Windows Server 2016 Hardening Guidelines

Version 1.1

September 2018

Response Contact	
Name	Ashish Gupta
Title	Manager - InfoSec
Address	Gurgaon Phase V
Email	
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

Version No.	Version Date	Type of Changes	Owner / 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

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 running with 2016 operating systems in Genpact managed Domains.

1.3. Abbreviations

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

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 has to 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	60 days or less	60 days or less
Minimum Password Age	1 or more days	1 or more days
Minimum Password Length	14 or more characters	14 or more characters
Passwords Must Meet Complexity Requirements	Enabled	Enabled
Store passwords using reversible encryption	Disabled	Disabled

Note: Changes in polices from old to new.

Policy Name	Old Value (OS 2012, 2008)	New Value (OS 2016)
Maximum Password Age	90 days or less	60 days or less
Minimum Password Length	8 or more characters	14 or more characters

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

2.2. 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
Allow log on locally	Administrators, Domain Admins	Administrators, Domain Admins
Allow log on through Remote Desktop Services	Administrators, Domain Admins, NT AUTHORITY\Authenticated Users	Administrators, Domain Admins, NT AUTHORITY\Authenticated Users
Change the system time	Administrators, Domain Admins, LOCAL SERVICES	Administrators, Domain Admins, LOCAL SERVICES
Change the time zone	Administrators, Domain Admins, LOCAL SERVICES	Administrators, Domain Admins, LOCAL SERVICES
Create a pagefile	Administrators	Administrators
Create a token object	No One	No One
Create permanent shared objects	No One	No One
Debug programs	Administrators	Administrators
Deny access to this computer from the network	NT AUTHORITY\ANONYMOUS LOGON, BUILTIN\Guests, Local Accounts	NT AUTHORITY\ANONYMOUS LOGON, BUILTIN\Guests, Local Accounts
Enable computer and user accounts to be trusted for delegation	Administrators	No One
Force shutdown from a remote system	Administrators	Administrators
Impersonate a client after authentication	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE, IIS_USERS
Load and unload device drivers	Administrators	Administrators
Log on as a batch job	Administrators, **[Service Accounts]**	[Service Accounts]
Log on as a service	Administrators, **[Service Accounts]**	**[Service Accounts]**
Manage auditing and security log	Exchange Servers, Administrators	Administrators

Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Shut down the system	Administrators	Administrators
Synchronize directory service data	No One	
Take ownership of files or other objects	Administrators	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	Rename and disabled local Administrator
Accounts: Rename guest account	Not Applicable	Rename and disabled local Guest
Accounts: Guest account status	Not Applicable	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled
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: Do not display last user name	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: 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: Disconnect clients when logon hours expire	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled
Network access: Remotely accessible registry paths and sub-paths	Not Defined	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	Classic - local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled
Network security: LDAP client signing requirements	Negotiate Signing	Negotiate Signing
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
System objects: Require case insensitivity for non – Windows subsystems	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Highest protection, source routing is completely disabled	Highest protection, source routing is completely disabled
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Enabled	Enabled
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: Virtualize file and registry write failures to per-user locations	Enabled	Enabled

2.3. 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 Center (CDC) for additional information.

2.3.1. Application

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
Retain Old Events	Disabled	Disabled

2.3.2. 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
Retain Old Events	Disabled	Disabled

2.3.3. 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
Retain Old Events	Disabled	Disabled

2.4. System Services

Windows Server Services Configuration				
Policy Path : Computer Configuration\Windows Settings\Security Settings\System Services\				
Display Name	**Service Reg Name**	**Status**	**2016 [Domain Controller]**	**2016 [Member Server]**
Application Experience	AeLookupSvc	Manual	Stopped	Stopped
Application Identity	AppIDSvc	Manual	Stopped	Stopped
Application Information	Appinfo	Manual	Started	Started
Application Layer Gateway Service	ALG	Automatic	Started	Stopped
Application Management	AppMgmt	Automatic	Started	Stopped
Background Intelligent Transfer Service	BITS	Manual	Started	Started
Base Filtering Engine	BFE	Automatic	Started	Started
Block Level Backup Engine Service	Wbengine	Manual	Started	Stopped
Certificate Propagation	CertPropSvc	Manual	Started	Started
CNG Key Isolation	KeyIso	Manual	Started	Started
COM+ Event System	EventSystem	Automatic	Started	Started
COM+ System Application	COMSysApp	Manual	Stopped	Started
Computer Browser	Browser	Automatic	Started	Started
Credential Manager	VaultSvc	Manual	Stopped	Stopped
Cryptographic Services	CryptSvc	Automatic	Started	Started
DCOM Server Process Launcher	DcomLaunch	Automatic	Started	Started
Desktop Window Manager Session Manager	UxSms	Automatic	Not Available	Not Available
DFS Namespace	Dfs	Automatic	Started	Started
DFS Replication	DFSR	Automatic	Started	Started
DHCP Client	Dhcp	Automatic	Started	Started
Diagnostic Policy Service	DPS	Automatic	Started	Started
Diagnostic Service Host	WdiServiceHost	Disabled	Stopped	Stopped
Diagnostic System Host	WdiSystemHost	Disabled	Stopped	Stopped
Diagnostics Tracking Service	DiagTrack	Automatic	Started	Started
Disk Defragmenter (Optimize Drive)	Defragsvc	Manual	Stopped	Stopped
Distributed Link Tracking Client	TrkWks	Automatic	Started	Started
Distributed Transaction Coordinator	MSDTC	Manual	Started	Stopped
DNS Client	Dnscache	Automatic	Started	Started
Encrypting File System (EFS)	EFS	Manual	Stopped	Stopped
Extensible Authentication Protocol	EapHost	Manual	Stopped	Stopped
File Replication Service	NtFrs	Automatic	Not Available	Not Available
Function Discovery Provider Host	fdPHost	Manual	Stopped	Stopped

