Windows Server 2016/2019 Hardening Guidelines

Version 1.7

Response Contact	
Name	Ashish Gupta
Title	Manager - InfoSec
Address	Gurgaon Phase V
Email	Ashish.Gupta31@Genpact.com
Telephone	+91 9910930098

Notice

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by GENPACT, nor is this document (in whole or in part) to be reproduced or disclosed to other GENPACT employees without a need to know, or to any third party or made public without the prior express written permission of GENPACT.

Version Control

Ver No.	Version Date	Type of Changes	Author	Reviewed By	Date of Next Review
1.0	21/09/2018	Initial Document	Ashish Gupta	Rohit Kohli	Need Based
1.1	24/09/2018	Changes Accepted & NTP Configuration	Ashish Gupta	Rohit Kohli	Need Based
1.2	14/01/2019	Modify Password Policies, SMBv1	Ashish Gupta	Rohit Kohli	Need Based
1.3	07/02/2019	Pass the Hash Mitigation Policies, Protected User group	Ashish Gupta	Rohit Kohli	Need Based
1.4	29/04/2019	Updated some new policies and services	Ashish Gupta	Rohit Kohli	Need Based
1.5	10/10/2019	October 2019 Changes, TLS Settings	Ashish Gupta	Rohit Kohli / Niraj Shukla	Need Based
1.6	27/01/2020	January 2020 Changes, modified few controls, Secure RDP Controls	Ashish Gupta	Rohit Kohli / Niraj Shukla	Need Based
1.7	02/09/2020	Rename few controls as per 2019 OS	Ashish Gupta	Rohit Kohli / Niraj Shukla	Need Based

Viewer

SMG-Wintel SMEs and team members, Compliance teams, Poles windows SPOC

Contents

1. Windows 2016 Hardening Guidelines

1.1. Objective

The objective of this document is to establish procedure for hardening all Windows servers of the Genpact managed domains.

1.2. Scope

All windows servers and domain controllers running with 2016 & 2019 operating systems in Genpact managed domains.

1.3. Abbreviations

- ➢ SMG – Server Management Group
- ➢ OS – Operating System
- ➢ InfoSec – Information Security
- ➢ CDC – Cyber Defense Centre

1.4. Stake Holders

1. InfoSec Team
2. SMG-Wintel Lead
3. SMG-Wintel SPOC
4. All poles windows SPOC
5. Datacentre teams

1.5. Detection

- Monthly vulnerability scanning and remediation of vulnerabilities found in server golden image
- Vulnerability assessment of window servers on a monthly basis and report vulnerabilities for remediation

1.6. Governance

Server Hardening document is periodically reviewed by Genpact InfoSec team. For any changes to the existing document, approval must be taken from InfoSec team

1.7. Incidence Logging / Escalation

- ☑ Notify members of the InfoSec team
- ☑ Notify SPOC for the SMG-Wintel team

2. Windows Settings - Security Settings

2.1. Account Policies

2.1.1. Password Policy

Password Policy		
Policy Path: Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Enforce Password History	24 Passwords or more passwords	24 Passwords or more passwords
Maximum Password Age	90 days or less	90 days or less
Minimum Password Age	1 or more days	1 or more days
Minimum Password Length	8 or more characters	8 or more characters
Passwords Must Meet Complexity Requirements	Enabled	Enabled
Store passwords using reversible encryption	Disabled	Disabled

2.1.2. Account Lockout Policy

Account Lockout Policy		
Policy Path: Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Account Lockout Duration	0 minutes	0 minutes
Account Lockout Threshold	5 invalid login attempts	5 invalid login attempts
Reset Account Lockout Threshold After	1440 minutes	1440 minutes

2.1.3. Kerberos Policy

Account Lockout Policy		
Policy Path: Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Enforce user logon restrictions	Enable	NA
Maximum lifetime for service ticket	600 Minutes	NA
Maximum lifetime for user ticket	10 Hours	NA
Maximum lifetime for user ticket renewal	7 days	NA
Maximum tolerance for computer clock synchronization	5 minutes	NA

2.2. Local Policies

2.2.1. User Right Assignments

User Rights Assignments		
Policy Path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Access this computer from the network	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators	NT AUTHORITY\Authenticated Users, BUILTIN\Administrators
Add workstations to domain	BUILTIN\Administrators	Not Configured
Adjust memory quotas for a process	BUILTIN\Administrators	Not Configured
Allow log on locally	BUILTIN\Administrators, Domain Admins	BUILTIN\Administrators, Domain Admins
Allow log on through Remote Desktop Services	BUILTIN\Administrators, Domain Admins, NT AUTHORITY\Authenticated Users	BUILTIN\Administrators, Domain Admins, NT AUTHORITY\Authenticated Users
Backup files and directories	BUILTIN\Administrators	BUILTIN\Administrators
Change the system time	BUILTIN\Administrators, Domain Admins, LOCAL SERVICES	BUILTIN\Administrators, Domain Admins, LOCAL SERVICES
Change the time zone	BUILTIN\Administrators, Domain Admins, LOCAL SERVICES	BUILTIN\Administrators, Domain Admins, LOCAL SERVICES
Create a pagefile	BUILTIN\Administrators	BUILTIN\Administrators
Create a token object	BUILTIN\Administrators	BUILTIN\Administrators
Create global objects	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE
Create permanent shared objects	BUILTIN\Administrators	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators	BUILTIN\Administrators
Deny access to this computer from the network	NT AUTHORITY\ANONYMOUS LOGON, BUILTIN\Guests	NT AUTHORITY\ANONYMOUS LOGON, BUILTIN\Guests
Deny log on locally	BUILTIN\Guests	BUILTIN\Guests
Deny log on as a batch job	BUILTIN\Guests	BUILTIN\Guests
Deny log on through Remote Desktop Services	BUILTIN\Guests	BUILTIN\Guests, NT AUTHORITY\Local Account
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators	No One (Configure without adding anyone)
Force shutdown from a remote system	BUILTIN\Administrators	BUILTIN\Administrators
Impersonate a client after authentication	BUILTIN\Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE	BUILTIN\Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE, IIS_USERS
Increase scheduling priority	BUILTIN\Administrators	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Administrators	BUILTIN\Administrators
Log on as a batch job	BUILTIN\Administrators	BUILTIN\Administrators
Log on as a service	BUILTIN\Administrators	BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators	BUILTIN\Administrators

