Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Guide visant à sécuriser les services Active Directory de Microsoft dans votre organisation

Praticien·nes

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

TLP:CLEAR

Canada

Avant-propos

Le Guide visant à sécuriser les services Active Directory de Microsoft dans votre organisation (ITSP.60.100) est un publication NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

Centre de coordination des services

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 12 décembre 2023.

Historique des révisions

Révision	Modifications	Date
1	Première version.	12 décembre 2023

D97-3/60-100-2023F-PDF
978-0-660-68471-0

Vue d'ensemble

Les services d'annuaire sont des composants fondamentaux essentiels pour les environnements d'architecture de technologies de l'information (TI) d'entreprise. Ils servent principalement à stocker et à gérer les justificatifs d'identité et les membres des groupes (rôles) connexes. Les services d'annuaire peuvent être mis en œuvre de plusieurs façons. Les services Active Directory (AD) de Microsoft comprennent un référentiel de données structuré que les organisations utilisent fréquemment pour stocker et gérer des objets de données d'annuaire d'entreprise, notamment des stratégies, des utilisatrices et utilisateurs, des dispositifs, des justificatifs d'identité ainsi que d'autres ressources réseau. Les services AD sont une cible clé pour les auteures et auteurs de menace qui cherchent à s'introduire dans le réseau d'une organisation dans le but d'accéder à ses systèmes et à ses données, puisqu'on les considère comme étant un type de compromission susceptible de fournir les « clés du royaume ».

La présente publication fait mention des facteurs à considérer pour sécuriser les services AD de Microsoft dans votre organisation, plus particulièrement en ce qui a trait aux déploiements sur site. Ce guide fournit des recommandations sur le renforcement de la sécurité des déploiements sur site de Microsoft AD pour la gestion des environnements avec un niveau moyen de confidentialité, d'intégrité et de disponibilité, tel qu'il est décrit à l'annexe 2 de *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) [1]. Le modèle de menace prend en compte les scénarios de menace les plus courants et actifs, dont ceux dans lesquels des adversaires possèdent des ressources minimales, mais sont disposées et disposés à prendre des risques importants, comme les pirates informatiques dotées et dotés de moyens peu sophistiqués ou les cybercriminelles et cybercriminels solitaires. Il ne vise pas à atténuer des menaces plus sophistiquées, comme les attaques du jour zéro ou les menaces internes spécialisées. Si une organisation est confrontée à un contexte de menace plus poussé, elle peut s'adresser au Centre canadien pour la cybersécurité (Centre pour la cybersécurité) pour obtenir de l'orientation additionnelle. Des ressources supplémentaires pour la configuration de services AD sont également dérivées des pratiques exemplaires de Microsoft, du Guide de mise en œuvre technique de sécurité (STIG pour *Security Technical Implementation Guide*) de la Defense Information Systems Agency (DISA) et des rapports sur les objectifs repères du Centre for Internet Security (CIS).

Les recommandations formulées dans la présente ont été élaborées en collaboration avec Microsoft et sont inspirées des pratiques exemplaires générales pour sécuriser les environnements AD. Nos recommandations s'appliquent aux environnements AD de Microsoft exécutant Microsoft Windows Server 2019 ou une version plus récente, et elles s'appliquent à tous les environnements AD Domain Services de Microsoft pour ce qui est des déploiements sur site.

Les serveurs exécutant un système d'exploitation qui répondent à cette exigence peuvent être utilisés comme contrôleurs de domaine principaux. Certaines de ces recommandations peuvent s'appliquer à d'autres services connexes souvent employés dans un environnement d'entreprise, comme le service de noms de domaine (DNS pour *Domain Name Service*), le protocole DHCP (Dynamic Host Configuration Protocol) et les services de fichiers et d'impression.

Table des matières

1 Introduction

Les services d'annuaire sont des composants fondamentaux essentiels pour les environnements d'architecture de technologies de l'information (TI) d'entreprise. Ils servent à stocker et à gérer les justificatifs d'identité et leurs autorisations d'accès. Les violations de réseaux et de données continuent de s'accroître alors que les auteures et auteurs de menace sophistiqués tirent de plus en plus avantage des lacunes de sécurité que l'on trouve dans les technologies gérées et non gérées. Les services d'annuaire stockent les objets critiques, comme les justificatifs administratifs de nature sensible qui peuvent servir à accorder l'accès à tout l'environnement de l'entreprise. Ils sont donc des cibles de grande valeur pour les auteures et auteurs de menace qui tentent d'exploiter les vulnérabilités associées à l'infrastructure sur laquelle ces services sont déployés. En raison de la portée potentielle associée à leur compromission, il est capital que les organisations prennent les mesures nécessaires pour sécuriser leurs services d'annuaire d'entreprise.

Le service Active Directory (AD) de Microsoft est un référentiel de données structuré que les organisations utilisent fréquemment pour stocker et gérer des objets de données d'annuaire d'entreprise. L'unité de sécurité de base des services AD est la « forêt », qui peut être divisée en sous-unités que l'on appelle « domaines ». Si votre organisation devait être aux prises avec la compromission d'une quelconque partie de sa forêt, cette situation pourrait entraîner la compromission de la forêt dans son ensemble (tous les domaines pourraient être traversés). L'historique continu des compromissions de services AD démontre la nécessité de renforcer sa sécurité, ce qui entraînerait des coûts d'exploitation potentiellement plus élevés et davantage d'efforts pour prévenir des violations plus importantes et onéreuses. Il est essentiel de protéger et de renforcer le service AD de Microsoft pour assurer la protection du réseau d'entreprise, peu importe où il a été déployé.

La présente publication recommande des pratiques exemplaires à adopter pour sécuriser les services AD de Microsoft lors d'un déploiement sur site et autogéré pour la gestion des environnements avec un niveau moyen de confidentialité, d'intégrité et de disponibilité (réduisant le risque résiduel advenant un préjudice potentiel de niveau moyen). L'orientation et les conseils formulés visent à contrer les scénarios les plus souvent adoptés par les auteures et auteurs de menace dans le cadre desquels on s'attend à ce que les menaces émanent d'adversaires qui ont des ressources moyennes et qui sont disposées et disposés à prendre des risques moyens, comme des criminelles et criminels récidivistes, des pirates ordinaires ou des initiées et initiés malveillants. Si une organisation est confrontée à un contexte de menace plus poussé que celui indiqué, elle peut s'adresser au Centre pour la cybersécurité pour obtenir de l'orientation additionnelle.

Étant donné que la présente publication n'est pas un guide de déploiement et de configuration complet, des ressources supplémentaires pour la configuration de services AD sont également offertes auprès de Microsoft, dans le Guide de mise en œuvre technique de sécurité (STIG pour *Security Technical Implementation Guide*) de la Defense Information Systems Agency (DISA) et dans les rapports sur les objectifs repères du Centre for Internet Security (CIS). Le guide visant à sécuriser les services d'annuaire dans des environnements en nuage, axé sur Azure AD, sera publié à une date ultérieure.