Function Discovery Resource Publication	FDResPub	Manual	Stopped	Stopped
Group Policy Client	Gpsvc	Automatic	Started	Started
Health Key and Certificate Management	Hkmsvc	Manual	Stopped	Stopped
Human Interface Device Access	Hidserv	Manual	Stopped	Stopped
IKE and AuthIP IPsec Keying Modules	IKEEXT	Automatic	Started	Started
Interactive Services Detection	UI0Detect	Manual	Stopped	Stopped
Internet Connection Sharing (ICS)	SharedAccess	Disabled	Stopped	Stopped
Internet Explorer ETW Collector Service	IEEtwCollectorService	Manual	Stopped	Stopped
Intersite Messaging	IsmServ	Automatic	Started	Not Available
IP Helper	Iphlpsvc	Disabled	Stopped	Stopped
IPsec Policy Agent	PolicyAgent	Manual	Started	Started
Kerberos Key Distribution Center	Kdc	Automatic	Started	Not Available
KtmRm for Distributed Transaction Coordinator	KtmRm	Manual	Stopped	Stopped
Link-Layer Topology Discovery Mapper	Lltdsvc	Manual	Stopped	Stopped
Microsoft Fibre Channel Platform Registration Service	FCRegSvc	Manual	Not Available	Not Available
Microsoft iSCSI Initiator Service	MSiSCSI	Manual	Stopped	Stopped
Microsoft Software Shadow Copy Provider	Swprv	Manual	Stopped	Stopped
Multimedia Class Scheduler	MMCSS	Disabled	Stopped	Stopped
Netlogon	Netlogon	Automatic	Started	Started
Network Access Protection Agent	Napagent	Manual	Stopped	Stopped
Network Connections	Netman	Manual	Started	Started
Network List Service	Netprofm	Manual	Started	Started
Network Location Awareness	NlaSvc	Automatic	Started	Started
Network Store Interface Service	Nsi	Automatic	Started	Started
Performance Counter DLL Host	PerfHost	Manual	Stopped	Stopped
Performance Logs & Alerts	pla	Manual	Started	Started
Plug and Play	PlugPlay	Automatic	Started	Started
PnP-X IP Bus Enumerator	IPBusEnum	Disabled	Stopped	Stopped
Portable Device Enumerator Service	WPDBusEnum	Manual	Started	Started
Power	Power	Automatic	Started	Started
Print Spooler	Spooler	Disabled	Stopped	Stopped

Problem Reports and Solutions Control Panel Support	Wercplsupport	Disabled	Stopped	Stopped
Protected Storage	ProtectedStorage	Manual	Not Available	Not Available
Remote Access Auto Connection Manager	RasAuto	Manual	Stopped	Stopped
Remote Access Connection Manager	RasMan	Manual	Stopped	Stopped
Remote Desktop Configuration	SessionEnv	Manual	Started	Started
Remote Desktop Services	TermService	Manual	Started	Started
Remote Desktop Services UserMode Port Redirector	UmRdpService	Manual	Started	Started
Remote Procedure Call (RPC)	RpcSs	Automatic	Started	Started
Remote Procedure Call (RPC) Locator	RpcLocator	Automatic	Stopped	Stopped
Remote Registry	RemoteRegistry	Automatic	Started	Started
Resultant Set of Policy Provider	RSoPProv	Automatic	Started	Stopped
Routing and Remote Access	RemoteAccess	Disabled	Stopped	Stopped
RPC Endpoint Mapper	RpcEptMapper	Automatic	Started	Started
Secondary Logon	Seclogon	Manual	Stopped	Started
Secure Socket Tunneling Protocol Service	SstpSvc	Manual	Stopped	Stopped
Security Accounts Manager	SamSs	Automatic	Started	Started
Server	LanmanServer	Automatic	Started	Started
Shell Hardware Detection	ShellHWDetection	Disabled	Stopped	Stopped
Smart Card	SCardSvr	Manual	Stopped	Stopped
Smart Card Removal Policy	SCPolicySvc	Manual	Stopped	Stopped
SNMP Trap	SNMPTRAP	Disabled	Stopped	Stopped
Software Protection	Sppsvc	Automatic (Delayed Start, Started)	Stopped	Stopped
Special Administration Console Helper	Sacsvr	Manual	Stopped	Stopped
SPP Notification Service	Sppuinotify	Manual	Not Available	Not Available
SSDP Discovery	SSDPSRV	Disabled	Stopped	Stopped
System Event Notification Service	SENS	Automatic	Started	Started
Task Scheduler	Schedule	Automatic	Started	Started
TCP/IP NetBIOS Helper	Lmhosts	Automatic	Started	Started
Telephony	VaultSvc	Manual	Stopped	Stopped
Telnet Client	Telnet	Disabled	Stopped	Stopped
Thread Ordering Server	THREADORDER	Manual	Stopped	Stopped
UPnP Device Host	Upnphost	Disabled	Stopped	Stopped
User Profile Service	ProfSvc	Automatic	Started	Started
Virtual Disk	Vds	Automatic	Started	Started
Volume Shadow Copy	VSS	Automatic	Started	Started
Windows Audio	AudioSrv	Manual	Started	Stopped

Windows Audio Endpoint Builder	AudioEndpointBuilder	Manual	Started	Stopped
Windows Color System	WcsPlugInService	Manual	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	Stopped	Stopped
Windows Event Log	EventLog	Automatic	Started	Started
Windows Firewall	MpsSvc	Automatic	Started	Started
Windows Font Cache Service	FontCache	Disabled	Stopped	Started
Windows Installer	Msiserver	Automatic	Stopped	Stopped
Windows Management Instrumentation	Winmgmt	Automatic	Started	Started
Windows Modules Installer	TrustedInstaller	Manual	Stopped	Stopped
Windows Remote Management (WS-Management)	WinRM	Automatic (Delayed Start)	Started	Started
Windows Time	W32Time	Manual	Started	Started
Windows Update	Wuauserv	Automatic (Delayed Start)	Started	Started
WinHTTP Web Proxy Auto-Discovery Service	WinHttpAutoProxySvc	Automatic	Started	Stopped
Wired AutoConfig	dot3svc	Manual	Stopped	Stopped
WMI Performance Adapter	wmiApSrv	Manual	Stopped	Stopped
Workstation	LanmanWorkstation	Automatic	Started	Started

2.5. Public Key Policies

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

2.5.1. Certificate Services Client – Auto-Enrolment Settings

<table>
<tr><td colspan="3">Public Key Policies</td></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><td><b>Policy Name</b></td><td><b>Recommended Settings (Domain Controller)</b></td><td><b>Recommended Settings (Member Servers)</b></td></tr>
<tr><td>Configuration Model</td><td>Enabled</td><td>Enabled</td></tr>
<tr><td colspan="3">☑ Renew expired certificate, update pending certificate, and remove revoked certificates.</td></tr>
<tr><td colspan="3">☑ Update certificates that use certificate templates</td></tr>
</table>

2.5.2. 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".

2.5.3. 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".

2.6. Advance Audit Configuration Policy

2.6.1. Account Management

Account Management		
Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Audit Computer Account Management	Success, Failure	Success, Failure
Audit Other Account Management Events	Success, Failure	Success, Failure
Audit Security Group Management	Success, Failure	Success, Failure
Audit User Account Management	Success, Failure	Success, Failure

2.6.2. DS Access

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

2.6.3. Logon / Logoff

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

2.6.4. Audit Policy Change

Audit Policy Change		
Policy Path : Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration		
Policy Name	**Recommended Settings (Domain Controller)**	**Recommended Settings (Member Servers)**
Detailed Tracking Process Creation	Success	Success
Policy Change: Audit Policy Change	Success	Success
Policy Change: Authentication Policy Change	Success	Success
Account logon: Credential Validation	Success, Failure	Success, Failure

2.6.5. System

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

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. Network Provider

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

3.2.5. Offline Files

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

3.2.6. TCP IP Settings

Policy Name [Parameters]	Domain Controller	Member Server

Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents	0xff (255)	0xff (255)

3.3. System

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

3.3.1. 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

3.3.2. Kerberos

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

3.3.3. Local Services

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

3.3.4. Logon

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

3.3.5. 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

3.3.6. Remote Assistance

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

3.3.7. 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. Location and Sensors

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

3.4.5. 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	Enabled	Enabled
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 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 Idle session limit: **2 Hours**	Enabled	Enabled

3.4.6. Store

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

3.4.7. Windows Media Digital Rights Management

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

3.4.8. Windows PowerShell

Policy Name	Domain Controller	Member Server
Turn on Script Execution Execution Policy: **Allow local scripts and remote signed scripts**	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.

Thank you.