Perform volume maintenance tasks	BUILTIN\Administrators	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Administrators	BUILTIN\Administrators
Shut down the system	BUILTIN\Administrators	BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators	BUILTIN\Administrators

2.2.2. Security Options

Security Options		
Policy Path: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Accounts: Rename administrator account	Not Applicable	900026557
Accounts: Rename guest account	Not Applicable	NTUSER
Accounts: Guest account status	Not Applicable	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled	Enabled
Domain controller: LDAP server signing requirements	Require signing	Not Applicable
Domain controller: Refuse machine account password changes	Disabled	Not Applicable
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabled
Domain member: Disable machine account password changes	Disabled	Disabled
Domain member: Maximum machine account password age	30 Days	30 Days
Domain member: Require strong (Windows 2000 or later) session key	Enabled	Enabled
Interactive logon: Machine inactivity limit	900 seconds	900 seconds
Interactive logon: Do not display last username	Enabled	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled
Interactive logon: Message text for users attempting to log on	You are attempting to enter company owned and controlled computer systems and network. Access to these systems is restricted to authorized persons and these systems may not be used for any unlawful purpose or in any way which violates applicable laws, company policies, procedures, instructions or guidelines. Company reserves the right to electronically monitor access and use of company systems without any further warning. Your usage of company systems constitutes your consent to monitoring by company, subject to applicable laws. Violation of laws, company policies, procedures, instructions or guidelines may be grounds for disciplinary action, up to termination of employment and may subject the user to prosecution.	

Interactive logon: Message title for users attempting to log on	Important note, please read carefully:	
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0	0
Interactive logon: Prompt user to change password before expiration	14 Days	14 Days
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled	Enabled
Microsoft network client: Digitally sign communications (always)	Enabled	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled
Microsoft network client: Send unencrypted password to third – party SMB servers	Disabled	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 Minutes	15 Minutes
Microsoft network server: Digitally sign communications (always)	Enabled	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	Enabled
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	Classic - local users authenticate as themselves
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled
Network access: Restrict clients allowed to make remote calls to SAM	Not Configured	O:BAG:BAD:(A;;RC;;;BA)
Network security: Allow Local System to use computer identity for NTLM	Not Applicable	Enabled
Network security: Allow LocalSystem NULL session fallback	Not Applicable	Disabled
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled
Network security: Force logoff when logon hours expire	Enabled	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 Responses only, Refuse LM and NTLM	Send NTLMv2 Responses only, Refuse LM and NTLM
Network security: LDAP client signing requirements	Negotiate Signing	Negotiate Signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security, Require 128bit encryption	Require NTLMv2 session security, Require 128bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security, Require 128-bit encryption	Require NTLMv2 session security, Require 128-bit encryption
Recovery console: Allow automatic administrative logon	Disabled	Disabled

Shutdown: Allow system to be shut down without having to log on	Disabled	Disabled
	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop.	Disabled	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Elevate without Prompting	Elevate without Prompting
User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests	Automatically deny elevation requests
User Account Control: Detect application installations and prompt for elevation	Enabled	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled	Enabled

2.3. System Services (2016 & 2019 Server OS)

DisplayName	Name	StartType	Dmn Ctrl’s	Mem Srv’s
ActiveX Installer (AxInstSV)	AxInstSV	Disabled	Stopped	Stopped
App Readiness	AppReadiness	Manual	Running	Running
Application Identity	AppIDSvc	Manual	Stopped	Stopped
Application Information	Appinfo	Manual	Running	Running
Application Layer Gateway Service	ALG	Automatic	Running	Stopped
Application Management	AppMgmt	Automatic	Running	Stopped
Auto Time Zone Updater	tzautoupdate	Disabled	Stopped	Stopped
Background Intelligent Transfer Service	BITS	Manual	Running	Running
Background Tasks Infrastructure Service	BrokerInfrastructure	Automatic	Running	Running
Base Filtering Engine	BFE	Automatic	Running	Running
Bluetooth Support Service	bthserv	Disabled	Stopped	Stopped
CDPUserSvc	CDPUserSvc	Disabled	Stopped	Stopped
Certificate Propagation	CertPropSvc	Manual	Running	Running
CNG Key Isolation	KeyIso	Manual	Running	Running
COM+ Event System	EventSystem	Automatic	Running	Running
COM+ System Application	COMSysApp	Manual	Stopped	Started
Computer Browser	Browser	Disabled	Stopped	Stopped
Connected Devices Platform Service	CDPSvc	Automatic	Running	Running
Connected User Experiences and Telemetry	DiagTrack	Automatic	Running	Running
Contact Data	PimIndexMaintenanceSvc	Disabled	Stopped	Stopped
CoreMessaging	CoreMessagingRegistrar	Automatic	Running	Running
Credential Manager	VaultSvc	Manual	Stopped	Stopped
Cryptographic Services	CryptSvc	Automatic	Running	Running
DCOM Server Process Launcher	DcomLaunch	Automatic	Running	Running
DHCP Client	Dhcp	Automatic	Running	Running
Diagnostic Policy Service	DPS	Automatic	Running	Running
Diagnostic Service Host	WdiServiceHost	Disabled	Stopped	Stopped

