAssignment Denylogonasabatchjob {
-         Policy    = 'Deny_log_on_as_a_batch_job'
-         Identity   = 'Guests'
-     }
- pause

- Cceld: CCE-36867-0
-     # DataSource: Security Policy
-     # Ensure 'Deny log on through Remote Desktop Services' to include 'Guests'
-     UserRightsAssignment DenylogonthroughRemoteDesktopServices {
-         Policy    = 'Deny_log_on_through_Remote_Desktop_Services'
-         Identity   = 'Guests'
-     }
- pause

- # Cceld: CCE-37877-8
-     # DataSource: Security Policy
-     # Ensure 'Force shutdown from a remote system' is set to 'Administrators'
-     UserRightsAssignment Forceshutdownfromaremoteyesystem {
-         Policy    = 'Force_shutdown_from_a_remote_system'
-         Identity   = 'Administrators'
-     }
- pause

- # Cceld: CCE-36318-4
-     # DataSource: Security Policy
-     # Ensure 'Load and unload device drivers' is set to 'Administrators'
-     UserRightsAssignment Loadandunloaddevicedrivers {
-         Policy    = 'Load_and_unload_device_drivers'
-         Identity   = 'Administrators'
-     }
- pause

- # Cceld: CCE-37430-6
-     # DataSource: Security Policy

```

- # Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'
- UserRightsAssignment Replaceaprocesstoken {
- Policy = 'Replace_a_process_level_token'
- Identity = 'LOCAL SERVICE, NETWORK SERVICE'
- }
- pause

- # Ccld: CCE-38328-1
- # DataSource: Security Policy
- # Ensure 'Shut down the system' is set to 'Administrators'
- UserRightsAssignment Shutdownthesystem {
- Policy = 'Shut_down_the_system'
- Identity = 'Administrators'
- }
- pause

- # Ccld: CCE-38325-7
- # DataSource: Security Policy
- # Ensure 'Take ownership of files or other objects' is set to 'Administrators'
- UserRightsAssignment Takeownershipoffilesorotherobjects {
- Policy = 'Take_ownership_of_files_or_other_objects'
- Identity = 'Administrators'
- }
- pause

- # Ccld: CCE-38329-9
- # DataSource: Audit Policy
- # Ensure 'Audit Application Group Management' is set to 'Success and Failure'
- AuditPolicySubcategory 'Audit Application Group Management (Success)'
- {
- Name = 'Application Group Management'
- AuditFlag = 'Success'
- Ensure = 'Absent'
- }
- pause

- AuditPolicySubcategory 'Audit Application Group Management (Failure)'
- {
- Name = 'Application Group Management'
- AuditFlag = 'Failure'
- Ensure = 'Absent'

```

-     }
- pause

- # Cceld: CCE-37741-6
-     # DataSource: Audit Policy
-     # Audit Policy: Account Logon: Credential Validation
-     AuditPolicySubcategory "Audit Credential Validation (Success)"
-     {
-         Name     = 'Credential Validation'
-         AuditFlag = 'Success'
-         Ensure    = 'Present'
-     }
- pause

-     AuditPolicySubcategory 'Audit Credential Validation (Failure)'
-     {
-         Name     = 'Credential Validation'
-         AuditFlag = 'Failure'
-         Ensure    = 'Present'
-     }
- pause

- # Cceld: CCE-38237-4
-     # DataSource: Audit Policy
-     # EAudit Policy: Logon-Logoff: Logoff
-     AuditPolicySubcategory 'Audit Logoff (Success)'
-     {
-         Name     = 'Logoff'
-         AuditFlag = 'Success'
-         Ensure    = 'Present'
-     }
- pause

-     AuditPolicySubcategory 'Audit Logoff (Failure)'
-     {
-         Name     = 'Logoff'
-         AuditFlag = 'Failure'
-         Ensure    = 'Absent'
-     }
- pause

- # Cceld: CCE-38036-0
-     # DataSource: Audit Policy
-     # Audit Policy: Logon-Logoff: Logon

```

```

-     AuditPolicySubcategory 'Audit Logon (Success)'
-     {
-         Name    = 'Logon'
-         AuditFlag = 'Success'
-         Ensure   = 'Present'
-     }
- pause

-     AuditPolicySubcategory 'Audit Logon (Failure)'
-     {
-         Name    = 'Logon'
-         AuditFlag = 'Failure'
-         Ensure   = 'Present'
-     }
- pause