Elles s'appliquent aux environnements AD de Microsoft exécutant Microsoft Windows Server 2019 ou une version plus récente. Les organisations exécutant des versions de Microsoft AD antérieures à Windows Server 2019 devraient envisager de passer à des forêts « séparées » à sécurité renforcée jusqu'à ce qu'elles puissent mettre à niveau leur environnement ou migrer leurs services et leur information. Il n'est pas recommandé d'utiliser des environnements séparés de cette nature pendant de longues périodes au cours du cycle de développement des logiciels (CDS).

Dans les environnements Windows AD, la configuration de niveau fonctionnel détermine les caractéristiques et les fonctionnalités de sécurité accessibles à partir d'un domaine ou d'une forêt. Les exigences de niveau fonctionnel déterminent également quelles versions du système d'exploitation Windows Server peuvent être installées sur les contrôleurs de domaine au sein d'un domaine ou d'une forêt. Pour mettre en œuvre les recommandations formulées dans la présente, votre organisation devrait s'assurer que les niveaux fonctionnels de sa forêt et de son domaine sont définis aux niveaux fonctionnels de Windows Server 2016 ou d'une version plus récente. Pour de plus amples renseignements sur les niveaux fonctionnels, prière de consulter le document de référence de Microsoft intitulé *Niveaux fonctionnels de domaine et de forêt* [2].

La fréquence et la sophistication des attaques contre AD sont en hausse et la sécurité traditionnelle pour les services AD n'est plus adéquate. Afin d'améliorer la protection des services d'annuaire, votre organisation devra investir des ressources additionnelles et davantage d'efforts. Une mesure que votre organisation peut prendre est d'assurer la séparation des tâches au moyen de procédures et de stratégies. Plusieurs fonctions de sécurité, comme celles des administratrices et administrateurs des sauvegardes, des audits ou des alertes, devraient particulièrement être distinctes des fonctions d'administration des domaines. De plus, les organisations devraient tenir compte du fait que les administratrices et administrateurs de domaines (et d'autres rôles équivalents) peuvent s'accorder des autorisations à leur discrétion, puisque la capacité de restreindre techniquement une telle activité est limitée dans AD.

Votre organisation devrait également assurer la maintenance de son environnement AD en appliquant les plus récents correctifs disponibles pour atteindre le niveau de correction offert par Windows Server 2019 ou une version plus récente. En mettant à jour et en corrigeant ses environnements de TI, votre organisation peut s'assurer que les vulnérabilités et les bogues ont été corrigés et ainsi empêcher les auteures et auteurs de menace de les exploiter. Votre organisation peut également choisir d'isoler les services dont la maintenance est déficiente pour les éloigner des menaces provenant d'Internet.

1.1 Considérations stratégiques

Votre organisation doit se doter de ressources informatiques d'entreprise pour soutenir son personnel et remplir sa mission. Elle devrait tenir compte du contexte opérationnel et de l'environnement de menace qui lui sont propres au moment d'appliquer les recommandations formulées dans cette publication pour protéger son infrastructure AD. Les piliers suivants ont pour but de soutenir l'environnement opérationnel d'entreprise et d'étayer le contexte de menace pour les services d'annuaire :

- Architecture de TI d'entreprise;
- Gestion de l'identité des justificatifs d'identité et de l'accès (GIJIA);
- Évaluations des menaces et des risques (EMR).

1.1.1 Architecture de TI d'entreprise

L'architecture de TI d'entreprise définit la manière dont la structure et le fonctionnement des biens de TI de votre organisation sont censés soutenir vos objectifs opérationnels stratégiques, en tenant compte de la sécurité et des risques. L'architecture de TI d'entreprise fournit une orientation stratégique qui permet de savoir comment les investissements dans

les ressources d'information peuvent intégrer et favoriser les processus opérationnels. Votre organisation devrait comparer cette publication avec son architecture de TI d'entreprise afin de mieux comprendre comment ces changements pourraient avoir une incidence sur ses objectifs opérationnels.

1.1.2 Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)

La GIJIA fait référence aux processus d'authentification et d'autorisation nécessaires pour que les utilisatrices, les utilisateurs et les dispositifs interagissent avec l'infrastructure informatique de votre organisation et s'y connectent. Elle comprend un ensemble d'outils de sécurité, de stratégies et de systèmes qui aide votre organisation à gérer, à surveiller et à sécuriser l'accès à ses ressources technologiques. Les recommandations formulées dans cette publication auront une incidence sur les contrôles de GIJIA dans votre organisation. Vous devriez comparer ce document à l'infrastructure de GIJIA de votre organisation afin de mieux comprendre l'incidence que ces recommandations pourraient avoir sur ses activités de GIJIA.

1.1.3 Évaluation des menaces et des risques

L'évaluation des menaces et des risques comprend la détection des menaces, l'évaluation des risques découlant de ces menaces et l'atténuation des risques qui sont inacceptables pour les processus opérationnels et l'information essentielle de l'organisation. Les recommandations formulées dans le présent document devraient être prises en compte dans l'évaluation des risques et le cadre de gestion de votre organisation afin de déterminer la nature et la portée de tout changement apporté à sa posture de risque. Si elle collabore avec un fournisseur de services, comme Services partagés Canada (SPC), pour gérer la mise en œuvre des contrôles, votre organisation demeure responsable de la gestion des risques. Ces conseils concernent un modèle de menace selon lequel des adversaires possèdent des ressources minimales, mais sont disposées et disposés à prendre des risques importants, comme les pirates informatiques dotées et dotés de moyens peu sophistiqués ou les cybercriminelles et cybercriminels solitaires. Il ne vise pas à atténuer des menaces plus sophistiquées, comme les attaques du jour zéro ou les menaces internes spécialisées. Si une organisation est confrontée à un contexte de menace plus poussé, elle peut s'adresser au Centre canadien pour la cybersécurité (Centre pour la cybersécurité) pour obtenir de l'orientation additionnelle.

