Windows Server AD/DNS Playbook

By Nicolas Langenfeld (Updated Nathan Campbell SP2024)

* Microsoft Active Directory
* Microsoft DNS
* Windows Firewall

This playbook is designed to provide the resources to generally secure a windows server as well as secure AD and DNS.

The IP addresses in this document are for the hardware network! If configuring a server in the virtual network be sure to adjust!

Plan of Action

1. Passwords and accounts
2. Install Firefox
3. Run script from GitHub (and do additional steps)
4. Start loading updates
5. Back up DNS
6. Install & configure Splunk universal forwarder
7. Install wireshark

10. Monitor & Observe

1. **Accounts:**

**Change password**: Computer management > Local Users & Groups > Users > Right-click user

* Remove non-critical users from groups:
  + Domain Admins
  + Enterprise Admins
  + Administrators
  + Schema Admins
  + Disable users
    - Greg
    - Test
    - Pro mon

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service | User | Default Pass | New Pass | Groups |
| Windows | Administrator | !changeme123 |  | Administrators |
| Splunk Forwarder | Win2012spf |  |  |  |

1. **Fix DNS on NIC and forwarders**
   1. Run dnsmgmt.msc or go to server manager > tools > DNS
   2. Right click DNS name and click properties > forwarders
   3. Set 172.20.240.23 9.9.9.9 on forwarder
   4. Change DNS 127.0.0.1 on NIC
2. **Install Edge as IE is the only browser preinstalled**
   1. **You may need to let the site through in settings > internet options > security**
   2. **Start with edge and if that does not work, go to Firefox, then Chrome**
3. **Check for updates and/or run latest security update manually, restart**
   1. If Windows Update is broken, vist the Windows Update Catolog <https://www.catalog.update.microsoft.com/Home.aspx>
4. **Run windows\_baseline.bat from github**
   1. Go to <https://github.com/UWStout-CCDC/CCDC-scripts-2020/windows> and under windows, copy the text of windows\_baseline.bat to a notepad and save as a .bat file. (or wget https://raw.githubusercontent.com/UWStout-CCDC/CCDC-scripts-2020/master/windows)
   2. If you have the option, right click and run as administrator.
      1. Or int the search bar type run and then click the browse button and find the file you created.
   3. Check that firewall rules applied.
      1. Disable non-custom rules (if any)
   4. Re-enable SMB2 (required for GP Management console)
      1. Set-SmbServerConfiguration -EnableSMB2Protocol $true -Force
   5. Check security event logs to make sure Audits are logging. Set up auditing in GP if necessary.
   6. Disable RDS services in services.msc and Control panel
   7. Disable network discovery and File and Printer sharing
5. **Back up DNS**
   1. Back up DNS – stored in %systemroot%/System32/Dns
      1. dnscmd.exe /ZoneExport <ZoneName> <ZoneBackupFilename>
6. **Install Splunk Forwarder**
   1. Run MSI and follow steps. Enter below information for the deployment server

IP: 172.20.241.20

Port: 8089

1. **Install Wireshark from wireshark.org**
2. **Backup GPO** 
   1. Go to Group policy managemnet from tools.
   2. Under Forest > Domains > (domain Name) > Group Policy Objects > defulat Domain Policy. Right click and select Backup
3. Install anti**virus**
   1. Microsoft Security Essentials or Clam AV
4. **Check updates and restart**

Firewall:

* Use policy file or manually set firewall rules (at end of document)
* Server IP: 172.20.241.27
* Check listening ports (powershell):
  + Get-NetTCPConnection -State Listen,Established

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Port** | **IP** | **Type** |
| DNS | 53 | Any | TCP & UDP |
| LDAP  System32/lsass.exe | 389 | Any | TCP & UDP |
| LDAP Global  System32/lsass.exe | 3268 | Any | TCP |
| NetBIOS name resolution | 138 | Any | UDP |
| SAM/LSA | 445 | Any | TCP & UDP |
| Secure LDAP  Lsass.exe | 636 | Any | TCP |
| Secure LDAP Global  Lsass.exe | 3269 | Any | TCP |
| Time  Svhost.exe | 123 | Any | UDP |
| RPC  Lsass.exe | RPC Dynamic Ports | Any | TCP |
| RPC EPMAP | RPC Endpoint mapper | Any | TCP |
| DHCP | 67,68 | Any | UDP |
| **OUTBOUND** | | | |
| DNS | 53 | Any | TCP & UDP |
| Web | 80, 443 | Any | TCP |
| Splunk | 8000, 8089, 9997 | 172.20.241.20 | TCP |
| Time/NTP | 123 | 172.20.240.20 | UDP |
| Ping | Any ICMP | Any | ICMPv4 |

* Manually [disable SMB 1 via Powershell](https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3):
  + SMB2 is required for Group Policy Management to work for some reason. Can be disabled after GPO updates maybe?