- # Cceld: CCE-37855-4
-     # DataSource: Audit Policy
-     # Audit Policy: Account Management: Other Account Management Events
-     AuditPolicySubcategory 'Audit Other Account Management Events (Success)'
-     {
-         Name    = 'Other Account Management Events'
-         AuditFlag = 'Success'
-         Ensure   = 'Present'
-     }
- pause

-     AuditPolicySubcategory 'Audit Other Account Management Events (Failure)'
-     {
-         Name    = 'Other Account Management Events'
-         AuditFlag = 'Failure'
-         Ensure   = 'Absent'
-     }
- pause

- # Cceld: CCE-36059-4
-     # DataSource: Audit Policy
-     # Audit Policy: Detailed Tracking: Process Creation
-     AuditPolicySubcategory 'Audit Process Creation (Success)'
-     {
-         Name    = 'Process Creation'
-         AuditFlag = 'Success'
-         Ensure   = 'Present'
-     }

```

```

- pause

- AuditPolicySubcategory 'Audit Process Creation (Failure)'
- {
-     Name    = 'Process Creation'
-     AuditFlag = 'Failure'
-     Ensure   = 'Absent'
- }
- pause
- Cceld: CCE-38034-5
-     # DataSource: Audit Policy
-     # Audit Policy: Account Management: Security Group Management
-     AuditPolicySubcategory 'Audit Security Group Management (Success)'
-     {
-         Name    = 'Security Group Management'
-         AuditFlag = 'Success'
-         Ensure   = 'Present'
-     }
- pause

- AuditPolicySubcategory 'Audit Security Group Management (Failure)'
-     {
-         Name    = 'Security Group Management'
-         AuditFlag = 'Failure'
-         Ensure   = 'Absent'
-     }
- pause

- # Cceld: CCE-36266-5
-     # DataSource: Audit Policy
-     # Audit Policy: Logon-Logoff: Special Logon
-     AuditPolicySubcategory 'Audit Special Logon (Success)'
-     {
-         Name    = 'Special Logon'
-         AuditFlag = 'Success'
-         Ensure   = 'Present'
-     }
- pause

- AuditPolicySubcategory 'Audit Special Logon (Failure)'
-     {
-         Name    = 'Special Logon'
-         AuditFlag = 'Failure'
-         Ensure   = 'Absent'

```



```

-     }
- pause

- # Cceld: CCE-37856-2
-   # DataSource: Audit Policy
-   # Audit Policy: Account Management: User Account Management
-   AuditPolicySubcategory 'Audit User Account Management (Success)'
-   {
-       Name      = 'User Account Management'
-       AuditFlag = 'Success'
-       Ensure    = 'Present'
-   }
- pause

-   AuditPolicySubcategory 'Audit User Account Management (Failure)'
-   {
-       Name      = 'User Account Management'
-       AuditFlag = 'Failure'
-       Ensure    = 'Present'
-   }
- pause

- # Control no: AZ-WIN-00112
-   # DataSource: Audit Policy
-   # Audit Non Sensitive Privilege Use
-   AuditPolicySubcategory 'Audit Non Sensitive Privilege Use (Success)'
-   {
-       Name      = 'Non Sensitive Privilege Use'
-       AuditFlag = 'Success'
-       Ensure    = 'Absent'
-   }
- pause

-   AuditPolicySubcategory 'Audit Non Sensitive Privilege Use (Failure)'
-   {
-       Name      = 'Non Sensitive Privilege Use'
-       AuditFlag = 'Failure'
-       Ensure    = 'Absent'
-   }
- pause