1.2 Contexte de menace des services d'annuaire

L'annexe A présente un ensemble des contrôles de sécurité de base recommandés qu'il est possible d'appliquer au fonctionnement des services d'annuaire au sein d'une organisation. Les contrôles de sécurité mentionnés à l'annexe A ont été sélectionnés en se basant sur les hypothèses et les contraintes suivantes :

- On suppose que l'incidence ou le préjudice maximal possible associé à la compromission des processus opérationnels et de l'information devant être pris en charge par les services d'annuaire est de catégorie Confidentialité moyenne, Intégrité moyenne et Disponibilité moyenne. La catégorisation du contexte opérationnel est décrite à l'annexe 1 de l'ITSG-33 [1];
- On suppose que le contexte de menace des processus opérationnels et de l'information devant être pris en charge par les services d'annuaire tient compte des scénarios d'auteures et auteurs de menace les plus probables. Si une

organisation est confrontée à un contexte de menace plus poussé que celui indiqué précédemment, elle peut s'adresser au Centre canadien pour la cybersécurité pour obtenir de l'orientation additionnelle;

- On suppose que tous les contrôles applicables tirés du profil de contrôle de base sélectionné par votre organisation (par exemple, une version adaptée de l'annexe 4A de l'ITSG-33) ont déjà été mis en œuvre et évalués. Il est fortement recommandé de valider cette hypothèse et d'atténuer tout risque en suspens avant de mettre en pratique les conseils formulés dans le présent document. La compromission des services d'annuaire se traduira par la compromission de tous les systèmes qu'ils prennent en charge. Par conséquent, les fondements de la sécurité des services d'annuaire devraient à tout le moins être aussi rigoureux que ce qui les entoure;
- La sélection des contrôles et, dans certains cas, des mécanismes et des pratiques en matière d'assurance a été adaptée en fonction des conseils formulés par les fournisseurs et l'industrie. Des adaptations additionnelles sont toutefois recommandées pour tenir compte des capacités grandissantes et avancées des auteures et auteurs de menace;
- Certaines capacités associées aux auteures et auteurs de menace (comme les personnes à l'interne avec accès privilégiés ou le développement et l'utilisation de vulnérabilités du jour zéro) ne permettent pas d'atténuer les menaces par l'intermédiaire des configurations des composantes associées aux services d'annuaire. Il convient donc de les aborder au niveau organisationnel. La double autorisation, la séparation physique et la séparation des tâches sont des exemples de tels contrôles.

2 Ressources d'orientation sur la sécurisation d'AD

Les ressources ci-dessous ont été consultées dans le cadre de la préparation de la présente publication. Prière de consulter ces ressources additionnelles pour des pratiques exemplaires et de l'orientation sur la sécurité d'AD.

2.1 Pratiques exemplaires en matière de cybersécurité de Microsoft

Microsoft a publié un ensemble de lignes directrices sur la sécurisation d'AD en se basant sur les observations et les leçons tirées dans le cadre du soutien offert à ses clients pour ce qui est d'intervenir advenant la compromission de l'infrastructure d'AD et d'en assurer la reprise. Ces lignes directrices font mention des expositions courantes au sein des installations AD, des contrôles techniques nécessaires pour réduire la surface d'attaque des environnements AD et des recommandations en matière de surveillance continue formulées pour détecter les signes d'une possible compromission. Cette ressource souligne l'importance de concevoir l'architecture AD selon une approche basée sur les risques et la nécessité d'assurer la séparation des biens indispensables et la gestion sécurisée des systèmes, des applications, des utilisatrices et des utilisateurs tout au long du cycle de vie. Consultez le document intitulé *Meilleures pratiques pour la sécurisation d'Active Directory* [3] pour obtenir de plus amples renseignements.

2.2 Defense Information Systems Agency (DISA) : Security Technical Implementation Guide (STIG)

La DISA est une agence de soutien au combat du Department of Defense (DoD) des États-Unis composée de personnel militaire, de civils et d'entrepreneurs. Dans le cadre de son mandat, la DISA produit régulièrement une liste de publications désignées sous le nom de STIG. Le contenu et le thème de ces publications varient selon le domaine ou l'application de la technologie. Ce document de la DISA, *Active Directory Domain Security Technical Implementation Guide (STIG)* (en anglais seulement) [4] a été consulté aux fins de la présente publication.

En ce qui concerne le STIG, il est recommandé de passer en revue les éléments de gravité de la catégorie 1 (CAT I – Élevée) et de la catégorie 2 (CAT II – Moyenne) pour comprendre les pratiques en matière de sécurité qu'il contient et de les combiner aux pratiques exemplaires de Microsoft et aux objectifs repères du CIS mentionnés à la sous-section ci-dessous. Le STIG du domaine Active Directory (en anglais seulement) [4] fournit les détails des configurations de niveau CAT I et CAT II, en plus de décrire et de détailler la façon de mettre en œuvre les configurations de sécurité recommandées.

Pour ce qui est des domaines où les conseils formulés ne correspondent pas aux utilisations pratiques dans l'infrastructure AD existante, il est recommandé de procéder à une évaluation des risques pour veiller à ce que le contrôle n'accroisse pas l'exposition aux risques ou la compromission de l'infrastructure AD en question. L'évaluation des risques permettra également de déterminer s'il est possible de mettre en place des contrôles compensatoires de sorte à tenir compte de tout écart ou de toute lacune perçue.

2.3 Center for Internet Security (CIS)

Il est recommandé d'utiliser les objectifs repères du Center for Internet Security (CIS) répertoriés ci-dessous pour favoriser l'adoption des pratiques exemplaires de Microsoft AD et en assurer la vérification.

- *Center for Internet Security (CIS) Controls version 8* (en anglais seulement) [5]
- *CIS Microsoft Windows Server 2019 Benchmark version 1.3.0* (en anglais seulement) [6]
- *CIS Microsoft Windows Server 2019 STIG Benchmark version 1.1.0* (en anglais seulement) [7]

Remarque : La section 2.3 du document des objectifs repères du CIS met l'accent sur les fonctions de sécurité, mais il est recommandé de considérer tous les domaines mentionnés.

Remarque : Les tableaux retrouvés à chaque section dressent la liste des désignations des groupes de mise en œuvre (IG pour *Implementation Group*). Il s'agit des conseils que l'on recommande de suivre pour prioriser la mise en œuvre des contrôles de sécurité essentiels du CIS (contrôles du CIS). Les IG sont divisés en trois catégories : IG1, IG2 et IG3. Chacune de ces catégories fournit un ensemble de mesures de cyberdéfense et on y présente un total de 153 mesures. Les orientations des contrôles du CIS sont définies ci-dessous.

2.3.1 IG1 – Pratiques exemplaires de base en cybersécurité

La version 8 des contrôles du CIS définit le groupe de mise en œuvre 1 (IG1) comme étant des pratiques exemplaires essentielles en cybersécurité. Elle constitue une nouvelle norme minimale en matière de sécurité de l'information pour toutes les organisations. L'IG1 est la base de référence des contrôles du CIS. Il comprend un ensemble fondamental de 56 mesures de cyberdéfense. Les mesures comprises dans l'IG1 correspondent à tout ce que les organisations devraient mettre en place pour se défendre contre les cyberattaques les plus courantes.

Les organisations de l'IG1 sont généralement de petite ou moyenne taille avec une expertise limitée en TI et en cybersécurité et peu de ressources à consacrer à la protection des biens de TI et du personnel. Le maintien des activités opérationnelles est une préoccupation courante pour ces organisations, puisqu'elles ont une tolérance limitée envers les périodes d'indisponibilité.