Diagnostic System Host	WdiSystemHost	Disabled	Stopped	Stopped
Distributed Link Tracking Client	TrkWks	Automatic	Running	Running
Distributed Transaction Coordinator	MSDTC	Automatic	Running	Stopped
DNS Client	Dnscache	Automatic	Running	Running
Encrypting File System (EFS)	EFS	Manual	Stopped	Stopped
Extensible Authentication Protocol	EapHost	Manual	Stopped	Stopped
Function Discovery Provider Host	fdPHost	Manual	Stopped	Stopped
Function Discovery Resource Publication	FDResPub	Manual	Stopped	Stopped
Group Policy Client	gpsvc	Automatic	Running	Running
Human Interface Device Service	hidserv	Manual	Stopped	Stopped
HV Host Service	HvHost	Manual	Running	Running
Hyper-V Data Exchange Service	vmickvpexchange	Manual	Running	Running
Hyper-V Guest Service Interface	vmicguestinterface	Manual	Running	Running
Hyper-V Guest Shutdown Service	vmicshutdown	Manual	Running	Running
Hyper-V Heartbeat Service	vmicheartbeat	Manual	Running	Running
Hyper-V PowerShell Direct Service	vmicvmsession	Manual	Running	Running
Hyper-V Remote Desktop Virtualization Service	vmicrdv	Manual	Running	Running
Hyper-V Time Synchronization Service	vmictimesync	Manual	Running	Running
Hyper-V Volume Shadow Copy Requestor	vmicvss	Manual	Running	Running
IKE and AuthIP IPsec Keying Modules	IKEEXT	Automatic	Running	Running
Interactive Services Detection	UI0Detect	Manual	Stopped	Stopped
Internet Connection Sharing (ICS)	SharedAccess	Disabled	Stopped	Stopped
IP Helper	iphlpsvc	Disabled	Stopped	Stopped
IPsec Policy Agent	PolicyAgent	Manual	Running	Running
KtmRm for Distributed Transaction Coordinator	KtmRm	Manual	Stopped	Stopped
Link-Layer Topology Discovery Mapper	lltdsvc	Manual	Stopped	Stopped
Microsoft App-V Client	AppVClient	Disabled	Stopped	Stopped
Microsoft iSCSI Initiator Service	MSiSCSI	Manual	Stopped	Stopped
Microsoft Software Shadow Copy Provider	swprv	Manual	Stopped	Stopped
Microsoft Storage Spaces SMP	smphost	Manual	Running	Running
Net.Tcp Port Sharing Service	NetTcpPortSharing	Disabled	Stopped	Stopped
Netlogon	Netlogon	Automatic	Running	Running
Network Connections	Netman	Manual	Running	Running
Network List Service	netprofm	Manual	Running	Running
Network Store Interface Service	nsi	Automatic	Running	Running
Offline Files	CscService	Disabled	Stopped	Stopped
Optimize drives	defragsvc	Manual	Stopped	Stopped
Performance Counter DLL Host	PerfHost	Manual	Stopped	Stopped
Performance Logs & Alerts	pla	Manual	Running	Running
Plug and Play	PlugPlay	Automatic	Running	Running
Portable Device Enumerator Service	WPDBusEnum	Manual	Running	Running
Power	Power	Automatic	Running	Running
Print Spooler	Spooler	Disabled	Stopped	Stopped
Printer Extensions and Notifications	PrintNotify	Disabled	Stopped	Stopped
Problem Reports and Solutions Control Panel Support	wercplsupport	Disabled	Stopped	Stopped
Quality Windows Audio Video Experience	QWAVE	Disabled	Stopped	Stopped