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Set-SmbServerConfiguration -EnableSMB1Protocol $false

sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi

sc.exe config mrxsmb10 start= disabled

**Check Status:**

Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Get-SmbServerConfiguration | Select EnableSMB1Protocol

Get-SmbServerConfiguration | Select EnableSMB2Protocol

sc.exe qc lanmanworkstation

**Securing DNS**

* Enable DNS Zone signing with default settings
* Protect from DNS spoofing by increasing socket pool
  + From CMD: dnscmd /Config /SocketPoolSize 10000
* Ensure cache locking is set to maximum
  + dnscmd /Config /CacheLockingPercent 100
* Back up DNS – stored in %systemroot%/System32/Dns
  + dnscmd.exe /ZoneExport <ZoneName> <ZoneBackupFilename>\

[**Securing Active Directory**](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory)

* Built In administrator accounts
  + Enable the "Account is sensitive and cannot be delegated" flag
* Create GPO that applies to domain
  + Set password policies
    - Computer config>Policies>Windows>Security>Account>Password
    - Computer config>Policies>Windows>Security>Account>Account Lockout
  + Disable Remote Desktop
    - Computer config>Policies>Windows>Security>Local>User Rights
      * Deny log on through remote Desktop Services
        + Add Users Group
* Create GPO that applies to Domain Controllers and Workstation OUs
  + add each domain's Administrator account, Enterprise Admins Group, Domain Admins Group, and Administrators Group to:
    - Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignments:
      * Deny log on as a batch job
      * Deny log on through Remote Desktop Services
* At the domain controllers OU in each domain in the forest, the Administrators group should be granted the following user rights (if they do not already have these rights):
  + Allow log on locally
* Remove non-critical users from groups:
  + Domain Admins
  + Enterprise Admins
  + Schema Admins
  + Administrators
* Check for and disable rogue accounts
* Enable file system and registry auditing (optional)
  + In domain GPO
    - Computer>Windows>Security> Advanced Audit> Global Object Access
      * Configure file system and/or Registry resources
    - Computer>Windows>Security> Advanced Audit>Object Access
      * Configure Audit File System and Audit Registry

**Checking Logs**

* Logs stored in Windows\System32\winevt\Logs
* Use Event Viewer or Server Manager to view logs
  + System
  + Security
  + Application
* Install Wireshark to monitor network traffic

**Checking Processes (powershell)**

* View running processes: Get-Process
* Kill processes
  + By name: Stop-Process -name <application name>
  + By ID: Stop-Process -Id <processID>

**Useful Commands & Tools**

* Kill all NICs powershell: Get-NetAdapter | Disable-NetAdapter
* Get all AD users: Get-AdUser -Filter \* | select name

**Firewall Rules (command prompt)**

set ccdcpath="c:\ccdc"

mkdir %ccdcpath% >NUL

icacls %ccdcpath% /inheritancelevel:e >NUL

mkdir %ccdcpath%\ThreatHunting >NUL

mkdir %ccdcpath%\Config >NUL

mkdir %ccdcpath%\Regback >NUL

mkdir %ccdcpath%\Proof >NUL

:: Set IP Addresses

set EComm=172.20.241.30

set DNSNTP=172.20.240.20

set WebMail=172.20.241.40

set Splunk=172.20.241.20

set ADDNS=172.20.242.200

set PAMI=172.20.242.150

set 2016Docker=172.20.240.10

set UbuntuWeb=172.20.242.10

set UbuntuWkst=172.20.242.100

set Internal=%Ecomm%,%DNSNTP%,%WebMail%,%Splunk%,%ADDNS%,%UbuntuWkst%,%PAMI%,%2016Docker%,%UbuntuWeb%

:: Export exisiting Firewall

netsh advfirewall export %ccdcpath%\firewall.old

netsh advfirewall set allprofiles state on

:: Block by default

netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound

netsh advfirewall set allprofiles settings inboundusernotification enable

:: Enable Logging

netsh advfirewall set allprofiles logging filename %ccdcpath%\pfirewall.log

netsh advfirewall set allprofiles logging maxfilesize 8192

netsh advfirewall set allprofiles logging droppedconnections enable

netsh advfirewall set allprofiles logging allowedconnections enable

netsh advfirewall set global statefulftp disable

netsh advfirewall set global statefulpptp disable

::Disable existing rules

netsh advfirewall firewall set rule name=all new enable=no

::Outbound rules

netsh advfirewall firewall add rule name="Allow Pings out" dir=out action=allow enable=yes protocol=icmpv4:8,any

netsh advfirewall firewall add rule name="Splunk OUT" dir=out action=allow enable=yes profile=any remoteip=%Splunk% remoteport=8000,8089,9997 protocol=tcp

netsh advfirewall firewall add rule name="Web OUT" dir=out action=allow enable=yes profile=any remoteport=80,443 protocol=tcp

netsh advfirewall firewall add rule name="NTP OUT" dir=out action=allow enable=yes profile=any remoteport=123 remoteip=any protocol=udp

netsh advfirewall firewall add rule name="Active Directory TCP OUT" dir=out action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any remoteport=any remoteip=any protocol=tcp

netsh advfirewall firewall add rule name="Active Directory UDP OUT" dir=out action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any remoteport=any remoteip=any protocol=udp

netsh advfirewall firewall add rule name="DNS TCP OUT" dir=out action=allow program="C:\Windows\System32\dns.exe" enable=yes profile=any remoteport=any remoteip=any protocol=tcp

netsh advfirewall firewall add rule name="DNS UDP OUT" dir=out action=allow program="C:\Windows\System32\dns.exe" enable=yes profile=any remoteport=any remoteip=any protocol=udp

netsh advfirewall firewall add rule name="DNS OUT" dir=out action=allow enable=yes profile=any remoteport=53 protocol=udp remoteip=%DNSNTP%,9.9.9.9

netsh advfirewall firewall add rule name="DHCP" dir=out action=allow program="C:\Windows\System32\svhost.exe" enable=yes profile=any localport=68 remoteport=67 remoteip=any protocol=udp