La sensibilité des données que ces organisations veulent protéger est faible dans la mesure où elles contiennent principalement de l'information sur le personnel ou de nature financière. Il est possible de mettre en œuvre les mesures sélectionnées pour l'IG1 avec une expertise limitée en cybersécurité. Elles visent à contrer des attaques générales et non ciblées. Ces mesures seront généralement conçues pour être déployées avec du matériel et des logiciels commerciaux sur étagère (COTS pour *Commercial Off-the-Shelf*) dans de petites entreprises ou des bureaux à domicile.

2.3.2 IG2 – Entreprise

L'IG2 est fondé sur les mesures définies pour l'IG1. Il compte 74 mesures additionnelles visant à assister les équipes de sécurité confrontées à une plus grande complexité opérationnelle. Certaines des mesures de l'IG2 varient selon la technologie de niveau entreprise et l'expertise spécialisée nécessaire pour procéder à l'installation et à la configuration.

Dans une organisation IG2 typique, la gestion et la protection de l'infrastructure de TI sont assurées par des personnes. Ces organisations offrent généralement du soutien à plusieurs ministères dont les profils de risque varient selon leurs fonctions

et leur mission. Certaines unités au sein de ces organisations peuvent également être sujettes à des obligations en matière de conformité à la réglementation. Les organisations prises en charge par l'IG2 stockent et traitent souvent de l'information sensible sur les clients ou de nature opérationnelle. Elles peuvent toutefois tolérer de brèves interruptions de service. Perdre la confiance du public advenant une violation est l'une de leurs principales préoccupations.

2.3.3 IG3 – Entreprise de nature sensible

L'IG3 est fondé sur les mesures définies pour l'IG1 et l'IG2. Il compte 23 mesures additionnelles.

Une entreprise IG3 emploie souvent des expertes et experts en sécurité qui se spécialisent dans les différents aspects de la cybersécurité, comme la gestion des risques, les tests d'intrusion et la sécurité des applications. Les biens et les données de l'IG3 contiennent de l'information sensible ou des fonctions sujettes à une surveillance réglementaire et de la conformité. Une entreprise IG3 doit tenir compte de la disponibilité des services, ainsi que de la confidentialité et de l'intégrité des données sensibles. Comme des cyberattaques fructueuses peuvent nuire considérablement au bien-être public, les entreprises IG3 doivent sélectionner des mesures susceptibles d'atténuer les attaques ciblées menées par des auteures ou auteurs de menace dotés de moyens sophistiqués et de réduire les répercussions des attaques du jour zéro.

En ce qui concerne les aspects où il est difficile, voire impossible de mettre en place les mesures de l'IG3 en raison de l'architecture ou de la configuration actuelle de l'infrastructure AD de votre organisation, il est recommandé de procéder à l'évaluation des risques pour l'ensemble des contrôles qui ne peuvent se conformer qu'à l'IG1 ou à l'IG2.

3 Microsoft AD

AD de Microsoft est un référentiel de données structuré pour le stockage d'objets de données d'annuaire. Il peut être utilisé pour gérer les ressources informatiques de votre organisation, comme l'infrastructure réseau, les services de courrier, les services d'infrastructure à clé publique (ICP) et les services sans fil.

Remarque : Bien que la présente traite de la capacité de services de domaines d'AD, on peut employer la suite pour des rôles additionnels.

Chacune des sections ci-dessous définit les différentes fonctions d'AD et fournit des références qui peuvent faciliter le déploiement d'AD dans votre organisation. Il importe de souligner que la présente n'a pas pour but de servir de « manuel de conception » pour les services AD, puisque le contexte du déploiement varie d'une organisation à l'autre. L'information comprise dans cette section fait plutôt référence à des points des pratiques exemplaires qu'une organisation peut considérer et inclure dans les résultats de son évaluation des risques et le contexte de son déploiement.

3.1 Capacités d'AD

Les sous-sections ci-dessous donnent des détails généraux sur chacune des capacités pertinentes d'AD. Des ressources additionnelles ont été fournies aux praticiennes et praticiens qui veulent acquérir des connaissances approfondies sur la capacité.

3.1.1 Services de domaines AD (AD DS)

Les AD DS sont utilisés pour assurer la gestion des utilisatrices, des utilisateurs et des ressources. Ils prennent en charge les applications avec annuaire comme Microsoft Exchange Server. Les AD DS fournissent une base de données distribuée permettant de stocker et de gérer l'information relative aux ressources et aux données propres aux applications avec annuaire. Prière de consulter les documents complémentaires suivants sur AD DS pour une meilleure compréhension et les pratiques exemplaires recommandées :

- *Meilleures pratiques pour la sécurisation d'Active Directory de Microsoft* [3];
- *AD DS Security Technical Implementation Guide (STIG)* (en anglais seulement) [4].

3.1.2 Services de fédération AD (AD FS)

Les services de fédération AD (AD FS pour *Active Directory Federation Services*) offrent des capacités de fédération des identités et d'authentification unique (SSO pour *Single Sign-On*) pour les applications Web. Les AD FS servent de fournisseur d'identités et authentifient les utilisatrices et utilisateurs afin de fournir les jetons de sécurité pour les applications qui autorisent le recours aux AD FS. Ils offrent également les capacités de fédération nécessaires pour utiliser les jetons d'autres fournisseurs d'identités et fournir les jetons de sécurité aux autres applications. Prière de consulter les documents complémentaires suivants sur les AD FS :

- *Mettre à niveau une batterie de serveurs AD FS existante à l'aide de la base de données interne Windows* [8];

- *Meilleures pratiques en matière de services de fédération Active Directory (AD FS)* [9].

Il convient de considérer les AD FS lorsque l'on déploie AD, et plus précisément, les contrôleurs de domaines (DC pour *Domain Controller*) de votre organisation, puisque l'emplacement et la configuration des services de fédération faciliteront le contrôle des justificatifs d'identité, aideront à mettre en place l'authentification unique et fourniront plus d'options pour ce qui est d'adopter ultérieurement la GIJIA dans les plateformes des fournisseurs de services infonuagiques (FSI).

3.1.3 Services de certificat AD (AD CS)

Les services de certificat AD (AD CS pour *Active Directory Certificate Services*) servent à créer et à gérer l'ICP et à fournir la cryptographie à clé publique, les certificats numériques et les capacités de signature numérique nécessaires à votre organisation. Prière de se reporter aux conseils suivants sur les AD CS :

- *Active Directory Certificate Services Overview* (en anglais seulement)[10];
- *Microsoft Certification Authority Guidance* (en anglais seulement) [11].

3.1.4 Services de gestion des droits AD (AD RMS)

Les services de gestion AD (AD RMS pour *Active Directory Rights Management Services*) aident à protéger l'information en ayant recours à la gestion des droits au sein de votre organisation. Prière de consulter ce qui suit :

- *Active Directory Rights Management Services Overview* (en anglais seulement) [12].

