RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

WINDOWS SERVER: START-UP SECURITY FOR A DOMAIN CONTROLLER

In 17 key best practices, ANSSI – the French Cybersecurity Agency – endeavours to help organisations achieve the secure implementation of a Windows Server 2016 (and later versions) intended to operate as an active directory domain controller.

1/ PREREQUISITES FOR INSTALLATION

→ **Enable physical or virtual TPMv2 and UEFI Secure Boot mode** by activating Kernel DMA Protection within the BIOS settings**.** From Windows Server 2022 onwards, configure physical or virtual servers (Hyper-V or hypervisors supporting it), favouring Secured-core hardware when compatible.

→ **Check physical access to the server**. Simultaneously, control console access to the server via IPMI for a physical server, or from the hypervisor console.

→ **Choose a hypervisor supporting VM-GenerationId for virtual machines** to ensure compliance with the architecture of virtualised domain controllers.

→ **Use a basic Windows Server media (ISO, USB key)** or, alternatively, a dedicated mastering environment administered solely by Tier 0 administrators (if available).

2/ SYSTEM INSTALLATION

→ **Favour installation in server core mode**, as this contains fewer components and therefore reduces the attack surface.

→ **Do not disable native security features that are specifically suited to the system.** On the integrated Windows Defender firewall, enable incoming firewall rules when using remote MMC consoles (events, firewall, scheduled tasks, etc.) without interactive connection. Restrict these rules to traffic originating from AD-DS administration stations only.

→ **Do not enable remote desktop administration**, as administration is performed from dedicated stations via MMC, WinRM, and WSAD (ADAC, PSAD, etc.).

→ **Do not disable IPv6.** It is being used for communications with the server itself and must therefore remain active. Alternatively, you might favor IPv4 protocol for all communications.

→ **Update the server before connecting to the production IS network**. Installation files must be downloaded from Microsoft Update. This also applies to quality updates and to drivers operating on physical servers.

→ **Make sure clock synchronisation is provided by other domain controllers.** If this is the first controller in the forest, configure external stratum 2 time sources to ensure proper Kerberos functioning.

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

3/ POST-INSTALLATION SYSTEM CONFIGURATION

→ **Store AD-DS services data** (e.g. databases, logs, SYSVOL files) **outside of the system disk,** even if the configuration wizard suggests it by default. **Turn data disk write caching off.**

→ **Avoid co-locating roles or role services which could compromise security** (e.g. IIS and AD-CS) **on the domain controller.** Only the DNS server role is required.

→ **Encrypt system and data hard drives with BitLocker** to prevent theft.

→ **Enable VBS (Virtualisation-based Security)** and the security components which depend on it (notably the virtualisation-based protection of code integrity), within enabling Credential Guard on the domain controller. For more information on this topic, see Credential Guard protection limits.

→ **Harden the server environment.** Use security baselines with tools from the Security Compliance Toolkit (SCT) or, for Windows Server 2025, with the Windows PowerShell OSConfig module.

→ **Apply the principle of least privilege using** Just Enough Admin (RBAC System) when administering certain DNS server security features remotely via Windows PowerShell which cannot be performed using the MMC administration console.

→ **Avoid installing third-party services or agents** (antivirus, EDR, backup, etc.) on domain controllers.

4/ END OF INSTALLATION

With these best practices in place, the domain controller displays a reduced attack surface.

Note that additional security measures will later need to be implemented for AD-DS services and for the DNS server.