::Inbound rules

netsh advfirewall firewall add rule name="NTP in" dir=in action=allow enable=yes profile=any localport=123 remoteip=any protocol=udp

netsh advfirewall firewall add rule name="Allow Pings in" dir=in action=allow enable=yes protocol=icmpv4:8,any

netsh advfirewall firewall add rule name="DNS IN (UDP)" dir=in action=allow enable=yes profile=any localport=53 protocol=udp

netsh advfirewall firewall add rule name="DNS IN (TDP)" dir=in action=allow enable=yes profile=any localport=53 protocol=tcp

netsh advfirewall firewall add rule name="LDAP TCP IN" dir=in action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any localport=389 protocol=tcp

netsh advfirewall firewall add rule name="LDAP UDP IN" dir=in action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any localport=389 protocol=udp

netsh advfirewall firewall add rule name="LDAP Global Catalog IN" dir=in action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any localport=3268 protocol=tcp

netsh advfirewall firewall add rule name="NETBIOS Resolution IN" dir=in action=allow program="System" enable=yes profile=any localport=138 protocol=udp

netsh advfirewall firewall add rule name="SAM/LSA TCP In" dir=in action=allow program="System" enable=yes profile=any localport=445 protocol=tcp

netsh advfirewall firewall add rule name="SAM/LSA UDP In" dir=in action=allow program="System" enable=yes profile=any localport=445 protocol=udp

netsh advfirewall firewall add rule name="Secure LDAP IN" dir=in action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any localport=636 protocol=tcp

netsh advfirewall firewall add rule name="Secure LDAP Global Catalog IN" dir=in action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any localport=3269 protocol=tcp

netsh advfirewall firewall add rule name="RPC IN" dir=in action=allow program="C:\Windows\System32\lsass.exe" enable=yes profile=any localport=RPC protocol=tcp

netsh advfirewall firewall add rule name="RPC-EPMAP IN" dir=in action=allow program="C:\Windows\System32\svhost.exe" enable=yes profile=any localport=RPC-EPMap protocol=tcp

netsh advfirewall firewall add rule name="DHCP UDP IN" dir=in action=allow program="C:\Windows\System32\svhost.exe" enable=yes profile=any localport=67,68 protocol=udp

netsh advfirewall firewall add rule name="RPC for DNS IN" dir=in action=allow program="C:\Windows\System32\dns.exe" enable=yes profile=any localport=RPC protocol=tcp

