RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

WINDOWS SERVER : SÉCURISATION INITIALE D'UN SERVEUR MEMBRE

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 membre d'un domaine Active Directory (AD-DS).

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

→ **Privilégier l'installation en mode *server core*,** qui contient moins de composants et offre donc une surface d'attaque plus réduite. Depuis *Windows Server 2019*, il est possible, sur le *server core*, d'activer une interface graphique minimale (navigateurs, explorateur, consoles et outils d'administration graphiques) sans bureau, ni éléments multimédia. Certains rôles ou fonctionnalités peuvent être indisponibles avec le mode *server core*. Dans ce cas, l'installation de *Windows Server* doit se faire en mode *Desktop Experience*.

→ **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 pour la production sur le pare-feu *Windows Defender*** et, le cas échéant, l'administration distante via console MMC. S'il est prévu, malgré tout, d'utiliser RDP, ne pas désactiver l'authentification au niveau réseau (NLA).

→ **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.

→ **Joindre le serveur au domaine AD-DS.** Créer préalablement un compte ordinateur dans l'OU de destination en s'assurant que le propriétaire de l'objet est le groupe Administrateurs intégré par défaut. L'utilisation de l'utilitaire djoin est une bonne pratique.

→ **Vérifier que la synchronisation horaire est fournie par les contrôleurs de domaine** pour le bon fonctionnement de Kerberos.

→ **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. Il est fortement recommandé d'utiliser LAPS.

V1.0 (10/25)

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

→ **Ne pas colocaliser sur un même serveur des rôles, services de rôle ou applications pouvant altérer le niveau de sécurité** (ex. : IIS et autorité de certification AD-CS). Des rôles pourraient être installés sur le même serveur en environnement de test. En revanche, ils sont soumis à des besoins de sécurité différents en production (ex. : accès sécurisés sur une autorité de certification et disponibilité pour le site web de publication de CRL et AIA).

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 WID et SQL, etc.).

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

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

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

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

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

4/ FIN DE L'INSTALLATION

Une fois ces bonnes pratiques mises en œuvre, le serveur membre est prêt à recevoir les rôles, services et applications demandés, tout en exposant une surface d'attaque réduite.

Noter que d'autres étapes de sécurisation seront nécessaires en fonction des fonctionnalités 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 ;

> Recommandations pour l'administration sécurisée des SI reposant sur Active Directory (octobre 2023) ;

> Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory.