



Windows Server 2016 Security

Table of Contents

1. Protecting Credentials in Windows Server	4
1.1 Using the Protected Users group	4
1.2 Using account preferences	5
1.3 Using Windows Defender Credential Guard	7
1.4 Using the Local Administrator Password Solution	8
1.5 Using the Active Directory Administrative Center	8
2. Logging and Auditing Windows Server	9
2.1 Logging and Auditing Windows Server	9
2.2 Auditing and Advanced Auditing	10
2.3 Audit Collection Services	12
2.4 Windows PowerShell Logging	12
3. Privileged Access Management in Windows Server	13
3.1 User Rights	13
3.2 Delegation of Control wizard	14
3.3 Privileged Access Workstation	15
3.4 Just Enough Administration (JEA)	16
3.5 Securing domain controllers	17
3.6 ESAE forests	18
3.7 Just-in-time (JIT) administration	18
3.8 Microsoft Identity Manager (MIM)	19
4. Protecting Data in Windows Server	20
4.1. File Server Resource Manager (FSRM)	20
4.2. Encrypting File System (EFS)	21
4.3. BitLocker	22

5. Mitigating Malware and Threats in Windows Server	23
5.1. Windows Defender Security Center App	23
5.2. Windows Defender Device Guard	24
5.3. Control Flow Guard	24
5.4. Software Restriction Policies (SRPs)	25
5.5. AppLocker	25
5.6. Security Compliance Toolkit (SCT)	26
6. Securing Virtualization Environment in Windows Server	27
6.1. Guarded Fabric	27
6.2. Shielded VMs	28
7. Securing Application Development in Windows Server	29
7.1. Containers	29
7.2. Docker	30
7.3. Nano Server	30
8. Securing Network Connections in Windows Server	31
8.1. Windows Firewall with Advanced Security	31
8.2. IPsec	32
8.3. Message Analyzer	33
Useful References	34
About Netwrix	34

1. Protecting Credentials in Windows Server

Credentials are the keys to an account. By harvesting credentials, attackers can enter your network, move laterally and escalate their privileges to steal your data. Windows Server 2016 has several features for minimizing the chance that attackers will be able to harvest credentials.

1.1 Using the Protected Users group

Putting users, especially highly privileged users, in the “Protected Users” group helps you protect against compromise of their credentials by disabling authentication options that are less secure. For example, Windows does not cache the credentials of members of this group locally, so they are never left on workstations for attackers to harvest. In addition, user accounts that are members of this group cannot:

- Use default credentials delegation
- Use Windows Digest
- Use NTLM
- Use Kerberos long-term keys
- Sign on offline
- Use NT LAN Manager (NTLM) for authentication
- Use DES for Kerberos pre-authentication
- Use RC4 cipher suites for Kerberos pre-authentication
- Be delegated privileges using constrained delegation
- Be delegated privileges using unconstrained delegation
- Renew user ticket-granting tickets (TGTs) past the initial 240-minute lifetime

1.2 Using account preferences

User Accounts

For user accounts that need less stringent protection, you can use the following security options, which are available for any AD account:

- **Logon Hours** — Enables you to specify when users can use an account.
- **Logon Workstations** — Enables you to limit the computers the account can sign in to.
- **Password Never Expires** — Absolves the account from the “Maximum password age” policy setting; don’t configure this option for privileged accounts.
- **Smart card is required for interactive logon** — Requires a smart card to be presented for the account to sign in.
- **Account is sensitive and cannot be delegated** — Ensures that trusted applications cannot forward the account’s credentials to other services or computers on the network.
- **This account supports Kerberos AES 128-bit encryption** — Allows Kerberos AES 128-bit encryption.
- **This account supports Kerberos AES 256-bit encryption** — Allows Kerberos AES 256-bit encryption. Use this option for privileged accounts.
- **Account expires** — Enables you to specify an end date for the account.

Computer Accounts

In addition to controlling user accounts, you also need to understand and manage the reach of computer and service accounts. When you join a computer to the domain for the first time, Windows creates a computer account in Active Directory in the “Computers” container and automatically assigns it a password. AD manages these passwords and updates them automatically every 30 days.

To manage the permissions of computer accounts and control which Group Policies are applied to them, you can add them to groups and move them to different OUs. You can also disable and reset computer accounts:

- **Disabling** a computer account means that the computer cannot connect to the domain anymore. If you delete a computer account and the computer is still operational, you’ll need to rejoin the computer to the domain if you want it to regain domain membership.
- **Resetting** a computer account removes the connection between the computer and the domain.

Service Accounts

Service accounts are a special type of account that Windows services use to interact with the operating system and resources on the network. (It's also possible to create user accounts and configure them to run as service accounts, but that is not convenient.)

There are three types of built-in service accounts:

- **Local system** — The NT AUTHORITY\SYSTEM account has privileges equivalent to the local Administrators group on the computer.
- **Local service** — The NT AUTHORITY\LocalService account has privileges equivalent to the local Users group on the computer.
- **Network service** — The NT AUTHORITY\NetworkService account has privileges equivalent to the local Users group on the computer.