:: Diable IPv6 Teredo tunneling

netsh interface teredo set state disabled

netsh interface ipv6 6to4 set state state=disabled undoonstop=disabled

netsh interface ipv6 isatap set state state=disabled

Get to event viewer by typing eventvwr

| **Current Windows Event ID** | **Legacy Windows Event ID** | **Potential Criticality** | **Event Summary** |
| --- | --- | --- | --- |
| 4618 | N/A | High | A monitored security event pattern has occurred. |
| 4649 | N/A | High | A replay attack was detected. May be a harmless false positive due to misconfiguration error. |
| 4719 | 612 | High | System audit policy was changed. |
| 4765 | N/A | High | SID History was added to an account. |
| 4766 | N/A | High | An attempt to add SID History to an account failed. |
| 4794 | N/A | High | An attempt was made to set the Directory Services Restore Mode. |
| 4897 | 801 | High | Role separation enabled: |
| 4964 | N/A | High | Special groups have been assigned to a new logon. |
| 5124 | N/A | High | A security setting was updated on the OCSP Responder Service |
| N/A | 550 | Medium to High | Possible denial-of-service (DoS) attack |
| 1102 | 517 | Medium to High | The audit log was cleared |
| 4621 | N/A | Medium | Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded. |
| 4675 | N/A | Medium | SIDs were filtered. |
| 4692 | N/A | Medium | Backup of data protection master key was attempted. |
| 4693 | N/A | Medium | Recovery of data protection master key was attempted. |
| 4706 | 610 | Medium | A new trust was created to a domain. |
| 4713 | 617 | Medium | Kerberos policy was changed. |
| 4714 | 618 | Medium | Encrypted data recovery policy was changed. |
| 4715 | N/A | Medium | The audit policy (SACL) on an object was changed. |
| 4716 | 620 | Medium | Trusted domain information was modified. |
| 4724 | 628 | Medium | An attempt was made to reset an account's password. |
| 4727 | 631 | Medium | A security-enabled global group was created. |
| 4735 | 639 | Medium | A security-enabled local group was changed. |
| 4737 | 641 | Medium | A security-enabled global group was changed. |
| 4739 | 643 | Medium | Domain Policy was changed. |
| 4754 | 658 | Medium | A security-enabled universal group was created. |
| 4755 | 659 | Medium | A security-enabled universal group was changed. |
| 4764 | 667 | Medium | A security-disabled group was deleted |
| 4764 | 668 | Medium | A group's type was changed. |
| 4780 | 684 | Medium | The ACL was set on accounts which are members of administrators groups. |
| 4816 | N/A | Medium | RPC detected an integrity violation while decrypting an incoming message. |
| 4865 | N/A | Medium | A trusted forest information entry was added. |
| 4866 | N/A | Medium | A trusted forest information entry was removed. |
| 4867 | N/A | Medium | A trusted forest information entry was modified. |
| 4868 | 772 | Medium | The certificate manager denied a pending certificate request. |
| 4870 | 774 | Medium | Certificate Services revoked a certificate. |
| 4882 | 786 | Medium | The security permissions for Certificate Services changed. |
| 4885 | 789 | Medium | The audit filter for Certificate Services changed. |
| 4890 | 794 | Medium | The certificate manager settings for Certificate Services changed. |
| 4892 | 796 | Medium | A property of Certificate Services changed. |
| 4896 | 800 | Medium | One or more rows have been deleted from the certificate database. |
| 4906 | N/A | Medium | The CrashOnAuditFail value has changed. |
| 4907 | N/A | Medium | Auditing settings on object were changed. |
| 4908 | N/A | Medium | Special Groups Logon table modified. |
| 4912 | 807 | Medium | Per User Audit Policy was changed. |
| 4960 | N/A | Medium | IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations. |
| 4961 | N/A | Medium | IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer. |
| 4962 | N/A | Medium | IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay. |
| 4963 | N/A | Medium | IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt. |
| 4965 | N/A | Medium | IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored. |
| 4976 | N/A | Medium | During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. |
| 4977 | N/A | Medium | During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. |
| 4978 | N/A | Medium | During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. |
| 4983 | N/A | Medium | An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. |
| 4984 | N/A | Medium | An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. |
| 5027 | N/A | Medium | The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy. |
| 5028 | N/A | Medium | The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy. |
| 5029 | N/A | Medium | The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy. |
| 5030 | N/A | Medium | The Windows Firewall Service failed to start. |
| 5035 | N/A | Medium | The Windows Firewall Driver failed to start. |
| 5037 | N/A | Medium | The Windows Firewall Driver detected critical runtime error. Terminating. |
| 5038 | N/A | Medium | Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error. |
| 5120 | N/A | Medium | OCSP Responder Service Started |
| 5121 | N/A | Medium | OCSP Responder Service Stopped |
| 5122 | N/A | Medium | A configuration entry changed in OCSP Responder Service |
| 5123 | N/A | Medium | A configuration entry changed in OCSP Responder Service |
| 5376 | N/A | Medium | Credential Manager credentials were backed up. |
| 5377 | N/A | Medium | Credential Manager credentials were restored from a backup. |
| 5453 | N/A | Medium | An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started. |
| 5480 | N/A | Medium | IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. |
| 5483 | N/A | Medium | IPsec Services failed to initialize RPC server. IPsec Services could not be started. |
| 5484 | N/A | Medium | IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. |
| 5485 | N/A | Medium | IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. |