Radio Management Service	RmSvc	Disabled	Stopped	Stopped
Remote Access Auto Connection Manager	RasAuto	Manual	Stopped	Stopped
Remote Access Connection Manager	RasMan	Manual	Stopped	Stopped
Remote Desktop Configuration	SessionEnv	Manual	Running	Running
Remote Desktop Services	TermService	Manual	Running	Running
Remote Desktop Services UserMode Port Redirector	UmRdpService	Manual	Running	Running
Remote Procedure Call (RPC)	RpcSs	Automatic	Running	Running
Remote Procedure Call (RPC) Locator	RpcLocator	Automatic	Stopped	Stopped
Remote Registry	RemoteRegistry	Automatic	Running	Running
Resultant Set of Policy Provider	RSoPProv	Manual	Running	Stopped
Routing and Remote Access	RemoteAccess	Disabled	Stopped	Stopped
RPC Endpoint Mapper	RpcEptMapper	Automatic	Running	Running
Secondary Logon	seclogon	Manual	Stopped	Running
Secure Socket Tunneling Protocol Service	SstpSvc	Manual	Stopped	Stopped
Security Accounts Manager	SamSs	Automatic	Running	Running
Sensor Data Service	SensorDataService	Disabled	Stopped	Stopped
Sensor Monitoring Service	SensrSvc	Disabled	Stopped	Stopped
Sensor Service	SensorService	Disabled	Stopped	Stopped
Server	LanmanServer	Automatic	Running	Running
Shell Hardware Detection	ShellHWDetection	Disabled	Stopped	Stopped
Smart Card	SCardSvr	Disabled	Stopped	Stopped
Smart Card Device Enumeration Service	ScDeviceEnum	Disabled	Stopped	Stopped
Smart Card Removal Policy	SCPolicySvc	Manual	Stopped	Stopped
SNMP Trap	SNMPTRAP	Disabled	Stopped	Stopped
Software Protection	sppsvc	Automatic	Stopped	Stopped
Special Administration Console Helper	sacsvr	Manual	Stopped	Stopped
SSDP Discovery	SSDPSRV	Disabled	Stopped	Stopped
Still Image Acquisition Events	WiaRpc	Disabled	Stopped	Stopped
Sync Host	OneSyncSvc	Disabled	Stopped	Stopped
System Event Notification Service	SENS	Automatic	Running	Running
System Events Broker	SystemEventsBroker	Automatic	Running	Running
Task Scheduler	Schedule	Automatic	Running	Running
TCP/IP NetBIOS Helper	lmhosts	Manual	Running	Running
Telephony	TapiSrv	Manual	Stopped	Stopped
Themes	Themes	Automatic	Running	Running
Tile Data model server	tiledatamodelsvc	Automatic	Running	Running
Time Broker	TimeBrokerSvc	Manual	Stopped	Stopped
Touch Keyboard and Handwriting Panel Service	TabletInputService	Disabled	Stopped	Stopped
Update Orchestrator Service for Windows Update	UsoSvc	Manual	Running	Running
UPnP Device Host	upnphost	Disabled	Stopped	Stopped
User Data Access	UserDataSvc	Disabled	Stopped	Stopped
User Data Storage	UnistoreSvc	Disabled	Stopped	Stopped
User Experience Virtualization Service	UevAgentService	Disabled	Stopped	Stopped
User Profile Service	ProfSvc	Automatic	Running	Running
Virtual Disk	vds	Automatic	Running	Running
Volume Shadow Copy	VSS	Automatic	Running	Running
WalletService	WalletService	Disabled	Stopped	Stopped
Windows Audio	Audiosrv	Manual	Running	Stopped

Windows Audio Endpoint Builder	AudioEndpointBuilder	Manual	Running	Stopped
Windows Camera Frame Server	FrameServer	Disabled	Stopped	Stopped
Windows Driver Foundation - User-mode Driver Framework	wudfsvc	Manual	Stopped	Stopped
Windows Error Reporting Service	WerSvc	Manual	Stopped	Stopped
Windows Event Collector	Wecsvc	Manual	Running	Running
Windows Event Log	EventLog	Automatic	Running	Running
Windows Firewall	MpsSvc	Automatic	Running	Running
Windows Font Cache Service	FontCache	Disabled	Stopped	Stopped
Windows Image Acquisition (WIA)	stisvc	Disabled	Stopped	Stopped
Windows Insider Service	wisvc	Disabled	Stopped	Stopped
Windows Installer	msiserver	Manual	Stopped	Stopped
Windows Management Instrumentation	Winmgmt	Automatic	Running	Running
Windows Mobile Hotspot Service	icssvc	Disabled	Stopped	Stopped
Windows Modules Installer	TrustedInstaller	Manual	Stopped	Stopped
Windows Push Notifications System Service	WpnService	Disabled	Stopped	Stopped
Windows Push Notifications User Service	WpnUserService	Disabled	Stopped	Stopped
Windows Remote Management (WS-Management)	WinRM	Automatic	Running	Running
Windows Search	WSearch	Disabled	Stopped	Stopped
Windows Time	W32Time	Automatic	Running	Running
Windows Update	wuauserv	Automatic	Running	Running
WinHTTP Web Proxy Auto-Discovery Service	WinHttpAutoProxySvc	Automatic	Running	Stopped
Wired AutoConfig	dot3svc	Manual	Stopped	Stopped
WMI Performance Adapter	wmiApSrv	Manual	Stopped	Stopped
Workstation	LanmanWorkstation	Automatic	Running	Running
Xbox Live Auth Manager	XblAuthManager	Disabled	Stopped	Stopped
Xbox Live Game Save	XblGameSave	Disabled	Stopped	Stopped

2.4. Public Key Policies

This section will contain all PKI policies related to Auto-enrolment, Trusted Root Certificates, Intermediate Certificates, etc.

2.4.1. Certificate Services Client – Auto-Enrolment Settings

<table>
<tr><th colspan="3">Public Key Policies</th></tr>
<tr><td colspan="3">Policy Path: Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Services Client – Auto-Enrollment Settings</td></tr>
<tr><th>Policy Name</th><th>Recommended Settings (Domain Controller)</th><th>Recommended Settings (Member Servers)</th></tr>
<tr><td>Automatic certificate management</td><td>Enabled</td><td>Enabled</td></tr>
<tr><td colspan="3">☑ Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates</td></tr>
<tr><td colspan="3">☑ Update and manage certificates that use certificate templates from Active Directory</td></tr>
</table>

2.4.2. Trusted Root Certificate Authorities

Policy Path: Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certificate Authorities

Import Root certificate by right clicking in the black area and click "Import".