To protect these accounts, ensure a sysadmin updates their passwords on a regular basis. This is a manual process if you use native tools.

Group Managed Service Accounts and Virtual Accounts

A Group Managed Service Account is a special type of service account; AD automatically updates the passwords of these accounts. A virtual account is the computer-specific local equivalent of a Group Managed Service Account.

1.3 Using Windows Defender Credential Guard

Windows Defender Credential Guard is a new technology in Windows 10 and Windows Server 2016 that helps to protect credentials from attackers who try to harvest them by using malware. Windows Defender Credential Guard uses virtualization-based security that allows you to isolate secrets, such as cached credentials, so that only privileged software can access them.

In virtualization-based security, the specific processes that use credentials or data, and the memory associated with those processes, run in a separate operating system parallel with, but independent of, the host operating system. This virtual operating system protects processes from attempts by any external software to read the data that those processes store and use. Windows Defender Credential Guard takes advantage of hardware security, including secure boot and virtualization.

You can manage Windows Defender Credential Guard using Group Policy, Windows Management Instrumentation (WMI), or Windows PowerShell.

Windows Defender Credential Guard does not allow the use of:

- Unconstrained Kerberos delegation
- NT LAN Manager version 1 (NTLMv1)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2)
- Digest
- Credential Security Support Provider (CredSSP)
- Kerberos DES encryption

1.4 Using the Local Administrator Password Solution

Microsoft's Local Administrator Password Solution (LAPS) provides a secure central repository for the passwords all built-in local Administrator accounts and automates proper management of those passwords. In particular, LAPS:

- Ensures that local administrator passwords are unique on each computer
- Automatically changes all local administrator passwords every 30 days
- Provides configurable permissions to control access to passwords
- Transmits passwords to the client in a secure, encrypted manner

1.5 Using the Active Directory Administrative Center

The Active Directory Administrative Center enables you to search your Active Directory for accounts that are ripe for takeover by attackers. In particular, you should regularly look for the following types of accounts:

- **User accounts whose passwords never expire** — You should avoid configuring accounts with fixed passwords because they are less secure than accounts with passwords that users have to update periodically.
- **Inactive user accounts** — Inactive user accounts usually belong to a person who has left the organization. The Active Directory Administrative Center console enables you to find accounts that haven't signed in for a specified number of days.

Deleting or disabling these user accounts prevents them from being misused by outside attackers or malicious insiders.

2. Auditing Windows Server

Continuously auditing the activity in your network is one of the most critical security best practice, since it helps you notice potentially malicious activity early enough to take action and prevent data breaches, system downtime and compliance failures.

2.1 Event Logs and Event Log Forwarding

Event logs record the activity on a particular computer. When you configure auditing properly, almost all events that have security significance are logged. This makes event logs the first thing to look at during IT security investigations. Here are two important tips:

- Configure the event log size to the maximum (4GB) to minimize the chance that events will be overwritten because the log becomes full.
- Archive your event logs, so if you do detect an attack, you can look at older event logs to find out exactly when and how attackers were able to compromise the system.

Event Log Forwarding

You should also move event logs off your computers regularly, because attackers often scrub event logs to escape detection. Windows Server's event log forwarding feature enables you to automatically forward events logs from all your computers to a designated machine (the event collector) that stores them all securely. There are two types of event subscriptions:

- **Source-initiated subscriptions** allow you to define an event subscription on the event collector computer without defining the source computers. Then you use Group Policy to control which source computers forward events to the event collector.
- **Collector-initiated subscriptions** allow you to create an event subscription that specifies the source computers that will forward event logs.

You can learn more about how to configure event log forwarding by reading [this article](#).

2.2 Auditing and Advanced Auditing

Auditing policies enable you to record a variety of activities to the Windows security log. You then can examine these auditing logs to identify issues that need further investigation. Auditing successful activities provides documentation of changes so you can troubleshoot which changes led to a failure or a breach. Logging failed attempts can spot malicious hackers or unauthorized users to access enterprise resources.

Your auditing policy specifies the categories of security-related events that you want to audit. Here are the basic policy settings you can configure and what happens if you turn them on:

- **Audit account logon events** — Creates an event when a user or computer attempts to use a Windows Server Active Directory account to authenticate.
- **Audit account management** — Audits events such as the creation, deletion or modification of a user, group or computer account and the resetting of user passwords.
- **Audit directory service access** — Audits events that are specified in the system access control list, such as permissions.
- **Audit logon events** — Creates an event when a user logs on to a computer interactively (locally) or over the network (remotely).
- **Audit object access** — Audits access to objects such as files, folders, registry keys and printers that have their own SACLs.
- **Audit policy change** — Audits changes to user rights assignment policies, audit policies and trust policies.
- **Audit privilege use** — Audits attempts to use permissions or user rights. You can choose whether to audit successful attempts, failed attempts or both.
- **Audit process tracking** — Audits process-related events, such as process creation, process termination, handle duplication and indirect object access.
- **Audit system events** — Audits system restarts and shutdowns, and changes that affect the system or security logs.

