RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

WINDOWS SERVER : SÉCURISATION INITIALE D'UN SERVEUR AUTONOME

Retrouvez, en une vingtaine de bonnes pratiques, les ressources essentielles de l'ANSSI permettant la mise en œuvre sécurisée d'un serveur *Windows Server 2016* (et versions ultérieures) destiné à devenir un serveur autonome non joint à un domaine Active Directory.

1/ ÉTAPES PRÉALABLES À L'INSTALLATION

→ **Activer un TPMv2 matériel ou virtuel, et le mode de démarrage UEFI *Secure Boot*.** A compter de *Windows Server 2022*, configurer les serveurs physiques ou virtuels (Hyper-V ou hyperviseurs le supportant) en privilégiant ***Secured-core*** lorsque le matériel est compatible.

→ **Vérifier l'accès physique au serveur.** Contrôler parallèlement les accès console au serveur (IPMI pour un serveur physique, ou console de l'hyperviseur).

2/ INSTALLATION DU SYSTÈME

→ **Vérifier la synchronisation horaire** depuis des sources de temps NTP fiables pour le bon fonctionnement de la journalisation.

→ **Ne pas désactiver les fonctionnalités de sécurité, natives et adaptées au système,** comme par exemple l'UAC (excepté pour quelques cas de désactivation légitimes) ou encore le pare-feu *Windows Defender* intégré.

→ **Activer uniquement les règles de pare-feu nécessaires** à la production et, le cas échéant, à l'administration distante. Si *Remote PowerShell* est utilisé, positionner le profil du pare-feu à « privé ».

→ **Ne pas désactiver la NLA** (authentification au niveau réseau) **du RDP**, s'il est utilisé.

→ **Ne pas désactiver IPv6**, notamment utilisé pour les communications vers le serveur lui-même et devant ainsi rester actif. En revanche, il est possible de privilégier le protocole IPv4 pour toutes les communications.

→ **Mettre à jour le serveur avant de le connecter au réseau du SI de production.** Les fichiers d'installation doivent provenir de *Microsoft Update*. Cela concerne également les mises à jour de qualité et les pilotes sur un serveur physique.

→ **Définir un mot de passe fort pour les comptes membres du groupe des administrateurs locaux** afin qu'ils soient différents de ceux des autres serveurs.

→ **Ne pas colocaliser sur un même serveur des rôles, services de rôle ou applications pouvant altérer le niveau de sécurité** (ex. : IIS et AD-CS). Des rôles pourraient être installés sur le même serveur en environnement de test. En revanche, ils peuvent être soumis à des besoins de sécurité différents en production.

V1.0 (10/25)

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

LES ESSENTIELS

3/ CONFIGURATION POST-INSTALLATION DU SYSTÈME

→ **Stocker les données des services et applications hors du disque système**, même si l'assistant de configuration le propose par défaut (ex. : bases AD-CS, bases SQL, etc.).

→ **Chiffrer les disques durs système et de données** avec la fonctionnalité *BitLocker* pour de se prémunir des risques de vol.

→ **Activer la VBS (*Virtualisation Based Security*)** et les composants de sécurité qui en dépendent (ex. : *Credential Guard*). Attention : il existe des composants incompatibles avec certains rôles ou applications.

→ **Appliquer le principe du moindre privilège** pour les comptes des service et des applications, ainsi que pour l'administration.

→ **Remplacer les certificats autosignés** pour RDP, WinRM sur https et l'administration distante d'IIS, par des certificats issus d'une IGC avec un fournisseur cryptographique récent (ex. : avec AD-CS, *Key Storage Provider*).

→ **Durcir l'environnement du serveur.** Utiliser les outils du kit de ressources de conformité de la sécurité (SCT) ou, pour *Windows Server 2025*, le module *Windows PowerShell OSConfig*.

→ **Configurer *Windows Event Forwarding*** dans une démarche d'audit et de traçabilité s'il existe un serveur de centralisation des journaux *Windows* (WEC) dans le SI**. Une authentification mutuelle basée sur des certificats doit être mise en œuvre.**

→ **Configurer IPSec pour sécuriser les communications entre serveurs autonomes critiques.**

4/ FIN DE L'INSTALLATION

Une fois ces bonnes pratiques implémentées, le serveur autonome est prêt à recevoir les rôles, services et applications nécessaires, tout en exposant une surface d'attaque réduite.

Noter que d'autres étapes de sécurisation seront nécessaires en fonction des fonctionnalités ou applications installées ultérieurement.

5/ LIENS VERS D'AUTRES RESSOURCES ANSSI

Pour aller plus, consulter les guides de l'ANSSI sur le sujet :

> Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation ;

> Restreindre la collecte de données sous Windows 10.