| 5827 | N/A | Medium | The Netlogon service denied a vulnerable Netlogon secure channel connection from a machine account. |
| 5828 | N/A | Medium | The Netlogon service denied a vulnerable Netlogon secure channel connection using a trust account. |
| 6145 | N/A | Medium | One or more errors occurred while processing security policy in the Group Policy objects. |
| 6273 | N/A | Medium | Network Policy Server denied access to a user. |
| 6274 | N/A | Medium | Network Policy Server discarded the request for a user. |
| 6275 | N/A | Medium | Network Policy Server discarded the accounting request for a user. |
| 6276 | N/A | Medium | Network Policy Server quarantined a user. |
| 6277 | N/A | Medium | Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy. |
| 6278 | N/A | Medium | Network Policy Server granted full access to a user because the host met the defined health policy. |
| 6279 | N/A | Medium | Network Policy Server locked the user account due to repeated failed authentication attempts. |
| 6280 | N/A | Medium | Network Policy Server unlocked the user account. |
| - | 640 | Medium | General account database changed |
| - | 619 | Medium | Quality of Service Policy changed |
| 24586 | N/A | Medium | An error was encountered converting volume |
| 24592 | N/A | Medium | An attempt to automatically restart conversion on volume %2 failed. |
| 24593 | N/A | Medium | Metadata write: Volume %2 returning errors while trying to modify metadata. If failures continue, decrypt volume |
| 24594 | N/A | Medium | Metadata rebuild: An attempt to write a copy of metadata on volume %2 failed and may appear as disk corruption. If failures continue, decrypt volume. |
| 4608 | 512 | Low | Windows is starting up. |
| 4609 | 513 | Low | Windows is shutting down. |
| 4610 | 514 | Low | An authentication package has been loaded by the Local Security Authority. |
| 4611 | 515 | Low | A trusted logon process has been registered with the Local Security Authority. |
| 4612 | 516 | Low | Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. |
| 4614 | 518 | Low | A notification package has been loaded by the Security Account Manager. |
| 4615 | 519 | Low | Invalid use of LPC port. |
| 4616 | 520 | Low | The system time was changed. |
| 4622 | N/A | Low | A security package has been loaded by the Local Security Authority. |
| 4624 | 528,540 | Low | An account was successfully logged on. |
| 4625 | 529-537,539 | Low | An account failed to log on. |
| 4634 | 538 | Low | An account was logged off. |
| 4646 | N/A | Low | IKE DoS-prevention mode started. |
| 4647 | 551 | Low | User initiated logoff. |
| 4648 | 552 | Low | A logon was attempted using explicit credentials. |
| 4650 | N/A | Low | An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used. |
| 4651 | N/A | Low | An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication. |
| 4652 | N/A | Low | An IPsec Main Mode negotiation failed. |
| 4653 | N/A | Low | An IPsec Main Mode negotiation failed. |
| 4654 | N/A | Low | An IPsec Quick Mode negotiation failed. |
| 4655 | N/A | Low | An IPsec Main Mode security association ended. |
| 4656 | 560 | Low | A handle to an object was requested. |
| 4657 | 567 | Low | A registry value was modified. |
| 4658 | 562 | Low | The handle to an object was closed. |
| 4659 | N/A | Low | A handle to an object was requested with intent to delete. |
| 4660 | 564 | Low | An object was deleted. |
| 4661 | 565 | Low | A handle to an object was requested. |
| 4662 | 566 | Low | An operation was performed on an object. |
| 4663 | 567 | Low | An attempt was made to access an object. |
| 4664 | N/A | Low | An attempt was made to create a hard link. |
| 4665 | N/A | Low | An attempt was made to create an application client context. |
| 4666 | N/A | Low | An application attempted an operation: |
| 4667 | N/A | Low | An application client context was deleted. |
| 4668 | N/A | Low | An application was initialized. |
| 4670 | N/A | Low | Permissions on an object were changed. |
| 4671 | N/A | Low | An application attempted to access a blocked ordinal through the TBS. |
| 4672 | 576 | Low | Special privileges assigned to new logon. |
| 4673 | 577 | Low | A privileged service was called. |
| 4674 | 578 | Low | An operation was attempted on a privileged object. |
| 4688 | 592 | Low | A new process has been created. |
| 4689 | 593 | Low | A process has exited. |
| 4690 | 594 | Low | An attempt was made to duplicate a handle to an object. |
| 4691 | 595 | Low | Indirect access to an object was requested. |
| 4694 | N/A | Low | Protection of auditable protected data was attempted. |
| 4695 | N/A | Low | Unprotection of auditable protected data was attempted. |
| 4696 | 600 | Low | A primary token was assigned to process. |
| 4697 | 601 | Low | Attempt to install a service |
| 4698 | 602 | Low | A scheduled task was created. |
| 4699 | 602 | Low | A scheduled task was deleted. |
| 4700 | 602 | Low | A scheduled task was enabled. |
| 4701 | 602 | Low | A scheduled task was disabled. |
| 4702 | 602 | Low | A scheduled task was updated. |
| 4704 | 608 | Low | A user right was assigned. |
| 4705 | 609 | Low | A user right was removed. |
| 4707 | 611 | Low | A trust to a domain was removed. |
| 4709 | N/A | Low | IPsec Services was started. |
| 4710 | N/A | Low | IPsec Services was disabled. |
| 4711 | N/A | Low | May contain any one of the following: PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine applied Active Directory storage IPsec policy on the computer. PAStore Engine applied local registry storage IPsec policy on the computer. PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply local registry storage IPsec policy on the computer. PAStore Engine failed to apply some rules of the active IPsec policy on the computer. PAStore Engine failed to load directory storage IPsec policy on the computer. PAStore Engine loaded directory storage IPsec policy on the computer. PAStore Engine failed to load local storage IPsec policy on the computer. PAStore Engine loaded local storage IPsec policy on the computer.PAStore Engine polled for changes to the active IPsec policy and detected no changes. |