Issued To	Issued By	Intended Purposes
AddTrust External CA Root	AddTrust External CA Root	<All>
CorpCA	CorpCA	<All>
CORPCA-2K8	CORPCA-2K8	<All>
gateway-bcp.genpact.com	Trusted Secure Certificate Authority	Server Authentication, Client Authentication
Gecis Authority	Gecis Authority	<All>
Genpact	Genpact	<All>
Genpact Authority	Genpact Authority	<All>
McAfee Web Gateway	McAfee Web Gateway	<All>
Trusted Secure Certificate Authority	AddTrust External CA Root	<All>
Zscaler Root CA	Zscaler Root CA	<All>

2.4.3. Intermediate Certificate Authorities

Policy Path: Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Intermediate Certificate Authorities
Import Root certificate by right clicking in the black area and click "Import".

Issued To	Issued By	Intended Purposes
CorpCA	CorpCA	<All>
CORPCA-2K8	CORPCA-2K8	<All>
Gecis Authority	Gecis Authority	<All>
Genpact Authority	Genpact Authority	<All>

2.5. Advance Audit Configuration Policy

2.5.1. Account Logon

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Account Logon		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Credential Validation	Success and Failure	Success and Failure
Audit Kerberos Authentication Service	Success and Failure	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure	Success and Failure
Audit Other Account Logon Events	Success and Failure	Success and Failure

2.5.2. Account Management

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Account Management		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Computer Account Management	Success	No Auditing
Audit Other Account Management Events	Success and Failure	Success and Failure
Audit Security Group Management	Success and Failure	Success and Failure
Audit User Account Management	Success and Failure	Success and Failure

2.5.3. Detailed Tracking

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Detailed Tacking		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Plug and Play Events	Success	Success
Audit Process Creation	Success	Success

2.5.4. DS Access

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\DS Access		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Directory Service Access	Success and Failure	No Auditing
Audit Directory Service Changes	Success and Failure	No Auditing

2.5.5. Logon / Logoff

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Logon / Logoff		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Account Lockout	Success and Failure	Success and Failure
Audit Group Membership	Success	Success
Audit Logoff	Success	Success
Audit Logon	Success and Failure	Success and Failure
Special Logon	Success	Success

2.5.6. Object Access

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Removable Storage	Success, Failure	Success, Failure
Audit Other Object Access Events	Success, Failure	Success, Failure

2.5.7. Policy Change

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Policy Change		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Policy Change	Success, Failure	Success, Failure
Authentication Policy Change	Success	Success
Audit Authorization Policy Change	Success	Success

2.5.8. Privilege Use

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Privilege Use		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Sensitive Privilege Use	Success, Failure	Success, Failure
Audit Non-Sensitive Privilege Use	Success, Failure	Success, Failure
Audit Other Privilege Use Events	Success, Failure	Success, Failure

2.5.9. System

Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit IPsec Driver	Success, Failure	Success, Failure
Audit Other System Events	Success, Failure	Success, Failure
Audit Security State Change	Success	Success
Audit Security System Extension	Success, Failure	Success, Failure
Audit System Integrity	Success, Failure	Success, Failure

3. Administrative Templates

3.1. Control Panel

This section contains recommendations for Control Panel settings.

3.1.1. Personalization

Policy Name	Domain Controller	Member Server
Prevent enabling lock screen camera	Enabled	Enabled
Prevent enabling lock screen slide show	Enabled	Enabled

3.2. Network

3.2.1. DNS Client

Policy Name	Domain Controller	Member Server
Turn off multicast name resolution	Not Applicable	Enabled

3.2.2. Fonts

Policy Name	Domain Controller	Member Server
Enable Font Providers	Disabled	Disabled

3.2.3. Link-Layer Topology Discovery

Policy Name	Domain Controller	Member Server
Turn on Mapper I/O (LLTDIO) driver	Disabled	Disabled
Turn on Responder (RSPNDR) driver	Disabled	Disabled

3.2.4. Lanman Workstation

Policy Name	Domain Controller	Member Server
Enable insecure guest logons	Disabled	Disabled

3.2.5. Network Provider

Policy Name	Domain Controller	Member Server
Hardened UNC Paths **\*\NETLOGON** *RequireMutualAuthentication=1, RequireIntegrity=1* **\*\SYSVOL** *RequireMutualAuthentication=1, RequireIntegrity=1*	Enabled	Enabled

3.2.6. Offline Files

Policy Name	Domain Controller	Member Server
Allow or Disallow use of the Offline Files feature	Disabled	Disabled

3.3. System

Policy Name	Domain Controller	Member Server
Do not display Manage Your Server page at logon	Enabled	Enabled

3.3.1. Credentials Delegation

Policy Name	Domain Controller	Member Server
Remote host allows delegation of non-exportable credentials	Enabled	Enabled
Restrict delegation of credentials to remote servers	Enabled *Restrict credential delegation*	Enabled *Restrict credential delegation*

3.3.2. Device Guard

Policy Name	Domain Controller	Member Server
Turn On Virtualization Based Security	Enabled: Secure Boot and DMA Protectors X - Enable Virtualization Based Protection of Code Integrity without Lock X - Enable Credential Guard without Lock	Enabled: Secure Boot and DMA Protectors X - Enable Virtualization Based Protection of Code Integrity without Lock X - Enable Credential Guard without Lock

3.3.3. Filesystem

Policy Name	Domain Controller	Member Server
Enable NTFS long paths	Not Configured	Enabled