3.1.5 Services d'annuaire légers AD (AD LDS)

Les services d'annuaire légers AD (AD LDS pour *Active Directory Lightweight Directory Services*) sont des services d'annuaire compatibles avec le protocole allégé d'accès annuaire (LDAP pour *Lightweight Directory Access Protocol*) qui permettent d'assurer le stockage et la récupération des données pour les applications avec annuaire, sans être soumis aux dépendances et aux restrictions d'AD DS par rapport aux domaines. Les AD LDS fournissent les mêmes fonctionnalités qu'AD DS, sans exiger le déploiement de domaines ou de contrôleurs de domaines. Prière de se reporter aux conseils suivants sur les AD LDS :

- *Active Directory Lightweight Directory Services Overview* (en anglais seulement) [13].

3.2 Architecture de déploiement d'AD

Il est possible de déployer AD dans différents modes d'architecture et dans plusieurs cas, on déploie ces services pour gérer une infrastructure et des applications sur site traditionnelles. Cette option de déploiement permet à votre organisation de gérer pleinement son service d'annuaire de bout en bout. L'orientation offerte dans la section suivante concerne principalement les environnements sur site où on déploie des services pour gérer une infrastructure et des applications sur site traditionnelles. Cette option de déploiement permet à votre organisation de gérer pleinement son service d'annuaire de bout en bout.

4 Stratégies de renforcement et d'atténuation additionnelles

Les déploiements sur site des services AD de Microsoft peuvent être protégés contre de nombreuses menaces en renforçant les défenses et les contrôles, tel qu'il est énoncé dans les résumés et les ressources mentionnés à la section 2 ci-dessus. Comme indiqué, les stratégies de renforcement et d'atténuation demandent la mise en place de mesures visant à protéger les justificatifs, les systèmes, les processus et les identités. Les sections suivantes proposent des stratégies additionnelles pour les éléments entourant AD qui relèvent du processus de sauvegarde.

4.1 Considérations en matière d'environnement

En plus des paramètres de configuration particuliers mentionnés à la section 3, la sécurisation d'AD dans votre organisation repose essentiellement sur l'utilisation des protocoles appropriés et des composants système établis dans l'ensemble de l'environnement utilisateur. Les sous-sections ci-dessous présentent les points à considérer et les mesures à prendre pour s'assurer que vos facteurs environnementaux ne restreignent pas la capacité de votre AD à maintenir une posture connue et sécurisée.

Gestion des systèmes

La gestion des systèmes porte sur les contrôles liés à l'établissement de frontières pour le système et à la mise en œuvre d'un plan sécurisé pour assurer l'approvisionnement des services AD et l'accès sécurisé continu à ces services.

Utiliser des stations de travail administratives dédiées pour toutes les tâches administratives

Par station de travail administrative dédiée, on entend un client léger ou un poste de travail sécurisé servant à accomplir des tâches administratives sensibles ou des tâches exigeant un accès privilégié. Ce dispositif ne doit pas permettre d'accéder à Internet et les services comme le courrier électronique et la navigation Web doivent être désactivés et interdits. Les utilisatrices et utilisateurs de votre organisation qui exécutent des tâches administratives ou privilégiées devraient tous le faire à partir d'une station de travail administrative dédiée conçue à cette fin. Vous devriez vous assurer que chaque station de travail administrative dédiée n'est pas administrée par l'utilisatrice ou l'utilisateur à qui elle a été assignée.

Votre organisation devrait configurer son serveur AD de manière à ce que l'accès privilégié ne puisse être utilisé qu'au moyen d'une station de travail administrative dédiée qui n'est pas partagée parmi plusieurs utilisatrices et utilisateurs. Chacune des stations de travail administratives dédiées devrait être configurée avec la sécurité la plus élevée disponible. Il convient également de restreindre les comptes d'administrateur locaux et les applications pouvant être installées.

Vous devriez faire en sorte que les comptes privilégiés utilisés sur les stations de travail administratives dédiées ne soient pas journalisés dans les zones de confiance des niveaux inférieurs. L'accès à Internet doit être impérativement désactivé, ainsi que les services non liés à l'administration, comme le courrier électronique et la navigation Web. Les connexions réseau de vos stations de travail administratives dédiées devraient se limiter à ce qui est requis pour exécuter les tâches administratives. Pour renforcer la sécurité de vos stations de travail, vous devriez mettre en place des outils permettant de créer des listes des applications autorisées, comme AppLocker ou le contrôle d'application de Windows Defender, pour vous assurer que seules les applications approuvées peuvent être installées ou exécutées. Vous devriez également activer le chiffrement de disque sur les dispositifs et les stations de travail administratives dédiées. Prière de consulter le guide du

DoD des États-Unis, Microsoft Windows Privileged Access Workstation (PAW) STIG (en anglais seulement) [14], pour des directives détaillées sur le paramétrage de ces systèmes. En plus des conseils formulés dans la présente section, il convient d'envisager de prendre des mesures pour sécuriser vos dispositifs et vos stations de travail administratives dédiées :

- Tenir compte des technologies permettant l'utilisation de bases matérielles de confiance
  - Module de plateforme sécurisée 2.0 (TPM pour *Trusted Platform Module*)
  - Chiffrement de lecteur BitLocker
  - Démarrage sécurisé Unified Extensible Firmware Interface (UEFI)
  - Protection d'E/S de l'accès direct à la mémoire (DMA pour *Direct Memory Access*)
- Activer les fonctionnalités de sécurité basée sur la virtualisation (SBV)
  - Intégrité du code protégé par hyperviseur (HVCI pour *Hypervisor-protected Code Integrity*)
  - Vue d'ensemble de Credential Guard [15]
- Activer le contrôle des applications pour permettre les listes d'applications autorisées

Utiliser des comptes privilégiés distincts pour les tâches administratives

Votre organisation devrait séparer les comptes privilégiés servant à exécuter des tâches administratives sur des systèmes locaux des comptes privilégiés servant à exécuter d'autres tâches administratives. Vous devriez également vous assurer qu'aucun compte administrateur n'est affecté à plusieurs groupes à l'extérieur du même domaine de sécurité. Tous les accès des administratrices et administrateurs de domaine et accès équivalents devraient être très restreints. Les comptes de service et d'agent devraient être contrôlés avec la même rigueur en matière de contrôle des modifications que l'accès des administratrices et administrateurs de domaine. Vous devez configurer les comptes privilégiés en tant que membres d'un groupe d'utilisateurs protégés, veiller à ce que les mécanismes de protection des justificatifs d'identité soient appliqués par défaut et éviter que les justificatifs d'identité non chiffrés soient mis en cache sur les dispositifs auxquels les utilisatrices et utilisateurs ont accès [16].