| 4712 | N/A | Low | IPsec Services encountered a potentially serious failure. |
| 4717 | 621 | Low | System security access was granted to an account. |
| 4718 | 622 | Low | System security access was removed from an account. |
| 4720 | 624 | Low | A user account was created. |
| 4722 | 626 | Low | A user account was enabled. |
| 4723 | 627 | Low | An attempt was made to change an account's password. |
| 4725 | 629 | Low | A user account was disabled. |
| 4726 | 630 | Low | A user account was deleted. |
| 4728 | 632 | Low | A member was added to a security-enabled global group. |
| 4729 | 633 | Low | A member was removed from a security-enabled global group. |
| 4730 | 634 | Low | A security-enabled global group was deleted. |
| 4731 | 635 | Low | A security-enabled local group was created. |
| 4732 | 636 | Low | A member was added to a security-enabled local group. |
| 4733 | 637 | Low | A member was removed from a security-enabled local group. |
| 4734 | 638 | Low | A security-enabled local group was deleted. |
| 4738 | 642 | Low | A user account was changed. |
| 4740 | 644 | Low | A user account was locked out. |
| 4741 | 645 | Low | A computer account was changed. |
| 4742 | 646 | Low | A computer account was changed. |
| 4743 | 647 | Low | A computer account was deleted. |
| 4744 | 648 | Low | A security-disabled local group was created. |
| 4745 | 649 | Low | A security-disabled local group was changed. |
| 4746 | 650 | Low | A member was added to a security-disabled local group. |
| 4747 | 651 | Low | A member was removed from a security-disabled local group. |
| 4748 | 652 | Low | A security-disabled local group was deleted. |
| 4749 | 653 | Low | A security-disabled global group was created. |
| 4750 | 654 | Low | A security-disabled global group was changed. |
| 4751 | 655 | Low | A member was added to a security-disabled global group. |
| 4752 | 656 | Low | A member was removed from a security-disabled global group. |
| 4753 | 657 | Low | A security-disabled global group was deleted. |
| 4756 | 660 | Low | A member was added to a security-enabled universal group. |
| 4757 | 661 | Low | A member was removed from a security-enabled universal group. |
| 4758 | 662 | Low | A security-enabled universal group was deleted. |
| 4759 | 663 | Low | A security-disabled universal group was created. |
| 4760 | 664 | Low | A security-disabled universal group was changed. |
| 4761 | 665 | Low | A member was added to a security-disabled universal group. |
| 4762 | 666 | Low | A member was removed from a security-disabled universal group. |
| 4767 | 671 | Low | A user account was unlocked. |
| 4768 | 672,676 | Low | A Kerberos authentication ticket (TGT) was requested. |
| 4769 | 673 | Low | A Kerberos service ticket was requested. |
| 4770 | 674 | Low | A Kerberos service ticket was renewed. |
| 4771 | 675 | Low | Kerberos pre-authentication failed. |
| 4772 | 672 | Low | A Kerberos authentication ticket request failed. |
| 4774 | 678 | Low | An account was mapped for logon. |
| 4775 | 679 | Low | An account could not be mapped for logon. |
| 4776 | 680,681 | Low | The domain controller attempted to validate the credentials for an account. |
| 4777 | N/A | Low | The domain controller failed to validate the credentials for an account. |
| 4778 | 682 | Low | A session was reconnected to a Window Station. |
| 4779 | 683 | Low | A session was disconnected from a Window Station. |
| 4781 | 685 | Low | The name of an account was changed: |
| 4782 | N/A | Low | The password hash an account was accessed. |
| 4783 | 667 | Low | A basic application group was created. |
| 4784 | N/A | Low | A basic application group was changed. |
| 4785 | 689 | Low | A member was added to a basic application group. |
| 4786 | 690 | Low | A member was removed from a basic application group. |
| 4787 | 691 | Low | A nonmember was added to a basic application group. |
| 4788 | 692 | Low | A nonmember was removed from a basic application group. |
| 4789 | 693 | Low | A basic application group was deleted. |
| 4790 | 694 | Low | An LDAP query group was created. |
| 4793 | N/A | Low | The Password Policy Checking API was called. |
| 4800 | N/A | Low | The workstation was locked. |
| 4801 | N/A | Low | The workstation was unlocked. |
| 4802 | N/A | Low | The screen saver was invoked. |
| 4803 | N/A | Low | The screen saver was dismissed. |
| 4864 | N/A | Low | A namespace collision was detected. |
| 4869 | 773 | Low | Certificate Services received a resubmitted certificate request. |
| 4871 | 775 | Low | Certificate Services received a request to publish the certificate revocation list (CRL). |
| 4872 | 776 | Low | Certificate Services published the certificate revocation list (CRL). |
| 4873 | 777 | Low | A certificate request extension changed. |
| 4874 | 778 | Low | One or more certificate request attributes changed. |
| 4875 | 779 | Low | Certificate Services received a request to shut down. |
| 4876 | 780 | Low | Certificate Services backup started. |
| 4877 | 781 | Low | Certificate Services backup completed. |
| 4878 | 782 | Low | Certificate Services restore started. |
| 4879 | 783 | Low | Certificate Services restore completed. |
| 4880 | 784 | Low | Certificate Services started. |
| 4881 | 785 | Low | Certificate Services stopped. |
| 4883 | 787 | Low | Certificate Services retrieved an archived key. |
| 4884 | 788 | Low | Certificate Services imported a certificate into its database. |
| 4886 | 790 | Low | Certificate Services received a certificate request. |
| 4887 | 791 | Low | Certificate Services approved a certificate request and issued a certificate. |
| 4888 | 792 | Low | Certificate Services denied a certificate request. |
| 4889 | 793 | Low | Certificate Services set the status of a certificate request to pending. |
| 4891 | 795 | Low | A configuration entry changed in Certificate Services. |
| 4893 | 797 | Low | Certificate Services archived a key. |
