RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

WINDOWS SERVER: START-UP SECURITY FOR A STANDALONE SERVER

In 16 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 a standalone server not joined to an Active Directory domain.

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

→ **Make sure clock synchronisation draws on trusted NTP time sources** for proper logging.

→ **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 and, when applicable, remote administration.** If Windows PowerShell is used, set the firewall profile to 'private'.

→ **Do not disable network-level authentication (NLA) for RDP,** if used.

→ **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.

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

→ **Avoid co-locating roles, role services, or applications which could compromise security** (e.g. IIS and AD-CS) **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.

V1.0 (10/25)

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

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, 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.

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

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

→ **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 Windows Event Forwarding for auditing and traceability purposes** whenever a Windows Event Centre (WEC) server is present in the information system. **Implement certificate-based mutual authentication.**

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

4/ END OF INSTALLATION

With these best practices in place, the standalone 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.