- # Cceld: CCE-38327-3
-   # DataSource: Audit Policy
-   # Audit Policy: Policy Change: Authentication Policy Change

```

- **AuditPolicySubcategory 'Audit Authentication Policy Change (Success)' {**
- **Name = 'Authentication Policy Change'**
- **Ensure = 'Present'**
- **AuditFlag = 'Success'**
- **}**
- **pause**

- **AuditPolicySubcategory 'Audit Authentication Policy Change (Failure)' {**
- **Name = 'Authentication Policy Change'**
- **Ensure = 'Absent'**
- **AuditFlag = 'Failure'**
- **}**
- **pause**

- **# Cceld: CCE-38114-5**
- **# DataSource: Audit Policy**
- **# Audit Policy: System: Security State Change**
- **AuditPolicySubcategory 'Audit Security State Change (Success)' {**
- **Name = 'Security State Change'**
- **Ensure = 'Present'**
- **AuditFlag = 'Success'**
- **}**
- **pause**

- **AuditPolicySubcategory 'Audit Security State Change (Failure)' {**
- **Name = 'Security State Change'**
- **Ensure = 'Absent'**
- **AuditFlag = 'Failure'**
- **}**
- **pause**

- **# Cceld: CCE-38028-7**
- **# DataSource: Audit Policy**
- **# Audit Policy: Policy Change: Audit Policy Change**
- **AuditPolicySubcategory 'Audit Policy Change (Success)'**
- **{**
- **Name = 'Audit Policy Change'**
- **AuditFlag = 'Success'**
- **Ensure = 'Present'**
- **}**
- **pause**

- **AuditPolicySubcategory 'Audit Policy Change (Failure)'**
- **{**

```

-      Name    = 'Audit Policy Change'
-      AuditFlag = 'Failure'
-      Ensure   = 'Present'
-    }
-  pause

-  # Cceld: CCE-37853-9
-    # DataSource: Audit Policy
-    # Audit Policy: System: IPsec Driver
-    AuditPolicySubcategory 'Audit IPsec Driver (Failure)' {
-      Name    = 'IPsec Driver'
-      Ensure   = 'Present'
-      AuditFlag = 'Failure'
-    }
-  pause

-  AuditPolicySubcategory 'Audit IPsec Driver (Success)' {
-    Name    = 'IPsec Driver'
-    Ensure   = 'Present'
-    AuditFlag = 'Success'
-  }
-  pause

-  # Cceld: CCE-38030-3
-    # DataSource: Audit Policy
-    # Audit Policy: System: Other System Events
-    AuditPolicySubcategory 'Audit Other System Events (Failure)'
-    {
-      Name    = 'Other System Events'
-      AuditFlag = 'Failure'
-      Ensure   = 'Present'
-    }
-  pause

-  # Cceld: CCE-36322-6
-    # DataSource: Audit Policy
-    # Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'
-    AuditPolicySubcategory 'Audit Other Logon/Logoff Events (Failure)' {
-      Name    = 'Other Logon/Logoff Events'
-      Ensure   = 'Present'
-      AuditFlag = 'Failure'
-    }
-  pause

```

```

-   AuditPolicySubcategory 'Audit Other Logon/Logoff Events (Success)' {
-       Name    = 'Other Logon/Logoff Events'
-       Ensure   = 'Present'
-       AuditFlag = 'Success'
-   }
-   pause

-   # Cceld: CCE-37133-6
-       # DataSource: Audit Policy
-       # Audit Policy: Logon-Logoff: Account Lockout
-       AuditPolicySubcategory 'Audit Account Lockout (Success)' {
-           Name    = 'Account Lockout'
-           Ensure   = 'Present'
-           AuditFlag = 'Success'
-       }
-   pause

-   AuditPolicySubcategory 'Audit Account Lockout (Failure)' {
-       Name    = 'Account Lockout'
-       Ensure   = 'Present'
-       AuditFlag = 'Failure'
-   }
-   pause

-   # Cceld: CCE-36320-0
-       # DataSource: Audit Policy
-       # Ensure 'Audit Authorization Policy Change' is set to 'Success'
-       AuditPolicySubcategory 'Audit Authorization Policy Change (Success)' {
-           Name    = 'Authorization Policy Change'
-           Ensure   = 'Present'
-           AuditFlag = 'Success'
-       }
-
-       AuditPolicySubcategory 'Audit Authorization Policy Change (Failure)' {
-           Name    = 'Authorization Policy Change'
-           Ensure   = 'Absent'
-           AuditFlag = 'Failure'
-       }
-   pause

-   # Cceld: CCE-36267-3
-       # DataSource: Audit Policy
-       # Audit Policy: Privilege Use: Sensitive Privilege Use
-       AuditPolicySubcategory 'Audit Sensitive Privilege Use (Failure)' {

```

```

-      Name    = 'Sensitive Privilege Use'
-      Ensure   = 'Present'
-      AuditFlag = 'Failure'
-    }
-
-    AuditPolicySubcategory 'Audit Sensitive Privilege Use (Success)' {
-      Name    = 'Sensitive Privilege Use'
-      Ensure   = 'Present'
-      AuditFlag = 'Success'
-    }
-  pause