| 4894 | 798 | Low | Certificate Services imported and archived a key. |
| 4895 | 799 | Low | Certificate Services published the CA certificate to Active Directory Domain Services. |
| 4898 | 802 | Low | Certificate Services loaded a template. |
| 4902 | N/A | Low | The Per-user audit policy table was created. |
| 4904 | N/A | Low | An attempt was made to register a security event source. |
| 4905 | N/A | Low | An attempt was made to unregister a security event source. |
| 4909 | N/A | Low | The local policy settings for the TBS were changed. |
| 4910 | N/A | Low | The Group Policy settings for the TBS were changed. |
| 4928 | N/A | Low | An Active Directory replica source naming context was established. |
| 4929 | N/A | Low | An Active Directory replica source naming context was removed. |
| 4930 | N/A | Low | An Active Directory replica source naming context was modified. |
| 4931 | N/A | Low | An Active Directory replica destination naming context was modified. |
| 4932 | N/A | Low | Synchronization of a replica of an Active Directory naming context has begun. |
| 4933 | N/A | Low | Synchronization of a replica of an Active Directory naming context has ended. |
| 4934 | N/A | Low | Attributes of an Active Directory object were replicated. |
| 4935 | N/A | Low | Replication failure begins. |
| 4936 | N/A | Low | Replication failure ends. |
| 4937 | N/A | Low | A lingering object was removed from a replica. |
| 4944 | N/A | Low | The following policy was active when the Windows Firewall started. |
| 4945 | N/A | Low | A rule was listed when the Windows Firewall started. |
| 4946 | N/A | Low | A change has been made to Windows Firewall exception list. A rule was added. |
| 4947 | N/A | Low | A change has been made to Windows Firewall exception list. A rule was modified. |
| 4948 | N/A | Low | A change has been made to Windows Firewall exception list. A rule was deleted. |
| 4949 | N/A | Low | Windows Firewall settings were restored to the default values. |
| 4950 | N/A | Low | A Windows Firewall setting has changed. |
| 4951 | N/A | Low | A rule has been ignored because its major version number was not recognized by Windows Firewall. |
| 4952 | N/A | Low | Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced. |
| 4953 | N/A | Low | A rule has been ignored by Windows Firewall because it could not parse the rule. |
| 4954 | N/A | Low | Windows Firewall Group Policy settings have changed. The new settings have been applied. |
| 4956 | N/A | Low | Windows Firewall has changed the active profile. |
| 4957 | N/A | Low | Windows Firewall did not apply the following rule: |
| 4958 | N/A | Low | Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer: |
| 4979 | N/A | Low | IPsec Main Mode and Extended Mode security associations were established. |
| 4980 | N/A | Low | IPsec Main Mode and Extended Mode security associations were established. |
| 4981 | N/A | Low | IPsec Main Mode and Extended Mode security associations were established. |
| 4982 | N/A | Low | IPsec Main Mode and Extended Mode security associations were established. |
| 4985 | N/A | Low | The state of a transaction has changed. |
| 5024 | N/A | Low | The Windows Firewall Service has started successfully. |
| 5025 | N/A | Low | The Windows Firewall Service has been stopped. |
| 5031 | N/A | Low | The Windows Firewall Service blocked an application from accepting incoming connections on the network. |
| 5032 | N/A | Low | Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network. |
| 5033 | N/A | Low | The Windows Firewall Driver has started successfully. |
| 5034 | N/A | Low | The Windows Firewall Driver has been stopped. |
| 5039 | N/A | Low | A registry key was virtualized. |
| 5040 | N/A | Low | A change has been made to IPsec settings. An Authentication Set was added. |
| 5041 | N/A | Low | A change has been made to IPsec settings. An Authentication Set was modified. |
| 5042 | N/A | Low | A change has been made to IPsec settings. An Authentication Set was deleted. |
| 5043 | N/A | Low | A change has been made to IPsec settings. A Connection Security Rule was added. |
| 5044 | N/A | Low | A change has been made to IPsec settings. A Connection Security Rule was modified. |
| 5045 | N/A | Low | A change has been made to IPsec settings. A Connection Security Rule was deleted. |
| 5046 | N/A | Low | A change has been made to IPsec settings. A Crypto Set was added. |
| 5047 | N/A | Low | A change has been made to IPsec settings. A Crypto Set was modified. |
| 5048 | N/A | Low | A change has been made to IPsec settings. A Crypto Set was deleted. |
| 5050 | N/A | Low | An attempt to programmatically disable the Windows Firewall using a call to InetFwProfile.FirewallEnabled(False) |
| 5051 | N/A | Low | A file was virtualized. |
| 5056 | N/A | Low | A cryptographic self test was performed. |
| 5057 | N/A | Low | A cryptographic primitive operation failed. |
| 5058 | N/A | Low | Key file operation. |
| 5059 | N/A | Low | Key migration operation. |
| 5060 | N/A | Low | Verification operation failed. |
| 5061 | N/A | Low | Cryptographic operation. |
| 5062 | N/A | Low | A kernel-mode cryptographic self test was performed. |
| 5063 | N/A | Low | A cryptographic provider operation was attempted. |
| 5064 | N/A | Low | A cryptographic context operation was attempted. |
| 5065 | N/A | Low | A cryptographic context modification was attempted. |
| 5066 | N/A | Low | A cryptographic function operation was attempted. |
| 5067 | N/A | Low | A cryptographic function modification was attempted. |
| 5068 | N/A | Low | A cryptographic function provider operation was attempted. |
| 5069 | N/A | Low | A cryptographic function property operation was attempted. |
| 5070 | N/A | Low | A cryptographic function property modification was attempted. |
| 5125 | N/A | Low | A request was submitted to the OCSP Responder Service |
| 5126 | N/A | Low | Signing Certificate was automatically updated by the OCSP Responder Service |