3.3.4. Internet Communication Management

Internet Communication settings		
Policy Name	**Domain Controller**	**Member Server**
Turn off access to the Store	Enabled	Not Applicable
Turn off downloading of print drivers over HTTP	Enabled	Not Applicable
Turn off handwriting personalization data sharing	Enabled	Not Applicable
Turn off handwriting recognition error reporting	Enabled	Not Applicable
Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Enabled	Not Applicable
Turn off Internet download for Web publishing and online ordering wizards	Enabled	Not Applicable
Turn off printing over HTTP	Enabled	Not Applicable
Turn off Registration if URL connection is referring to Microsoft.com	Enabled	Not Applicable
Turn off Search Companion content file updates	Enabled	Not Applicable
Turn off the "Order Prints" picture task	Enabled	Not Applicable
Turn off the "Publish to Web" task for files and folders	Enabled	Not Applicable
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled	Not Applicable
Turn off Windows Customer Experience Improvement Program	Enabled	Not Applicable
Turn off Windows Error Reporting	Enabled	Not Applicable

3.3.5. Kerberos

Policy Name	Domain Controller	Member Server
Support device authentication using certificate **Device authentication behavior using certificate:** *Automatic*	Enabled	Enabled

3.3.6. Local Services

Policy Name	Domain Controller	Member Server
Disallow copying of user input methods to the system account for sign-in	Enabled	Enabled

3.3.7. Logon

Policy Name	Domain Controller	Member Server
Do not display network selection UI	Enabled	Enabled
Do not display the Getting Started welcome screen at logon	Enabled	Enabled

3.3.8. Net logon

Policy Name	Domain Controller	Member Server
Specify log file debug output level	Disabled	Disabled
Specify maximum log file size **Bytes: 20971520**	Enabled	Enabled

3.3.9. Remote Assistance

Policy Name	Domain Controller	Member Server
Configure Solicited Remote Assistance	Disabled	Disabled

3.3.10. Remote Procedure Call

Policy Name	Domain Controller	Member Server
Restrict Unauthenticated RPC clients	Not Configured	Enabled: Authenticated

3.3.11. User Profiles

Policy Name	Domain Controller	Member Server
Turn off the advertising ID	Enabled	Enabled

3.4. Windows Components

This section contains recommendations for Windows Components settings.

3.4.1. App Package Deployment

Policy Name	Domain Controller	Member Server
Allow a Windows app to share application data between users	Disabled	Disabled

3.4.2. App Privacy

Policy Name	Domain Controller	Member Server

Let Windows apps access account information Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access call history Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access contacts Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access diagnostic information about other apps Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access email Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access location Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access messaging Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access motion Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access notifications Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access Tasks Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access the calendar Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access the camera Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access the microphone Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps access trusted devices Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps control radios Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps make phone calls Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps run in the background Default for all apps: **Force Deny**	Enabled	Enabled
Let Windows apps sync with devices Default for all apps: **Force Deny**	Enabled	Enabled

3.4.3. App Runtime

Policy Name	Domain Controller	Member Server
Block launching Windows Store apps with Windows Runtime API access from hosted content.	Enabled	Enabled

3.4.4. Autoplay Policies

Policy Name	Domain Controller	Member Server
Disallow Autoplay for non-volume devices	Enabled	Enabled
Set the default behavior for AutoRun	Enabled: Do not execute any autorun commands	Enabled: Do not execute any autorun commands
Turn off Autoplay	Enabled: All Drives	Enabled: All Drives

3.4.5. Event Logs

Windows server application, system, and security event logs must be forwarded to IBM Qradar for logging and monitoring, kindly connect with Cyber Defense Centre (CDC) for additional information.

3.4.5.1. Application Event Logs

Application Event Logs		
Policy Path: Computer Configuration\Administrative Templates\Windows Components\Event Log Service		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Maximum Log Size (MB)	200000 KB	262144 KB
Control Event Log behavior when the log file reaches its maximum size	Disabled	Disabled

3.4.5.2. Security

Security Event Logs		
Policy Path: Computer Configuration\Administrative Templates\Windows Components\Event Log Service		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Maximum Log Size (MB)	1572864 KB	524288 KB
Control Event Log behavior when the log file reaches its maximum size	Disabled	Disabled

3.4.5.3. System

System Event Logs		
Policy Path: Computer Configuration\Administrative Templates\Windows Components\Event Log Service		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Maximum Log Size (MB)	200000 KB	262144 KB
Control Event Log behavior when the log file reaches its maximum size	Disabled	Disabled

3.4.6. Windows Explorer

Policy Name	**Domain Controller**	**Member Server**
Configure Windows SmartScreen	Enabled	Enabled
Turn off Data Execution Prevention for Explorer	Disabled	Disabled
Turn off heap termination on corruption	Disabled	Disabled

3.4.7. Location and Sensors

Policy Name [Windows Location Provider]	**Domain Controller**	**Member Server**
Turn off Windows Location Provider	Enabled	Enabled
Turn off location	Enabled	Enabled

3.4.8. Remote Desktop Services

Remote Desktop Connection Client

Policy Name	Domain Controller	Member Server
Do not allow passwords to be saved	Enabled	Enabled

Remote Desktop Session Host - Connections

Policy Name	Domain Controller	Member Server
Restrict Remote Desktop Services users to a single Remote Desktop Services session	Enabled	Enabled

Remote Desktop Session Host – Device and Resource Redirection

Policy Name	Domain Controller	Member Server
Allow audio and video playback redirection	Disabled	Disabled
Allow audio recording redirection	Disabled	Disabled
Do not allow COM port redirection	Enabled	Enabled
Do not allow drive redirection	Enabled	Enabled
Do not allow LPT port redirection	Enabled	Enabled
Do not allow supported Plug and Play device redirection	Enabled	Enabled