-  # Control no: AZ-WIN-00105
-  # DataSource: Audit Policy
-  # Audit Filtering Platform Packet Drop
-  AuditPolicySubcategory 'Audit Filtering Platform Packet Drop (Success)'
-  {
-    Name    = 'Filtering Platform Packet Drop'
-    AuditFlag = 'Success'
-    Ensure   = 'Absent'
-  }
-
-  AuditPolicySubcategory 'Audit Filtering Platform Packet Drop (Failure)'
-  {
-    Name    = 'Filtering Platform Packet Drop'
-    AuditFlag = 'Failure'
-    Ensure   = 'Absent'
-  }
-  pause

-  # Control no: AZ-WIN-00006
-  # DataSource: Audit Policy
-  # Audit Other Account Logon Events
-  AuditPolicySubcategory "Audit Other Account Logon Events (Success)"
-  {
-    Name    = 'Other Account Logon Events'
-    AuditFlag = 'Success'
-    Ensure   = 'Present'
-  }
-
-  AuditPolicySubcategory 'Other Account Logon Events (Failure)'
-  {
-    Name    = 'Other Account Logon Events'
-    AuditFlag = 'Failure'

```

```

-         Ensure    = 'Present'
-     }
- pause

-     # Control no: AZ-WIN-00115
-     # DataSource: Audit Policy
-     # Audit Registry
-     AuditPolicySubcategory 'Audit Registry (Success)'
-     {
-         Name      = 'Registry'
-         AuditFlag = 'Success'
-         Ensure    = 'Present'
-     }
- pause

-     # Cceld: CCE-36512-2
-     # DataSource: Registry Policy
-     # Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'
-     Registry 'EnumerateAdministrators' {
-         Ensure    = 'Present'
-         Key       =
'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
\CredUI'
-         ValueName = 'EnumerateAdministrators'
-         ValueType = 'DWord'
-         ValueData  = '0'
-     }
- pause

-     # Cceld: CCE-36400-0
-     # DataSource: Registry Policy
-     # Ensure 'Allow user control over installs' is set to 'Disabled'
-     Registry 'EnableUserControl' {
-         Ensure    = 'Present'
-         Key       =
'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer'
-         ValueName = 'EnableUserControl'
-         ValueType = 'DWord'
-         ValueData  = '0'
-     }
- pause

-     # Cceld: CCE-38223-4
-     # DataSource: Registry Policy

```

```

-      # Ensure 'Allow unencrypted traffic' is set to 'Disabled'
-      Registry 'AllowUnencryptedTraffic' {
-          Ensure    = 'Present'
-          Key       =
-          'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client'
-          ValueName = 'AllowUnencryptedTraffic'
-          ValueType = 'DWord'
-          ValueData = '0'
-      }
-      pause

-      # Cceld: CCE-37490-0
-      # DataSource: Registry Policy
-      # Ensure 'Always install with elevated privileges' is set to 'Disabled'
-      Registry 'AlwaysInstallElevated' {
-          Ensure    = 'Present'
-          Key       =
-          'HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer'
-          ValueName = 'AlwaysInstallElevated'
-          ValueType = 'DWord'
-          ValueData = '0'
-      }
-      pause

-      # Cceld: CCE-36223-6
-      # DataSource: Registry Policy
-      # Ensure 'Do not allow passwords to be saved' is set to 'Enabled'
-      Registry 'DisablePasswordSaving' {
-          Ensure    = 'Present'
-          Key       =
-          'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services'
-          ValueName = 'DisablePasswordSaving'
-          ValueType = 'DWord'
-          ValueData = '1'
-      }
-      pause

-      # Cceld: CCE-36627-8
-      # DataSource: Registry Policy
-      # Ensure 'Set client connection encryption level' is set to 'Enabled: High
Level'
-      Registry 'MinEncryptionLevel' {
-          Ensure    = 'Present'

```

```

-         Key      =
'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services'
-         ValueName = 'MinEncryptionLevel'
-         ValueType = 'DWord'
-         ValueData = '3'
-     }
- pause

- # Cceld: CCE-37695-4
- # DataSource: Registry Policy
- # Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled:
196,608 or greater'
-     Registry 'MaxSizeSecurityLog' {
-         Ensure = 'Present'
-         Key      =
'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Secu
rity'
-         ValueName = 'MaxSize'
-         ValueType = 'DWord'
-         ValueData = '196608'
-     }
- pause

```