RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

WINDOWS SERVER : SÉCURISATION INITIALE D'UN CONTRÔLEUR DE DOMAINE

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 contrôleur de domaine.

1/ ÉTAPES PRÉALABLES À L'INSTALLATION

→ **Activer un TPMv2 matériel ou virtuel, et le mode de démarrage UEFI *Secure Boot*** en activant l'option *Kernel DMA Protection* dans l'interface BIOS**.** 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).

→ **Utiliser un hyperviseur supportant la technologie *VM-GenerationId* pour les ordinateurs virtuels** afin de garantir le respect de l'architecture des contrôleurs de domaine virtualisés.

→ **Utiliser une image *Windows Server* de base (ISO, clé USB)** ou, à défaut, un environnement de masterisation dédié, administré uniquement par les administrateurs *Tier 0* (si existant)**.**

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.

→ **Ne pas désactiver les fonctionnalités de sécurité, natives et adaptées au système**. Sur le pare-feu *Windows Defender* intégré, activer les règles de pare-feu entrantes pour l'usage de consoles MMC distantes (évènements, pare-feu, tâches planifiées, etc.) sans connexion interactive. Restreindre ces règles aux flux provenant des stations d'administration AD-DS uniquement.

→ **Ne pas activer l'administration par bureau distant,** l'administration se faisant depuis les stations dédiées à cet usage via MMC, WinRM et WSAD (ADAC, PSAD, etc.).

→ **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.

→ **Vérifier que la synchronisation horaire est fournie par les autres contrôleurs de domaine.** S'il s'agit du premier contrôleur de la forêt, configurer des **sources de temps externes de strate 2,** pour le bon fonctionnement de Kerberos.

V1.0 (10/25)

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

LES ESSENTIELS

3/ CONFIGURATION POST-INSTALLATION DU RÔLE

→ **Stocker les données des services AD-DS** (bases de données, journaux et dossiers SYSVOL) **sur des disques de données** hors du disque système, même si l'assistant de configuration le propose par défaut. **Désactiver le cache en écriture** sur ces disques de données.

→ **Ne pas colocaliser sur le contrôleur de domaine des rôles ou services de rôle pouvant altérer le niveau de sécurité.** Seul le rôle serveur DNS est nécessaire.

→ **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*)** ainsi que les composants de sécurité - notamment la protection de l'intégrité de la mémoire matérielle (HVCI) - qui en dépendent, sans activer *Credential Guard* sur un contrôleur de domaine (voir à ce sujet les limites de *Credential Guard*).

→ **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*.

→ **Activer le principe du moindre privilège** à l'aide *de Just Enough Admin* (RBAC *System*) pour l'administration via *Windows PowerShell* distant de certaines fonctionnalités de sécurisation du serveur DNS qui ne s'effectuent pas par la console d'administration MMC.

→ **Ne pas installer des services ou agents tiers** (antivirus, EDR, sauvegarde, etc.) **sur des contrôleurs de domaine.**

4/ FIN DE L'INSTALLATION

Une fois ces bonnes pratiques mises en œuvre, vous disposez d'un contrôleur de domaine exposant une surface d'attaque réduite.

Noter néanmoins que d'autres étapes de sécurisation seront nécessaires pour les services AD-DS, mais aussi pour le serveur DNS.

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 ;

> Investigation numérique sur l'annuaire Active Directory avec les métadonnées de réplication - Outil ADTimeline.