Advanced Audit Policy

Since Windows Server 2008 R2, administrators can audit more specific events using advanced audit policy settings in the following categories:

- **Account Logon** — These settings control auditing of the validation of credentials and other Kerberos-specific authentication and ticket operation events.
- **Account Management** — These policy settings are related to the modification of user accounts, computer accounts, group membership changes, and the logging of password change events.
- **Detailed Tracking** — These settings control the auditing of encryption events, Windows process creation and termination events, and remote procedure call (RPC) events.
- **DS Access** — These policy settings determine whether to track access to AD, AD changes and replication.
- **Logon/Logoff** — This group of settings control auditing of standard logon and logoff events.
- **Object Access** — These settings cover access to AD, the registry, applications and file storage.
- **Policy Change** — These settings control tracking of changes to policy settings.
- **Privilege Use** — These settings determine whether to audit privilege use attempts within the Windows environment.
- **System**. These settings are used to audit changes to the state of the security subsystem.
- **Global Object Access Auditing**. These settings are for controlling the SACL settings for all objects on one or more computers.

You can learn how to properly configure Windows Server auditing by reading [Windows Server Auditing Quick Reference Guide](#) and [Audit Policy Best Practices](#).

2.3 Audit Collection Services

Windows Server provides a tool for pulling security logs from servers running Windows Server to a centralized location in order to simplify security auditing and log analysis — Audit Collection Services (ACS). ACS is an agent-based utility that aggregates the logs into a Microsoft SQL Server database.

By default, when an audit policy is implemented on a Windows-based computer, that computer automatically saves all events generated by the audit policy to its local security log. Using ACS, organizations can consolidate all those individual security logs into a centrally managed database, and then filter and analyze the events using the data analysis and reporting tools in Microsoft SQL Server.

2.4 Windows PowerShell Logging

Administrators can use Windows PowerShell to enable or disable logging at the Windows PowerShell module level. By default, all logging in Windows PowerShell is disabled. You can enable it by setting the “LogPipelineExecutionDetails” property to “\$true”; to disable it again, set the property back to “\$false”.

Windows PowerShell also offers a detailed script tracing feature that makes it possible to enable detailed tracking and analysis of the use of Windows PowerShell scripting on a system. If you enable detailed script tracing, Windows PowerShell logs all script blocks to the Event Tracing for Windows (ETW) event log in the “Microsoft-Windows-PowerShell/Operational” path.

3. Privileged Access Management in Windows Server

Many organizations struggle to secure their systems because their Active Directory is already compromised. AD is usually compromised by insiders or successful attacks on them. So how to keep environment protected even when a privileged your account got hacked?

3.1 User Rights

User rights determine which tasks a user account can complete. Best practices require assigning user rights in accordance with the principle of least privilege — each user should have the minimum rights required to do their assigned tasks. This limits the damage the account owner can do, either intentionally or accidentally, and also minimizes the reach of an attacker who gains control of an account. The best practice is to assign users right by adding them to groups that have been assigned the appropriate permissions. You can also assign user accounts rights directly, by assigning the account the rights in Group Policy, but this is not recommended because it makes it difficult to keep track of permissions and adhere to the least-privilege principle.

Unfortunately, organizations tend to grant accounts more privileges than they need because it's convenient — it's easier to add an account to the local Administrators group on a computer, for instance, than it is to figure out the precise privileges that the account needs and add the user to the proper groups. Lack of communication and standard procedures also often results in failure to revoke privileges that users no longer need as they change roles within the organization. As a result, these organizations are at unnecessary risk for data loss, downtime and compliance failures.

3.2 Delegation of Control wizard

Organizations often want to enable certain staff members to do perform specific administrative tasks without giving them full administrative privileges. For instance, they might want to enable IT operations personnel to reset user passwords but not create or delete accounts. To help, Microsoft Windows Server 2016 offers the Delegation of Control wizard, which enables you to delegate the following privileges:

- Create, delete, and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete, and manage groups
- Change group membership
- Manage Group Policy links
- Generate Resultant Set of Policy (Planning)
- Generate Resultant Set of Policy (Logging)
- Create, delete, and manage inetOrgPerson accounts
- Reset inetOrgPerson passwords and force password change at next logon
- Read all inetOrgPerson information

You can learn more about this capability by reading [Active Directory Delegated Permissions Best Practices](#).

3.3 Privileged Access Workstation

Another integral part of securing an environment is to ensure that IT admins use only secure Windows servers for tasks that require administrative privileges. They should use other machines for daily tasks, such as browsing the Internet, responding to email, and opening files authored by other people, since those actions increase the risk of a host being compromised.

A Privileged Access Workstation (PAW), or secure administrative host, is a special computer that you use only for performing privileged tasks. To create a PAW, you must:

- Ensure that only authorized users can sign in to the host.
- Use Device Guard and AppLocker policies to restrict application execution to trusted applications that your organization's employees use to perform administrative tasks.
- Enable Windows Defender Credential Guard to help protect against credential theft.
- Enable BitLocker to help protect the boot environment and the hard disk drives from tampering.
- Ensure that PAW is blocked from accessing all external sites by the perimeter network firewall.
- Block Remote Desktop Protocol (RDP), Windows PowerShell and management console connections from any computer that is not a PAW.
- Configure sign-in restrictions for accounts that are used to perform administrative actions.

