

Forum:[Hack Forums](#)

Thread: [Steps in securing a Microsoft Windows Server](#)

Foxy Proxies Ltd - December 23, 2024, 9:06 am

Below is a high-level guide that covers essential steps in securing a Microsoft Windows Server environment. As with any security effort, these recommendations should be adjusted to suit your specific business requirements and compliance mandates.

1. Keep the Server Updated Patch Management

Enable Automatic Updates: Ensure Windows Update is set to automatically download and install updates, or schedule updates during low-traffic periods.

Cumulative Updates and Hotfixes: Regularly verify that both security and critical updates (including hotfixes) are installed.

WSUS (Windows Server Update Services): Consider deploying WSUS in your organization for centralized update management if you have multiple servers.

Tip: Stay subscribed to Microsoft's security bulletins and advisories to remain informed of critical vulnerabilities and patches.

2. Enforce Strong Authentication and Access Controls Strong Password Policies

Minimum Password Length: Set a minimum length of at least 12 characters.

Complexity Requirements: Enable password complexity to require a mix of uppercase, lowercase, numbers, and symbols.

Password Expiration: Some organizations still enforce password expiration, but modern guidance suggests focusing on long, complex passwords and multi-factor authentication (MFA).

Limit Admin Rights

Least Privilege Model: Only grant the permissions necessary for a user's role.

Use Separate Accounts: Have dedicated administrative accounts strictly for server administration tasks. Do not log in with admin rights for day-to-day activities.

Multi-Factor Authentication (MFA)

RDP Sessions: Wherever possible, require MFA for remote management, whether using Windows Hello for Business, RSA tokens, or other MFA solutions.

3. Secure Remote Desktop Protocol (RDP) Change Default Port (Optional)

Default Port 3389: Changing it to a non-default port helps reduce automated attacks, but it is not a security guarantee. If you do change the port, ensure you update firewall rules and document it.

Network Level Authentication (NLA)

Require NLA: Forces RDP clients to authenticate before establishing a session, reducing the risk

of resource consumption by unauthenticated requests.

Limit Access

Scope RDP Access: Only allow RDP from specific IP addresses or through a VPN. Configure Windows Firewall rules to permit inbound RDP connections exclusively from trusted networks.

Tip: Consider deploying Remote Desktop Gateway or using a VPN to encapsulate RDP traffic for additional protection.

4. Configure Windows Firewall and Advanced Security Inbound/Outbound Rules

Restrict Inbound Traffic: Only enable the ports and services necessary for your server's role (e.g., HTTP/HTTPS for a web server).

Restrict Outbound Traffic: Limit outbound connections to only trusted networks, services, or IP addresses to prevent malware from "phoning home."

Application Whitelisting

Windows Defender Application Control or AppLocker: Create rules that allow only specific, trusted executables to run. This reduces the risk of malicious software execution.

5. Deploy Anti-Malware and Endpoint Protection Windows Defender

Enable Real-Time Protection: Windows Defender (or Microsoft Defender for Endpoint in enterprise environments) provides good baseline protection.

Regular Scans: Schedule full system scans and ensure definitions are always up to date.

Third-Party Solutions

Endpoint Security Suites: Deploy advanced anti-malware, anti-ransomware, and intrusion prevention tools if you require more robust protection or specific compliance measures.

6. Minimize the Attack Surface Remove Unused Roles and Features

Server Roles: Install only the roles and features your server needs. Extra roles expand the potential attack surface.

Services: Disable or set to 'Manual' any services not required by your server's primary function.

Use Core Editions Where Possible

Windows Server Core: This minimal installation option has a smaller footprint, reducing exposure to vulnerabilities and simplifying patch management.

7. Audit, Logging, and Monitoring Event Viewer

Enable Advanced Logging: Use Group Policy or local security policies to enable detailed auditing (e.g., account logon events, object access events).

Regularly Review Logs: Create a process or schedule to examine the Windows Event Viewer for unusual or suspicious activity.

Centralized Log Collection

Windows Event Forwarding (WEF): Forward logs to a central server for easier correlation and analysis.

SIEM Integration: Integrate with Security Information and Event Management (SIEM) solutions (e.g., Splunk, Microsoft Sentinel) to detect patterns across multiple hosts.

8. Enable BitLocker or Disk Encryption (When Applicable)

BitLocker Drive Encryption

Encrypt Data-At-Rest: For servers that host sensitive data, enable BitLocker on your volumes to protect data from physical theft or unauthorized access.

Hardware Requirements: Use Trusted Platform Module (TPM) to store encryption keys securely.

Tip: Always maintain secure backups of your BitLocker recovery keys and store them in a safe location or in Azure Active Directory (if domain-joined).

9. Implement Group Policy Hardening

Security Baselines

Microsoft Security Compliance Toolkit: Provides recommended Group Policy settings for Windows Servers. These baselines cover account policies, audit policies, and more.

Local Security Policy: For standalone servers (non-domain-joined), configure Local Security Policy to align with industry best practices, such as CIS Benchmarks or Microsoft's security guides.

10. Backup and Disaster Recovery

Regular Backups

System State Backups: Capture the registry, Active Directory database (on domain controllers), and other system state data.

Offsite or Cloud Storage: Store backups offsite or use cloud backup solutions for redundancy.

Test Your Restores

Recovery Drills: Periodically test the restore process to ensure backup integrity and quick disaster recovery.

11. Intrusion Detection and Prevention

Network IDS/IPS

Hardware or Software Solutions: Consider third-party solutions (e.g., Snort, Suricata) or advanced firewall appliances that analyze inbound and outbound traffic for threats.

Host-Based Intrusion Detection

Windows Defender Exploit Guard: Offers exploit mitigation, attack surface reduction (ASR) rules, and network protection to identify or block malicious behavior.

Sysmon: Microsoft Sysinternal's Sysmon tool extends logging capabilities, giving you detailed process creation logs with command line data.

12. Stay Informed and Continuously Improve

Ongoing Security Process

Vulnerability Scanning: Regularly run scans with tools like Microsoft Defender for Endpoint Vulnerability Management, Nessus, or OpenVAS to identify missing patches or misconfigurations.

Penetration Testing: Periodic internal or external penetration tests can help you find gaps in your defenses.

Security Updates and News

Microsoft Security Update Guide: Keep track of critical updates and zero-day vulnerabilities.

Threat Intelligence: Subscribe to relevant security bulletins or threat intelligence feeds to stay up-to-date on emerging threats.