Remote Desktop Session Host – Host Security

Policy Name	Domain Controller	Member Server
Always prompt for password upon connection	Enabled	Enabled
Require secure RPC communication	Enabled	Enabled
Set client connection encryption level	Enabled: High Level	Enabled: High Level
Require user authentication for remote connections by using Network Level Authentication	Enabled	Enabled

Remote Desktop Session Host – Session Time Limits

Policy Name	Domain Controller	Member Server
Set time limit for active but idle Remote Desktop Services sessions	Enabled 15 Minutes	Enabled 2 Hours
Set time limit for disconnected sessions	Enabled 30 Minutes	Enabled 2 Hours

3.4.9. Store

Policy Name	Domain Controller	Member Server
Disable all apps from Windows Store	Enabled	Enabled
Turn off the Store application	Enabled	Enabled

3.4.10. Search

Policy Name	Domain Controller	Member Server
Allow indexing of encrypted files	Disabled	Disabled

3.4.11. Windows Installer

Policy Name	Domain Controller	Member Server
Allow user control over installs	Disabled	Disabled

Always install with elevated privileges	Disabled	Disabled

3.4.12. Windows Logon Options

Policy Name	Domain Controller	Member Server
Sign-in last interactive user automatically after a system-initiated restart	Disabled	Disabled

3.4.13. Windows Media Digital Rights Management

Policy Name	Domain Controller	Member Server
Prevent Windows Media DRM Internet Access	Enabled	Enabled

3.4.14. Windows PowerShell

Policy Name	Domain Controller	Member Server
Turn on Script Execution Execution Policy: **Allow local scripts and remote signed scripts**	Enabled	Enabled
Turn on Module Logging	Enabled	Enabled
Turn on PowerShell Script Block Logging	Enabled	Enabled

3.4.15. Windows Remote Management (WinRM)\WinRM) Client

Policy Name	Domain Controller	Member Server
Allow Basic authentication	Disabled	Disabled
Allow unencrypted traffic	Disabled	Disabled
Disallow Digest authentication	Enabled	Enabled

3.4.16. Windows Remote Management (WinRM)\WinRM) Services

Policy Name	Domain Controller	Member Server
Allow Basic authentication	Disabled	Disabled
Allow unencrypted traffic	Disabled	Disabled
Disallow WinRM from storing RunAs credentials	Enabled	Enabled

4. NTP Configuration

4.1. Ports Requirement

Port number **123 [UDP]** should be open on firewall for NTP and SNTP.

4.2. NTP Configuration on PDC

Below are registry changes on PDC to make sure that it synchronizes its time with the external NTP server.
Registry Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time

- In **Config**, Open **"Announced Flag"** to **5**, by default it would be **10**.
- In Parameters, Open **"NTPServer"** and mention **"0.us.pool.ntp.org,0x9"** in the value.
- In Parameters, Open **"Type"** and mention **"NTP"** in the value.

After all these changes, run the command. **"w32tm /resync /rediscover"**
It should synchronize its time with the external NTP server.

4.3. NTP Configuration on Member DC

Below are registry changes on Member DC to make sure that it synchronizes its time with PDC.
Registry Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time

- In **Config**, Open **"Announced Flag"** to **10**, by default it would be **10**.
- In Parameters, Open **"NTPServer"** and make it blank if it has some value in it.
- In Parameters, Open **"Type"** and mention **"NT5DS"** in the value. By this value, it will use Domain hierarchy-based synchronization.

After all these changes, run the command. **"w32tm /resync /rediscover"**
It should synchronize its time with the external NTP server.

4.4. Domain joined systems

All systems, workstations and member servers, joined to domain will contact their authoritative domain controllers to synchronize their time services automatically. There is no need to make any configuration on them.

5. Pass the Hash Mitigations

5.1. WDigest Authentication

When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft.

Registry Change

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
Value Name	UseLogonCredential
Value Type	REG_DWORD
Disabled Value	0

If **"UseLogonCredential"** value is set to **1**, it means it is enabled. Please change it to **0** to make it disable.

Note:
Group policy template is not available by default, it can be download from link [1] from resource links.
Policy Path: Computer Configuration\Policies\Administrative Templates\MS Security Guide\WDigest Authentication
Select **disable** so that Lsass.exe does not retain a copy of the user's plaintext password in memory.

5.2. LSA Protection

Enable additional protection for the Local Security Authority (LSA) process to prevent code injection that could compromise credentials.

Registry Change

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SYSTEM\CurrentControlSet\Control\Lsa
Value Name	RunAsPPL
Value Type	REG_DWORD
Enabled Value	1

If **"RunAsPPL"** value is set to **0**, it means it is disabled. Please change it to **1** to make it enabled.

5.3. LSASS Audit Mode

Audit mode to identify LSA plug-ins and drivers that will fail to load in LSA Protection mode. While in the audit mode, the system will generate event logs, identifying all the plug-ins and drivers that will fail to load under LSA if LSA Protection is enabled.

Registry Change

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe
Value Name	AuditLevel
Value Type	REG_DWORD
Enabled Value	00000008

After this, it was start creating two events, Event **3065** and **3066**.

5.4. UAC restrictions to local accounts on network logon

This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk.