Jump servers

A jump server is a special server that users connect to using Remote Desktop when they want to perform administrative tasks. You should configure jump servers in a manner similar to Privileged Access Workstations. The difference is that instead of signing in locally, a member of the IT operations team makes a Remote Desktop connection to the jump server and then signs in to the jump server with an account that has the required administrative permissions. The drawback of jump servers is that the computer that makes the connection to a jump server might be compromised by malware because you use it to browse the Internet, read email, open files and so on. In highly secure environments, you can use jump servers in conjunction with Privileged Access Workstations.

3.4 Just Enough Administration (JEA)

Just Enough Administration is a new administrative technology that enables you to apply role-based access control (RBAC) principles through Windows PowerShell remote sessions. Instead of assigning users general roles that grant them more permissions than they need to do their jobs, you can use JEA to configure special Windows PowerShell endpoints that provide the functionality necessary to perform a specific task: An authorized user can connect to the endpoint and use a specific set of Windows PowerShell cmdlets, parameters and parameter values. The tasks are performed by a privileged virtual account, rather than the user's account.

The advantages of this approach include the following:

- The user's credentials are not stored on the remote system.
- The user account used to connect to the endpoint does not need to be privileged.
- The virtual account is limited to the system on which it is hosted.
- The virtual account has local administrator privileges but is limited to performing only the activities defined by JEA.

3.5 Securing domain controllers

Domain controllers are one of the most valuable targets on a network; an attacker who compromise a DC has control of all domain identities. To secure your DCs, consider taking the following steps:

- Ensure that all domain controllers run the most recent version of the Windows Server operating system and have current security updates.
- Deploy domain controllers using the “Server Core” installation option rather than the “Server with a Desktop” option.
- Keep physically deployed domain controllers in dedicated secure racks that are separate from other servers.
- Deploy domain controllers on hardware that includes a Trusted Platform Module (TPM) chip, and configure all volumes with BitLocker Drive Encryption.
- Run virtualized domain controllers either on separate virtualization hosts or as shielded virtual machines on a guarded fabric.
- Use Security Compliance Manager to apply configuration baselines to domain controllers.
- Use AppLocker and Device Guard to control the execution of executables and scripts on your domain controllers.
- Use the Group Policy assigned to the Domain Controllers OU to ensure that RDP connections can be made only from jump servers and Privileged Access Workstations.
- Configure the perimeter firewall to block outbound connections from domain controllers to the internet.

3.6 ESAE forests

An Enhanced Security Administrative Environment (ESAE) forest, also called a “red forest,” is a special Active Directory forest that hosts privileged accounts. Putting privileged accounts in an ESAE forest makes it easier to apply more restrictive policies to protect them. An ESAE forest is configured with a one-way trust relationship with a production forest — accounts from the ESAE forest can be used in the production forest, but accounts in the production forest cannot be used in the ESAE forest. The production forest is configured so that administrative tasks can be performed there only by accounts hosted in the ESAE forest.

ESAE forests have the following benefits:

- **Locked-down accounts.** Standard user accounts in the ESAE forest can be configured as highly privileged in the production forest.
- **Selective authentication.** Accounts in the ESAE forest can sign in only to specific hosts in the production forest.
- **Simple way to improve security.** Because privileged administrative accounts are hosted in a separate forest, it is easy to apply more stringent security requirements (such as requiring multifactor authentication) to them than to the standard user accounts in the production forest.

3.7 Just-in-time (JIT) administration

JIT administration is the idea of granting privileges to users when they need them to do a particular task, and only for a limited amount of time, rather than permanently. This limits the usefulness of the accounts to an attacker who compromises them, and also minimizes the opportunity for the account owner to accidentally or deliberately misuse the elevated privileges. JIT is implemented by granting the user temporary membership in a security group that has the required privileges.

When properly implemented, this approach can provide the following security improvements:

- All accounts that the IT Operations team uses are standard user accounts.
- All requests for privileges are logged.
- Privileges are temporary.

Once privileges are granted, a user must establish a new session (either by opening a new Windows PowerShell session or by signing out and signing in again) in order to leverage the new temporary group memberships and the associated permissions.

3.8 Microsoft Identity Manager (MIM)

Active Directory Domain Services (AD DS) allows you to create, modify and delete user accounts, but provides very few tools to automate lifecycle management of those accounts. MIM is an on-premises identity and access management solution that fills that gap. For example, with MIM, you can enable users to use a self-service portal to reset their own passwords, and allow identity synchronization between your on-premises identity stores and those in cloud applications.