Mettre hors service ou isoler les services et applications Active Directory hérités

Dans la mesure du possible, votre organisation devrait mettre hors service les systèmes exécutant des services AD désuets et des applications héritées. En ce qui a trait aux services essentiels aux activités qu'il est impossible de mettre hors service immédiatement, il est recommandé de déplacer ces applications et ces services dans une forêt séparée et isolée. Vous devriez désactiver l'utilisation de la norme de chiffrement de données (DES pour *Data Encryption Standard*) pour Kerberos, ainsi que la version 1 du bloc de messages de serveur (SMB pour *Server Message Block*) (SMBv1) sur le client SMB et les composants des serveurs [17].

Limiter les connexions réseau vers les serveurs Active Directory

Vous devriez utiliser un pare-feu hôte, comme le pare-feu de Windows, ainsi que des solutions d'infrastructure réseau pour limiter les connexions entrantes et sortantes aux systèmes AD dans la mesure où de telles connexions ne sont pas autorisées. Vous pouvez renforcer la protection de votre réseau en mettant en place une liste d'autorisation pour restreindre les connexions entrantes aux systèmes désignés et aux applications approuvées seulement. Il convient de bloquer tous les accès Internet entrants et sortants à votre service AD et de s'assurer que toute administration à distance est effectuée exclusivement à partir d'une station de travail administrative dédiée en faisant appel uniquement au protocole RDP (Remote Desktop Protocol) chiffré par protocole TLS (Transport Layer Security).

Configurer des comptes à accès privilégié uniques et des mots de passe d'administrateurs locaux pour les serveurs et les stations de travail

On doit s'assurer que l'organisation crée des justificatifs d'identité uniques en mode restauration des services d'annuaire sur les serveurs AD et des mots de passe uniques d'administration locale sur toutes les stations de travail accessibles aux utilisatrices et utilisateurs. On doit impérativement s'assurer que les mots de passe de vos comptes d'administrateur local sont uniques. Les comptes privilégiés ne devraient également être utilisés que par une seule utilisatrice ou un seul utilisateur et respecter le principe de droit d'accès minimal. Il est fortement recommandé de désactiver l'utilisation de comptes d'administrateur partagés et de mettre en œuvre le filtrage de mot de passe d'AD [18] pour bloquer l'utilisation de mots de passe compromis ou de mauvais mots de passe.

Appliquer la séparation des tâches pour les tâches administratives

Votre organisation peut mettre en place la séparation des tâches au moyen de stratégies et de procédures, ce qui permettra de gérer les risques posés par la menace interne et la compromission de comptes privilégiés.

Bloquer les comptes privilégiés pour empêcher leur utilisation sur des systèmes non autorisés

Il est recommandé d'éviter que des comptes privilégiés soient utilisés sur des systèmes non autorisés. Pour ce faire, il est possible, par exemple, de faire en sorte que les comptes privilégiés d'une station de travail administrative dédiée ne puissent pas être utilisés pour accéder à des biens de niveau inférieur.

Tenir compte des solutions de transfert géré de fichiers au moment de connecter différents domaines entre eux

Vous devriez envisager de mettre en œuvre des solutions de transfert géré ou sécurisé de fichiers avec des fonctionnalités similaires aux principes de la Solution interdomaines (SID) pour les interconnexions entre les différents environnements de la posture de sécurité. Comme la SID à assurance élevée est principalement utilisée pour les transferts entre domaines ayant un niveau supérieur ou inférieur de sensibilité, il est généralement déconseillé dans un tel scénario. Si une SID à assurance élevée est requise pour assurer la séparation locale d'AD, il est recommandé de consulter le Centre pour la cybersécurité.

4.2 Gestion des comptes

La gestion des comptes porte sur les contrôles fondamentaux qui permettent de gérer en toute sécurité tous les comptes privilégiés et d'utilisateur, et ce, de l'approvisionnement à la mise hors service dans les environnements de services AD. Parmi les exemples de comptes privilégiés, notons les comptes administratifs locaux et de domaine, les comptes de services et les comptes administratifs intégrés.

Mettre en place l'AMF pour tous les comptes d'utilisateur et d'administrateur

Tous les accès aux services d'Active Directory doivent faire appel à des jetons matériels (comme une carte à puce et un clavier, une clé USB) pour tous les comptes d'utilisateur et d'administrateur conformément aux conseils de Microsoft [19] [20]. Les cartes à puce sont peu coûteuses à remplacer au besoin et plusieurs modèles de claviers sont dotés de mécanismes robustes contre l'hameçonnage qui permettent de traiter les NIP indépendamment du point terminal pour le déverrouillage des clés privées. Certains jetons permettent d'utiliser un troisième facteur sous la forme d'un lecteur

d'empreinte digitale pour déverrouiller les clés privées, mais ceux-ci sont généralement plus chers qu'une combinaison de carte à puce et de clavier. L'utilisation de jetons logiciels (comme un point terminal ou un téléphone) ne constitue pas un véritable facteur d'authentification, puisqu'il est possible d'obtenir le certificat et de tenter de contourner le mécanisme. Une telle utilisation n'est donc pas jugée suffisante. Le mot de passe de tous les comptes d'utilisateur doit être stocké au moyen d'une clé à norme de chiffrement avancée (AES pour *Advanced Encryption Standard*).

Restreindre l'appartenance aux groupes Administrateur d'entreprise et Administrateur de domaine

Il convient de restreindre l'appartenance aux groupes Administrateur d'entreprise (EA pour *Enterprise Admins*), Administrateur de domaine et Administrateur intégré (BA pour *Built-in Administrator*). Ces groupes de comptes ne devraient comporter aucune appartenance permanente à des comptes d'utilisateur. On devrait accorder aux administratrices et administrateurs de système une appartenance EA et des autorisations d'administrateur de domaine, selon les besoins.

Utiliser le principe du droit d'accès minimal pour attribuer et gérer les droits et des privilèges d'administration

Tous les comptes privilégiés et d'utilisateur, dont les comptes de service et les comptes d'application, devraient être configurés selon le principe de droit d'accès minimal. Votre organisation devrait utiliser des comptes de service géré dans la mesure du possible et éviter d'attribuer des comptes de service à des groupes privilégiés intégrés, comme les groupes Administrateur local et Administrateur de domaine. Vous devriez également vous assurer que ces comptes de service ne sont utilisés que par les applications ou les services, plutôt que les utilisatrices ou utilisateurs, et refuser toutes les ouvertures de session interactives. Par ailleurs, votre organisation devrait empêcher les comptes de service d'exécuter des traitements par lots. On ne devrait accorder que les autorisations et privilèges nécessaires pour réaliser les tâches assignées. Les administratrices et administrateurs de système devraient fournir les comptes privilégiés et d'utilisateur, ainsi que les comptes locaux et de domaine, de manière à assurer le principe de droit d'accès minimal. Les comptes de service d'administration ou à accès limité devraient commencer par des autorisations d'utilisateur de base et un accès additionnel devrait être accordé selon les besoins organisationnels.