Registry Change

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Value Name	LocalAccountTokenFilterPolicy
Value Type	REG_DWORD
Enabled Value	0

6. RDP Over SSL

Path: Computer Configuration > Windows Components > Remote Desktop Services > Remote Desktop Session Host/Security

Policy Name	Domain Controller	Member Server
Require use of specific security layer for remote (RDP) connections	Enabled *SSL*	Enabled *SSL*
Server authentication certificate template	Enabled *RDPAuth*	Enabled *RDPAuth*
Set client connection encryption level	Enabled *High Level*	Enabled *High Level*

7. Recommended Settings

7.1. Disable SMBv1

Configure SMB v1 server

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Value Name	SMB1
Value Type	REG_DWORD
Disabled Value	0

If **“SMB1”** value is **1**, then it is enabled. If its value is set to **0**, then it is disabled.

Configure SMB v1 client driver

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SYSTEM\CurrentControlSet\Services\MrxSmb10
Value Name	Start
Value Type	REG_DWORD
Disabled Value	4

Value **4** means **“Disable Driver”**, **3** means **“Manual Start”**, **2** means **“Automatic Start”.**

Configure SMB v1 client driver (dependencies)

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SYSTEM\CurrentControlSet\Services\LanmanWorkstation
Value Name	DependOnService
Value Type	REG_MULTI_SZ
Disabled Value	“Bowser”,”MRxSmb20”,”NSI”

Value **4** means **“Disable Driver”**, **3** means **“Manual Start”**, **2** means **“Automatic Start”.**

7.2. Disable IP Source Routing

IP source routing protection level (protects against packet spoofing)

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	System\CurrentControlSet\Services\Tcpip\Parameters
Value Name	DisableIPSourceRouting
Value Type	REG_DWORD
Disabled Value	2

Value 0 means **“No additional protection, source routed packets are allowed”**
Value 1 means **“Medium, source routed packets ignored when IP forwarding is enabled”**
Value 2 means **“Highest protection, source routing is completely disabled”**

7.3. Disable ICMP Redirect

Disallow ICMP redirects to override OSPF generated routes

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	System\CurrentControlSet\Services\Tcpip\Parameters

Value Name	EnableICMPRedirect
Value Type	REG_DWORD
Disabled Value	0

7.4. Ignore NetBios name release request

Allow the computer to ignore NetBIOS name release requests except from WINS servers

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	System\CurrentControlSet\Services\Netbt\Parameters
Value Name	NoNameReleaseOnDemand
Value Type	REG_DWORD
Enabled Value	1

7.5. Enable Safe DLL search mode

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SYSTEM\CurrentControlSet\Control\Session Manager
Value Name	SafeDllSearchMode
Value Type	REG_DWORD
Enabled Value	1

7.6. Disable IPv6

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
Value Name	DisabledComponents
Value Type	REG_DWORD
Enabled Value	0xFF (IPv6 disabled)

8. Configure Transport Layer Security (TLS)

For more information regarding TLS configuration, please read the article [2] from resource links.

8.1. Disable TLS 1.0 and TLS 1.1

Registry entries needs to be created as they are not available by default. So, below entries should be configured as "Create" for registry entries. **Make sure, TLS 1.2 registry entries should be created after disabling TLS 1.0 and 1.1.**

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
Value Name	Enabled
Value Type	REG_DWORD
Disabled Value	0

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client
Value Name	Enabled
Value Type	REG_DWORD
Disabled Value	0

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
Value Name	Enabled
Value Type	REG_DWORD
Disabled Value	0

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client
Value Name	Enabled
Value Type	REG_DWORD
Disabled Value	0

8.2. Enable TLS 1.2

Registry entries needs to be created as they are not available by default. So, below entries should be configured as "Create" for registry entries.

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server
Value Name	Enabled
Value Type	REG_DWORD
Enabled Value	1

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
Value Name	Enabled
Value Type	REG_DWORD
Enabled Value	1

9. Protected Users Group

"Protected User" is an active directory group which was introduced in Windows Server 2012 R2. This security group is designed as part of a strategy to manage credential exposure within the enterprise. Members of this group automatically have non-configurable protections applied to their accounts. Membership in the Protected Users group is meant to be restrictive and proactively secure by default. The only method to modify these protections for an account is to remove the account from the security group.

Group Name	Members of the group
Protected User (AD Group)	• Account Operators • Administrator account • Administrators group • Backup Operators • Cryptographic Operators • DHCP Administrators • DHCP Users • DnsAdmins • Domain Admins • Enterprise Admins • Schema Admins • Server Operators

9.1. Benefits

Members of the Protected Users group who are signed-on to Windows 8.1 devices and Windows Server 2012 R2 hosts can no longer use:

- Default credential delegation (CredSSP) - plaintext credentials are not cached even when the Allow delegating default credentials policy is enabled
- Windows Digest - plaintext credentials are not cached even when they are enabled
- NTLM - NTOWF is not cached
- Kerberos long term keys - Kerberos ticket-granting ticket (TGT) is acquired at logon and cannot be re-acquired automatically
- Sign-on offline - the cached logon verifier is not created

If the domain functional level is Windows Server 2012 R2, members of the group can no longer:

- Authenticate by using NTLM authentication
- Use Data Encryption Standard (DES) or RC4 cipher suites in Kerberos pre-authentication
- Be delegated by using unconstrained or constrained delegation
- Renew user tickets (TGTs) beyond the initial 4-hour lifetime

9.2. Enable Auditing

To track events, enable the following logs on domain controllers:

- Microsoft-Windows-Authentication/ProtectedUserFailures-DomainController
- Microsoft-Windows-Authentication/ProtectedUserSuccesses-DomainController

10. Resource Links

[1] https://blogs.technet.microsoft.com/secguide/2017/08/30/security-baseline-for-windows-10-creators-update-v1703-final/
[2] https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

Thank you.