You can use MIM to manage:

- Users
- Credentials
- Policies
- Access

MIM offers the following functionality:

- **Self-service password reset.** Users can reset their own forgotten passwords after they answer questions to verify their identity.
- **Self-service account lockout remediation.** Users can unlock their accounts by answering questions to verify their identity.
- **Self-service user attribute management.** Users can update certain of their own Active Directory attributes, such as their phone numbers.
- **Manage the lifecycle of Active Directory users and groups.** MIM provides tools for managing groups and users that go beyond the creation, modification and deletion functionality of AD DS.
- **Manage the lifecycle of smart cards and certificates.** MIM provides tools for managing smart cards and certificates, including certificate provisioning and renewal.
- **Role management and assignment.** MIM helps you manage RBAC functionality.
- **Password synchronization across directories.** You can synchronize passwords to other directories, including Azure Active Directory (Azure AD).
- **Privileged account management (PAM).** Admins can be assigned privileges on a temporary, rather than permanent, basis.
- **Analytics and compliance reporting.** You can analyze and report on all activity that MIM 2016 performs.

4. Protecting Data in Windows Server

Organizations today store data in many places, including both the corporate file servers and users' personal devices. To ensure both security and regulatory compliance, IT administrators need to tightly control access to data stored on file servers, and also protect data on portable devices to minimize the risk of data loss or exposure if the devices are lost or stolen.

4.1 File Server Resource Manager (FSRM)

File servers hold most of the data that your users and applications use. FSRM is a set of tools that help you understand, control and manage the quantity and type of data stored on your servers. FSRM offers:

- **Quota management.** You can create, obtain and manage information about quotas to set storage limits on volumes or folders.
- **File screening management.** You can prevent specific file types from being stored on a volume or folder, or be notified when users store these types of files.
- **Storage report management.** You can schedule and configure reports on the components and aspects of FSRM, including:
 - Quota usage
 - File screening activity
 - Files that might negatively affect capacity management, such as large files, duplicate files or unused files
 - Files listed and filtered according to owner, file group or a specific file property
- **Classification management.** You can identify, categorize and manage files using a wide array of properties.
- **File management tasks.** You can delete old files or move files to a specific location based on a file property, such as filename or file type.

4.2 Encrypting File System (EFS)

If unauthorized users have physical access to a device (for example, if they have stolen a user's laptop or smartphone), they can bypass file security to access the data. If you use EFS to protect data, unauthorized users cannot view a file's content even if they have full access to the device.

Specifically, when an authorized user opens an encrypted file, EFS decrypts the file in the background and provides an unencrypted copy to the application. Authorized users can view or modify the file, and EFS saves changes transparently as encrypted data. If unauthorized users try to do the same, they receive an "Access denied" error.

EFS provides the following important capabilities:

- EFS works at the file level, and you can have encrypted and unencrypted files on the same volume.
- EFS operates in the background and is transparent to users and applications.
- Only authorized users can access encrypted files.
- You can use data recovery agents to recover data that was encrypted by any user.
- You can use EFS to encrypt files locally or across the network.
- In File Explorer, by default, EFS shows encrypted files and folders in a different color than unencrypted files.
- EFS can encrypt data at rest only; it does not encrypt data while it is being transmitted over the network.

4.3 BitLocker

BitLocker complements EFS by providing an additional layer of protection for data stored on Windows devices. BitLocker protects devices that are lost or stolen against data theft or exposure, and it offers secure data disposal when you decommission a device.

BitLocker has the following features:

- BitLocker can encrypt an entire volume (whether it contains the Windows operating system or is a data volume) or only the used parts of a volume.
- BitLocker can use a Trusted Platform Module (TPM) to protect the integrity of the Windows startup process. BitLocker verifies that the required boot files have not been tampered with or modified.
- BitLocker can require additional authentication, such as a PIN or a USB startup key.
- You can configure network unlock at startup for BitLocker. With network unlock, the BitLocker-protected device starts automatically when it is connected to a trusted company network; otherwise, you need to provide a startup PIN.
- If a TPM fails or the password is lost, BitLocker provides a recovery mechanism, a 48-digit recovery key or a recovery agent to access the volume data.
- BitLocker protects the whole volume from offline attacks.
- You can combine BitLocker with EFS. BitLocker encrypts at the volume level, whereas EFS encrypts data at the file level.
- BitLocker overhead is minimal; for most installations, the performance impact is not noticeable.

5. Mitigating Malware and Threats in Windows Server

Malware — computer viruses, worms, Trojan horses, ransomware, spyware and so on — is a continuous threat to organizations because it can damage devices and enable unauthorized parties to access the network remotely to collect and transmit sensitive information.

5.1 Windows Defender Security Center App

The Windows Defender Server 2016 Security Center app can help you identify and remove malware from computers and other devices in your environment. Here is some of the information and functionality it provides:

- **Virus & threat protection.** Includes information about and access to antivirus settings and the Controlled folder access feature of Windows Defender Exploit Guard.
- **Device performance & health.** Provides information about drivers, storage space and Windows Update.
- **Firewall & network protection.** Includes information about and access to firewall settings, including Windows Defender Firewall settings.
- **App & browser control.** Includes exploit-protection mitigations and Windows Defender SmartScreen settings.
- **Family options.** Includes access to parental controls and family settings.

5.2 Windows Defender Device Guard

Windows Defender Device Guard is a suite of security features introduced in Windows Server 2016. When you turn it on, instead of trusting all apps except those blocked by an antivirus or other security solution, the operating system will run only the applications on a whitelist your organization defines.