| 5127 | N/A | Low | The OCSP Revocation Provider successfully updated the revocation information |
| 5136 | 566 | Low | A directory service object was modified. |
| 5137 | 566 | Low | A directory service object was created. |
| 5138 | N/A | Low | A directory service object was undeleted. |
| 5139 | N/A | Low | A directory service object was moved. |
| 5140 | N/A | Low | A network share object was accessed. |
| 5141 | N/A | Low | A directory service object was deleted. |
| 5152 | N/A | Low | The Windows Filtering Platform blocked a packet. |
| 5153 | N/A | Low | A more restrictive Windows Filtering Platform filter has blocked a packet. |
| 5154 | N/A | Low | The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections. |
| 5155 | N/A | Low | The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections. |
| 5156 | N/A | Low | The Windows Filtering Platform has allowed a connection. |
| 5157 | N/A | Low | The Windows Filtering Platform has blocked a connection. |
| 5158 | N/A | Low | The Windows Filtering Platform has permitted a bind to a local port. |
| 5159 | N/A | Low | The Windows Filtering Platform has blocked a bind to a local port. |
| 5378 | N/A | Low | The requested credentials delegation was disallowed by policy. |
| 5440 | N/A | Low | The following callout was present when the Windows Filtering Platform Base Filtering Engine started. |
| 5441 | N/A | Low | The following filter was present when the Windows Filtering Platform Base Filtering Engine started. |
| 5442 | N/A | Low | The following provider was present when the Windows Filtering Platform Base Filtering Engine started. |
| 5443 | N/A | Low | The following provider context was present when the Windows Filtering Platform Base Filtering Engine started. |
| 5444 | N/A | Low | The following sublayer was present when the Windows Filtering Platform Base Filtering Engine started. |
| 5446 | N/A | Low | A Windows Filtering Platform callout has been changed. |
| 5447 | N/A | Low | A Windows Filtering Platform filter has been changed. |
| 5448 | N/A | Low | A Windows Filtering Platform provider has been changed. |
| 5449 | N/A | Low | A Windows Filtering Platform provider context has been changed. |
| 5450 | N/A | Low | A Windows Filtering Platform sublayer has been changed. |
| 5451 | N/A | Low | An IPsec Quick Mode security association was established. |
| 5452 | N/A | Low | An IPsec Quick Mode security association ended. |
| 5456 | N/A | Low | PAStore Engine applied Active Directory storage IPsec policy on the computer. |
| 5457 | N/A | Low | PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. |
| 5458 | N/A | Low | PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. |
| 5459 | N/A | Low | PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. |
| 5460 | N/A | Low | PAStore Engine applied local registry storage IPsec policy on the computer. |
| 5461 | N/A | Low | PAStore Engine failed to apply local registry storage IPsec policy on the computer. |
| 5462 | N/A | Low | PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem. |
| 5463 | N/A | Low | PAStore Engine polled for changes to the active IPsec policy and detected no changes. |
| 5464 | N/A | Low | PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services. |
| 5465 | N/A | Low | PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully. |
| 5466 | N/A | Low | PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied. |
| 5467 | N/A | Low | PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used. |
| 5468 | N/A | Low | PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used. |
| 5471 | N/A | Low | PAStore Engine loaded local storage IPsec policy on the computer. |
| 5472 | N/A | Low | PAStore Engine failed to load local storage IPsec policy on the computer. |
| 5473 | N/A | Low | PAStore Engine loaded directory storage IPsec policy on the computer. |
| 5474 | N/A | Low | PAStore Engine failed to load directory storage IPsec policy on the computer. |
| 5477 | N/A | Low | PAStore Engine failed to add quick mode filter. |
| 5479 | N/A | Low | IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. |
| 5632 | N/A | Low | A request was made to authenticate to a wireless network. |
| 5633 | N/A | Low | A request was made to authenticate to a wired network. |
| 5712 | N/A | Low | A Remote Procedure Call (RPC) was attempted. |
| 5888 | N/A | Low | An object in the COM+ Catalog was modified. |
| 5889 | N/A | Low | An object was deleted from the COM+ Catalog. |
| 5890 | N/A | Low | An object was added to the COM+ Catalog. |
| 6008 | N/A | Low | The previous system shutdown was unexpected |
| 6144 | N/A | Low | Security policy in the Group Policy objects has been applied successfully. |
| 6272 | N/A | Low | Network Policy Server granted access to a user. |
| N/A | 561 | Low | A handle to an object was requested. |
| N/A | 563 | Low | Object open for delete |
| N/A | 625 | Low | User Account Type Changed |
| N/A | 613 | Low | IPsec policy agent started |
| N/A | 614 | Low | IPsec policy agent disabled |
| N/A | 615 | Low | IPsec policy agent |
| N/A | 616 | Low | IPsec policy agent encountered a potential serious failure |
| 24577 | N/A | Low | Encryption of volume started |
| 24578 | N/A | Low | Encryption of volume stopped |
| 24579 | N/A | Low | Encryption of volume completed |
| 24580 | N/A | Low | Decryption of volume started |
| 24581 | N/A | Low | Decryption of volume stopped |
| 24582 | N/A | Low | Decryption of volume completed |
| 24583 | N/A | Low | Conversion worker thread for volume started |
| 24584 | N/A | Low | Conversion worker thread for volume temporarily stopped |
| 24588 | N/A | Low | The conversion operation on volume %2 encountered a bad sector error. Please validate the data on this volume |
| 24595 | N/A | Low | Volume %2 contains bad clusters. These clusters will be skipped during conversion. |
| 24621 | N/A | Low | Initial state check: Rolling volume conversion transaction on %2. |
| 5049 | N/A | Low | An IPsec Security Association was deleted. |
| 5478 | N/A | Low | IPsec Services has started successfully. |