RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

WINDOWS SERVER: START-UP SECURITY FOR A MEMBER SERVER

In 18 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 member server.

1/ PREREQUISITES FOR INSTALLATION

→ **Enable physical or virtual TPMv2 and UEFI Secure Boot mode.** 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.

2/ SYSTEM INSTALLATION

→ **Favor installation in server core mode**, as this contains fewer components and therefore reduces the attack surface. From Windows Server 2019 onwards, a minimal graphical interface (browsers, explorer, consoles and graphical administration tools) can be enabled on the server core without a desktop nor multimedia elements. Certain roles or features might be unavailable in server core mode. In such cases, Windows Server must be installed in Desktop Experience mode.

→ **Do not disable native security features that are specifically suited to the system.** Examples include UAC (except in a few legitimate cases), and the integrated Windows Defender firewall.

→ **Enable only the firewall rules necessary for production on the Windows Defender firewall** and, if applicable, remote administration via MMC console. If RDP is still to be used, do not disable network-level authentication (NLA).

→ **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.

→ **Join the server to the AD-DS domain.** First, create a computer account in the destination organisational unit (OU), ensuring that the owner of the object is the default built-in Administrators group. Good practice dictates using the djoin command line.

→ **Make sure clock synchronisation is provided by domain controllers,** to ensure proper Kerberos functioning.

→ **Define a strong password for local accounts belonging to the local administrators group,** ensuring they are distinct from passwords used on other servers. It is strongly recommended to use LAPS.

V1.0 (10/25)

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

→ **Avoid co-locating roles, role services, or applications which could compromise security** (e.g. IIS and AD-CS certificate authority (CA)) **on the same server.** Roles might be installed on the same server within a test environment. However, they may be subject to different security requirements in production (e.g. secure access to a CA, availability for the CRL and AIA extensions).

3/ POST-INSTALLATION SYSTEM CONFIGURATION

→ **Store service and application data outside of the system disk,** even if the configuration wizard suggests it by default (e.g. AD-CS databases, WID and SQL databases, etc.).

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

→ **Enable VBS (Virtualisation-based Security)** and the security components which depend on it (e.g. Credential Guard). Please note that some components are incompatible with certain roles or applications.

→ **Replace self-signed certificates** for RDP and IIS remote administration (when installed) with certificates issued by a trusted PKI using a recent cryptographic provider (e.g. with AD-CS**:** Key Storage Provider).

→ **Apply the principle of least privilege** to service and application accounts, along with administration accounts.

→ **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.

→ **Configure IPSec to secure communications between critical servers.**

4/ END OF INSTALLATION

With these best practices in place, the member server is ready to handle the required roles, services, and applications, with a reduced attack surface.

Note that, depending on the features and applications installed, additional security measures may later need to be implemented.