Windows Defender Device Guard uses virtualization-based security to isolate the code-integrity service from the Windows kernel. Windows Defender Device Guard can block any software, even if an unauthorized user manages to take control of the operating system. You can choose exactly what can run inside your environment by using a code-integrity policy to protect your environment.

Windows Defender Device Guard is not a single feature. It's a combination of several features, such as:

- **Virtual Secure Mode.** A virtual shell that isolates the ISASS.exe process from the operating system, which reduces the risk that malicious users will compromise your users' domain credentials.
- **Windows Defender Application Control.** A Windows component that provides a rules engine to help ensure executable security.
- **Virtual Secure Mode Protected Code Integrity.** Moves the Kernel Mode Code Integrity (KMCI) and Hypervisor Code Integrity (HVCI) components into virtual secure mode to harden them from attack.
- **Platform and UEFI Secure Boot.** Secure Boot provides a high-value security benefit by using signatures and measurements to help protect boot-loader code and firmware from tampering.

5.3 Control Flow Guard

CFG is a platform security feature that helps prevent memory-corruption vulnerabilities. CFG places restrictions on where an application can execute code, which makes it harder for malicious hackers to execute subjective code through common vulnerabilities, such as buffer overflows. CFG monitors and checks certain aspects of a program's control flow, including where execution changes from straight sequential instruction. The technology that supports CFG ensures that all indirect calls result in a jump to legal targets. Malicious hackers will supply uncommon input to a running program to make it perform unexpectedly.

5.4 Software Restriction Policies (SRPs)

One of the best ways to help block malicious software and other cyber threats is to limit or restrict the software that can run in an enterprise environment.

One option is to use SRPs, which enable administrators to create rules that specify which applications can run on client devices. Rules are based on one of the following criteria:

- **Hash.** The cryptographic fingerprint of the file
- **Certificate.** A software publisher certificate that signs a file digitally
- **Path.** The local or Universal Naming Convention (UNC) path to where the file is stored
- **Zone.** The internet zone

5.5 AppLocker

AppLocker is another way to control which applications users can run. You can apply AppLocker through Group Policy to computer objects within an organizational unit (OU). You also can apply individual AppLocker rules to individual Active Directory Domain Services (AD DS) users or groups. AppLocker also contains options that you can use to monitor or audit the application of rules.

For example, you can use AppLocker to restrict software that:

- You do not want anyone to use in your company.
- Employees don't use or that you have replaced with a newer version.
- Your company no longer supports.
- Software that only specific departments should use.

You can configure the settings for AppLocker at the following location in GPMC: "Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies".

5.6 Security Compliance Toolkit (SCT)

To help protect against security threats, organizations must have well-designed security policies that cover most organizational and IT-related components. Security policies should establish a baseline for a server's fundamental security and then ensure that baseline is applied to all servers.

SCT is a set of free Microsoft tools that administrators can use to help secure the computers in their environment, regardless of whether the computers reside locally, remotely or in the cloud. You can download Microsoft-recommended security configuration baselines; test, edit and store them; and apply them to your servers. You can also compare your current GPOs with the baselines.

The main features of SCT include:

- **Policy Analyzer.** Enables you to analyze and compare sets of Group Policy objects (GPOs).
- **Local Group Policy Object Utility.** Helps automate management of local Group Policy, including importing settings from Group Policy backups, registry policy files, security templates, and advanced-auditing backup CSV files that the Policy Analyzer generates

6. Securing Virtualization Environment in Windows Server

Administrator accounts work differently in virtualized environments than they do in physical ones. In particular, in a physical environment, administrative roles, such as storage administrator, network administrator, backup operator, and virtualization-host administrator, have limited or isolated rights. In contrast, in a virtual infrastructure, each of these roles with permissions to manage the physical infrastructure might have an inappropriate level of access to the virtual infrastructure.

You can mitigate this risk by using a guarded fabric. Guarded fabric is a collective term used to describe a fabric of Microsoft Hyper-V hosts and their Host Guardian Service (HGS) that can manage and run shielded virtual machines (VMs).

6.1 Guarded Fabric

In Windows Server 2016, Microsoft introduced an improved Hyper-V security model designed to help protect hosts and their VMs from malicious software that might be inside them. Because a VM is just a file, you need to protect it from attacks from the storage system or network while it is being backed up.

Guarded fabrics can run three types of VMs:

- A normal VM that offers no protection above and beyond that of earlier versions of Hyper-V
- An encryption-supported VM whose protections can be configured by a fabric admin
- A shielded VM whose protections are switched on and cannot be disabled by a fabric admin

Host Guardian Service

HGS is the centerpiece of the guarded fabric solution. It is responsible for ensuring that Hyper-V hosts in the fabric are known to the hoster or enterprise and running trusted software.

Specifically, HGS is a new server role introduced in Windows Server 2016 That provides the Attestation Service and Key Protection Service (KPS) that enable Hyper-V to run shielded VMs. A Hyper-V host becomes a guarded host as soon as the Attestation Service affirmatively validates its identity and configuration. KPS provides the transport key that is needed to unlock and run shielded VMs.