Mettre en place la création de comptes privilégiés « juste à temps »

Vous ne devriez mettre en place des autorisations d'accès privilégié que lorsque cela s'avère nécessaire et déployer les systèmes de manière à accorder une appartenance temporaire aux groupes privilégiés que selon les besoins. Vous devriez également vous assurer que les autorisations et les privilèges sont supprimés une fois que les tâches assignées sont achevées et éliminer toute appartenance temporaire aux groupes privilégiés.

Passer régulièrement en revue les comptes et supprimer les comptes inutilisés

On recommande à votre organisation de passer régulièrement en revue l'accès des utilisatrices et utilisateurs, et les comptes inutilisés. Vous devriez supprimer les autorisations d'accès non requises, ainsi que tout compte inutilisé. Il est également recommandé de désactiver dès que possible les comptes d'utilisateur périmés ou inactifs et de mettre en place un système de surveillance pour les événements liés à l'utilisation de ces comptes.

4.3 Sécurité des applications

En limitant les applications autorisées sur les serveurs AD et en permettant ou en installant uniquement les services et les applications qui sont essentiels à l'exécution et au soutien des fonctions des services d'annuaire, votre organisation aura une posture de renforcement plus solide pour ses services AD. Ainsi, votre organisation a un ensemble de services plus restreints qui s'exécutent sur ses serveurs AD, alors que les services cohébergés sont déplacés et mis à l'écart des services AD. Limiter le plus possible le nombre de logiciels exécutés est une étape essentielle du renforcement de la sécurité et de la réduction de la surface d'attaque. Vous devriez également mettre en place des listes d'applications autorisées sur les serveurs et les stations de travail administratives.

La mise en œuvre de listes d'applications autorisées sur les serveurs et les stations de travail administratives permet de garantir que seules les applications approuvées explicitement sont installées sur les systèmes de services d'annuaire. Des contrôles basés sur l'hôte et des contrôles basés sur les stratégies devraient aussi être mis en œuvre sur les serveurs AD et les stations de travail administratives dédiées pour empêcher l'installation et l'utilisation non autorisées d'applications. Seules les applications en mémoire et les installations permanentes figurant dans la liste d'applications autorisées doivent être en mesure de s'exécuter.

S'assurer que les comptes de service sont configurés et protégés adéquatement

Dans la mesure du possible, les comptes de service de votre organisation ne devraient pas appartenir à des groupes protégés intégrés dans AD. Pour y arriver, il est recommandé de déléguer un ensemble minimum des autorisations requises ou d'accorder des droits d'accès d'utilisateur par l'entremise d'une stratégie de groupe. Les comptes de service ne doivent pas dépasser les niveaux et il est interdit de les utiliser de façon interactive. La pré-authentification Kerberos doit être activée en permanence sur vos comptes de service. Cette fonctionnalité ne devrait jamais être désactivée. Dans la mesure du possible, vous devriez également remplacer vos comptes de service par des comptes de service géré de groupe et réinitialiser régulièrement les clés des comptes de service de nature sensible, comme *Krbtgt*. Enfin, votre organisation devrait s'assurer que le service spouleur d'impression est désactivé [21].

4.4 Journalisation, surveillance et audit

Des mécanismes de surveillance, d'audit et de journalisation doivent être mis en place pour les activités liées aux services d'annuaire. C'est particulièrement vrai pour les tâches de comptes privilégiés. Votre organisation devrait journaliser, surveiller et vérifier les événements d'échec et de réussite associés aux opérations sur les serveurs sensibles ou essentiels.

Les tâches exigeant un accès privilégié devraient être journalisées, surveillées et vérifiées

Votre organisation devrait s'assurer que tous les comptes administratifs et privilégiés sont surveillés, journalisés et vérifiés pour veiller à ce qu'on les utilise de façon appropriée. Le service d'annuaire est un bien indispensable. La priorité devrait être accordée à la surveillance et à l'audit des tâches administratives connexes. Protégez et surveillez les activités effectuées sur les comptes privilégiés. Activez les paramètres d'audit des systèmes et vérifiez régulièrement les comptes. Mettez en place un outil de vérification des changements dans AD pour surveiller tout changement apporté aux différents éléments de la configuration d'AD.

La collecte des journaux système devrait être automatisée, isolée et protégée

Votre organisation devrait automatiser la collecte des journaux système et veiller à ce que ces derniers soient protégés contre les menaces potentielles. Les systèmes organisationnels contenant les données de sauvegarde devraient être isolés de l'AD d'entreprise, puisque la compromission des justificatifs d'identité de domaine peut donner lieu à la suppression ou à la modification des journaux collectés précédemment. Les journaux d'événements peuvent également être acheminés à un serveur de GIES centralisé pour faciliter l'agrégation, le regroupement et l'analyse des événements. Des mécanismes d'alerte automatisés doivent être mis en place pour repérer toute violation des stratégies de sécurité à incidence élevée et permettre une prise de mesures d'intervention plus rapide.

4.5 Détection des menaces et intervention

La détection des menaces et l'intervention doivent tenir compte de différents scénarios possibles, comme une compromission de vos biens AD provenant d'une auteure ou d'un auteur de menace, et des contrôles de détection à mettre en place.

Détecter les menaces malveillantes au moyen d'indicateurs de compromission et de technologies de prévention des menaces automatisées

Votre organisation peut améliorer la prévention et la détection de techniques d'attaque connues en se servant d'indicateurs de compromission (IC) et de technologies de prévention des menaces automatisées. Vous devriez surveiller les événements Windows sensibles liés aux services AD susceptibles d'indiquer une tentative de compromission ou une compromission fructueuse. En faisant appel à des solutions de détection et de prévention des menaces sur le réseau ou les terminaux, votre organisation peut détecter les tentatives de compromission de ses services AD et prendre les mesures nécessaires pour intervenir.

Activer les solutions d'antimaliciels et les antivirus

Pour ajouter un niveau supplémentaire de protection, votre organisation devrait mettre en place des solutions d'antimaliciels et mettre à jour les antivirus et antimaliciels de tous les systèmes en temps opportun. Ces outils de détection devraient surveiller les tentatives visant à désactiver ou à neutraliser les solutions d'antimaliciels.

4.6 Application des correctifs et gestion des changements

L'infrastructure de vos services AD devrait être maintenue et mise à jour en appliquant les correctifs et mises à jour sur votre système d'exploitation et vos applications en temps opportun. L'application de correctifs devrait être effectuée par incrément, tel qu'il est mentionné à la section 4.1. Votre organisation devrait s'assurer d'adopter des processus de gestion des changements officiels pour confirmer et attester que les mises à jour ont bien été appliquées.