HGS supports two different attestation modes for a guarded fabric:

- **Admin-trusted attestation (Active Directory based).** Admin-trusted attestation is intended to support existing host hardware where TPM 2.0 is not available. It requires relatively few configuration steps and is compatible with commonplace server hardware.
- **TPM-trusted attestation (hardware based).** TPM-trusted attestation offers the strongest possible protection, but also requires more configuration steps. The host's hardware and firmware must include TPM 2.0 and UEFI 2.3.1 with Secure Boot enabled.

6.2 Shielded VMs

To help protect a fabric against compromise, Windows Server 2016 with Hyper-V introduced shielded virtual machines. A shielded VM is a generation 2 VM that has a virtual TPM, is encrypted by using BitLocker Drive Encryption, and can run only on healthy and approved hosts in the fabric.

HGS manages the keys used to start up shielded VMs. Without HGS, a Hyper-V host cannot power on a shielded VM because it cannot decrypt it. HGS will not provide the keys to a Hyper-V host until that host has been measured and is considered healthy.

Here are three examples that illustrate how shielded VMs help protect against attacks:

- There is less risk if a malicious employee steals a shielded VM's .vhd files because those files are encrypted.
- HGS will not release keys to hosts with debuggers attached.
- A malicious employee who attempts to move a shielded VM to an untrusted host will discover that the new host will not be recognized. Trusted hosts are added to HGS by means of identifiers unique to their TPMs and are protected even if they are moved to another HGS.

7. Securing Application Development in Windows Server

You can improve the security of your application development infrastructure by reducing the size and scope of application and compute resources. One way to do this is to containerize workloads. Windows Server and Microsoft Hyper-V containers enable you to isolate workloads from each other and the OS. Even if a container is compromised by an attacker, it will be difficult for the attacker to access the host OS. Containers also provide a standardized environment for development, test and production teams.

7.1 Containers

Containers provide an isolated and portable operating environment for apps. From the app's perspective, a container appears to be a complete, isolated Windows OS with its own file system, devices and configuration. Therefore, in many respects, containers are like VMs because they run an OS, they support a file system, and you can access them across a network similar to any other physical machine or VM.

Containers are virtual environments that share the kernel of the host OS but provide user space isolation, so they provides an ideal environment in which an app can run without affecting the rest of the user mode components of the OS and without the other user mode components affecting the app. Using containers, developers can create and test apps quickly in an isolated environment while using only a few OS resources. This means that containers do not need all of the processes and services that an OS on a VM might use.

Windows Server 2016 supports two types of containers:

- **Windows Server containers.** These containers provide app isolation through the process and namespace isolation technology. Windows Server containers share the OS kernel with the container host and with all other containers that run on the host.
- **Hyper-V containers.** These containers expand on the isolation that Windows Server containers provide by running each container in a highly optimized VM.

Using containers has multiple benefits. The reduced OS size means that you must maintain fewer operating-system components, which in turn results in fewer potential security risks. The reduced OS size also helps improves scalability.

7.2 Docker

To run an application workload in a container, you must use Docker. Docker is a collection of open-source tools and cloud-based services that provide a common model for packaging (containerizing) app code into a standardized unit for software development. This standardized unit, or Docker container, is software that is wrapped in a complete file system that includes everything it needs to run, including code, runtime, system tools, system libraries, and anything else you can install on a server. You must download Docker separately; it is not part of the Windows Server 2016 installation media.

7.3 Nano Server

Microsoft Nano Server is a fairly new installation option for Windows Server 2016. It is a lightweight operating system tailored for use with virtualized container instances. There is no UI; you must manage Nano Server remotely using PowerShell, but this PowerShell differs from the standard one. As of Windows Server version 1803, Nano Server is available only as a container-based OS image, and you must run it as a container in a container host, such as Docker. You can troubleshoot these new Nano containers using Docker and run them in IoT Core.

A Nano Server instance cannot function as an Active Directory domain controller. In particular, it does not support the following features:

- Group Policy
- Network interface card teaming
- Virtual host bus adapters
- Proxy server access to the internet
- System Center Configuration Manager
- System Center Data Protection Manager

Nano Server supports the following roles:

- File Services
- Hyper-V
- IIS
- DNS Server

8. Securing Network Connections in Windows Server

One key component in securing your IT infrastructure is protecting against network-related security threats. Windows Server offers several network security features to help.

8.1 Windows Firewall with Advanced Security

Windows Firewall with Advanced Security blocks unauthorized network traffic flowing into or out of a local device by providing host-based, two-way network traffic filtering. You can either manually configure Windows Firewall with Advanced Security on each server or use Group Policy to centrally configure the firewall rules.

While the old Windows Firewall allowed you to configure only a single set of inbound and outbound rules (a profile), Windows Firewall with Advanced Security includes three profiles (Domain, Private and Public), so you can apply the appropriate rules to each server based on its connection to the network. These profiles are tightly connected to three network profiles in the Network and Sharing Center:

- **Domain networks.** Networks at a workplace that are attached to a domain.
- **Private networks.** Networks at home or at work where you trust the people and devices on the network. When private networks are selected, network discovery is turned on but file and printer sharing is turned off.
- **Guest or public networks.** Networks in public places. This location keeps the computer from being visible to other computers. When a public network is the selected network location, network discovery and file and printer sharing are turned off.

You can also configure the following options for each of the three network profiles:

- **Firewall State.** You can turn the firewall on or off independently for each profile.
- **Inbound Connections.** You can block connections that do not match any active firewall rules (this is the default), block all connections regardless of inbound rule specifications, or allow inbound connections that do not match an active firewall rule.
- **Outbound Connections.** You can allow connections that do not match any active firewall rules (this is the default) or block outbound connections that do not match an active firewall rule.
- **Protected Network Connections.** You can select the connections — for example, the Local Area Connection — that you want Windows Firewall to help protect.

- **Settings.** You can configure display notifications and unicast responses, and merge rules that are distributed through Group Policy.
- **Logging.** You can configure and enable logging.
- **IPsec Settings.** You can configure the default values for IPsec configuration.

8.2 IPsec

Connecting to the internet exposes a company to many types of security threats, from malware to drive-by downloads to social engineering attacks. IPsec is a set of industry-standard, cryptography-based protection services and protocols that can help to protect data in transit through a network by providing authentication, integrity checking and encryption. IPsec protects all protocols in the TCP/IP protocol suite except Address Resolution Protocol (ARP).

The design of IPsec helps it provide much better security than protection methods such as Transport Layer Security (TLS) and Secure Shell (SSH), which provide only partial protection. Network administrators who use IPsec do not have to configure security for individual programs because all network traffic between the specified hosts is protected when they use IPsec.

IPsec:

- Offers mutual authentication before and during communications.
- Forces both parties to identify themselves during the communication process.
- Enables confidentiality through IP traffic encryption and digital packet authentication.

8.3 Message Analyzer

You can use Message Analyzer to capture, display and analyze protocol messaging traffic, events and other system or application messages in network troubleshooting and other diagnostic scenarios. Message Analyzer enables you to save and reload captures, aggregate saved captures, and analyze data from current and saved trace files. When Message Analyzer performs network captures, it limits irrelevant data, and exposes issues and hidden information that is critical for quick analysis. It accomplishes this by enabling you to remove lower-level details so you can perform analysis on higher-layer data of interest.

You can use Message Analyzer in a variety of scenarios:

- Capturing network traffic for security review
- Troubleshooting application issues
- Troubleshooting network and firewall configuration issues

As you can see, Windows Server 2016 offers a lot of to help you protect your IT environment. You can use some or all of them. In particular, it's smart to take advantage of Group Managed Service Accounts, Windows Defender, LAPS, Privileged access workstations, ESAE forests, BitLocker, Shielded VMs, Windows Firewall and IPsec because they can improve IT security dramatically with relatively little effort. Using these Windows Server features can greatly enhance your security during network communications, and help you block man-in-the-middle (MITM), replay, hijacking, distributed denial-of-service (DDoS) and other attacks.

Useful References

The following resources will help you improve Active Directory management and security:

Manage

Blog post | [How to Add, Delete and Change Local Users and Groups with PowerShell](#)

Blog post | [Protecting Credentials in Windows Server 2016](#)

How-to | [How to List All User Accounts on a Windows System](#)

How-to | [How to Get Local Administrators](#)

How-to | [How to List Local Groups](#)

How-to | [How to Get Local Group Members Report](#)

How-to | [How to Find Shared Folders](#)

How-to | [How to Get Server Inventory across Your Network](#)

eBook | [Windows PowerShell Scripting Tutorial for Beginners](#)

Monitor

How-to | [How to Detect Who Installed What Software on Your Windows Server](#)

How-to | [How to Detect Who Created a Scheduled Task on Windows Server](#)

How-to | [How to Detect Who Deleted a DHCP Reservation](#)

How-to | [How to Monitor Deletions of DNS Records](#)

How-to | [How to Enable Video Recording of Changes in Your Windows Server](#)

eBook | [Gaining Control over Windows Server Configurations](#)

Blog post | [Top 10 Best Windows Server Monitoring Software Tools](#)

Secure

Quick Reference Guide | [Windows Server Auditing](#)

How-to | [How to Detect Modifications to Startup Items in Windows Registry](#)

Best Practices | [Windows Server Hardening Checklist](#)

SysAdmin magazine | [Hardening Windows Server Security](#)

Harden the Security of Your Windows-Based Server Infrastructure

with Netwrix Auditor

- Limit your attack surface by regularly reviewing server configurations for deviations from a known good baseline
- Detect critical security events before they result in a breach
- Investigate suspicious changes made to your server objects and settings

[Download Free 20-Day Trial](#)

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com.

Next Steps

Free trial – Set up Netwrix in your own test environment: netwrix.com/freetrial

In-Browser Demo – Take an interactive product demo in your browser: netwrix.com/browser_demo

Live Demo – Take a product tour with a Netwrix expert: netwrix.com/livedemo

Request Quote – Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:

300 Spectrum Center Drive
Suite 200 Irvine, CA 92618

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:



netwrix.com/social