Activer l'application automatisée de correctifs sur le système d'exploitation, les applications et les dispositifs

Votre organisation devrait élaborer un énoncé de stratégies pour l'application automatisée des correctifs liés aux composants de son serveur d'AD, ce qui comprend le système d'exploitation, les applications installées et les périphériques.

Elle devrait journaliser les divulgations de vulnérabilité susceptibles d'avoir une incidence sur ses services AD et prioriser la mise en œuvre des correctifs.

Sécuriser les processus de gestion des changements

Votre processus de gestion des changements devrait s'assurer que vous mettez en œuvre la gestion des changements, passez fréquemment en revue les exigences en matière de conformité à la réglementation et évaluez les paramètres de chacune des nouvelles versions matérielles et logicielles déployées. Vous devriez veiller à ce que les changements apportés à la configuration soient configurés de manière à déclencher des alertes immédiates et que ces alertes soient passées en revue par l'unité de votre organisation chargée d'autoriser les changements de configuration. Vous devriez également mettre en place un outil de vérification des changements dans les services AD pour surveiller tout changement apporté aux différents éléments de la configuration d'AD.

4.7 Continuité des activités

La continuité des activités sous-entend que votre organisation doit avoir mis en place des activités de planification d'urgence pour aider à la reprise du service d'annuaire en cas de menaces de toute sorte, comme des interruptions de système ou des incidents liés à la cybersécurité.

Dans le cadre de vos efforts de continuité des activités, il serait bon d'établir des processus qui permettent la collecte automatisée des données essentielles du système et des sauvegardes de l'information. Veillez à ce que les sauvegardes fassent l'objet de tests périodiques. Ces tests pourraient avoir lieu chaque trimestre ou après un changement important pour valider l'intégrité et l'utilité. Vos données de sauvegarde doivent être isolées du réseau principal. Il convient également d'accorder une attention particulière à la conservation de sauvegardes hors ligne, en plus de toute autre stratégie de sauvegarde déjà en place. Votre organisation doit s'assurer que ses sauvegardes sont chiffrées et protégées et que seuls les comptes autorisés sont en mesure d'y accéder. Toute modification apportée aux sauvegardes devrait exiger plusieurs facteurs d'authentification pour y accéder. Vous devriez également envisager de mettre en œuvre la corbeille des services AD pour vous aider à récupérer vos objets AD [22].

Créer, tester et mettre à jour les plans d'intervention en cas d'incident

Dans le cadre de son processus de reprise global, votre organisation devrait créer, tester et mettre à jour des plans d'intervention en cas d'incident pour remédier aux scénarios de risques potentiels qui pourraient toucher l'organisation. Vous devriez également fournir des exercices de formation ou de simulation aux administratrices et administrateurs de système afin de leur permettre d'élaborer et de valider des plans d'intervention et de reprise.

Créer un plan de reprise de la forêt AD

Il est essentiel de pouvoir rétablir les services AD pour assurer la reprise des services advenant des perturbations de la sécurité. Votre plan de reprise devrait être axé sur les efforts à déployer à la suite d'incidents de sécurité qui pourraient avoir une incidence sur l'intégrité ou la disponibilité de votre environnement AD. Vous devriez inclure les procédures de reprise des systèmes et la documentation de l'environnement et mettre à l'essai vos plans de reprise sur une base régulière. Le plan de reprise devrait être mis à jour selon vos tests et les leçons tirées de manière à refléter les changements qu'il convient

d'apporter à vos processus, à vos procédures ou aux configurations dans votre environnement. Dans le cadre de vos initiatives de planification des sauvegardes et de la reprise, vous devez vous assurer que les sauvegardes des forêts AD et la documentation connexe sont stockées hors ligne. Dans la mesure du possible, votre organisation devrait également envisager de stocker les sauvegardes dans une solution de stockage ou une plateforme en nuage.

4.8 Formation des utilisatrices et utilisateurs

Votre organisation doit organiser régulièrement des séances de sensibilisation à la sécurité pour les détentrices et détenteurs de comptes privilégiés et les autres utilisatrices et utilisateurs finaux de système.

Former les administratrices et administrateurs de système et les utilisatrices et utilisateurs finaux sur les pratiques exemplaires en matière de sécurité

Votre programme de formation doit être conçu pour offrir une formation continue à l'ensemble des utilisatrices et utilisateurs sur les pratiques exemplaires en matière de sécurité, favoriser des comportements axés sur une bonne sensibilisation à la sécurité et adopter des pratiques en cybersécurité pour contrer les comportements indésirables plus à risque. Votre organisation devrait également établir des processus visant à simplifier les exigences de sécurité pour les utilisatrices et utilisateurs finaux, et ce, en tirant profit de séances de formation structurées et de supports visuels.

On recommande que les administratrices et administrateurs de système de votre organisation soient formés de manière à ce que la portée de leur contrôle soit moins vaste, comme se limiter à une seule forêt, et à pouvoir travailler avec une équipe de contrôle comptant deux personnes.

5 AD et le nuage

Il faut soigneusement prendre en compte les déploiements et les migrations en nuage hybrides. L'inclusion d'une fonction de service infonuagique sous-entend l'utilisation d'un hyperviseur, ce qui pourrait transformer radicalement la posture de sécurité d'un déploiement sur site, puisque l'on introduit également différentes préoccupations de sécurité et fonctions de mise en réseau qui doivent être prises en considération.

Les services AD peuvent quand même être utilisés pour les capacités de GIJIA sur le nuage au moyen de solutions sur site existantes. C'est ce que l'on appelle généralement une architecture « hybride », puisque certains éléments sont contrôlés et exploités sur site, et que d'autres éléments sont connectés et ensuite synchronisés aux services d'annuaire du FSI. Dans certains déploiements, les configurations d'un serveur AD restent en soi les mêmes, puisque la différence ou le changement principal consiste à utiliser la plateforme d'infrastructure-service (IaaS pour *Infrastructure as a Service*) du FSI. Dans ce type de déploiement, le contrôle de certains aspects physiques et du réseau changera en fonction du modèle d'infonuagique fondé sur le partage des responsabilités lié à l'infonuagique.

Les deux principales approches à l'égard d'une architecture « hybride » sont :

a) **Sur site (dans un centre de données de client) :** Les contrôleurs de domaine sont fédérés et affectés aux services infonuagiques par les services ADFS sur site.

b) **Sur site étendue (autogérée) :** Les contrôleurs de domaine sur site et déployés sur une plateforme IaaS de FSI.

- En utilisant la même forêt ou une approbation de forêt, les domaines déployés de cette façon sont techniquement hybrides, car ils se synchronisent et sont fédérés localement, en plus de faire vraisemblablement appel à ADFS sur site et à la fédération.
- Dans ce cas, il n'y a toujours pas une synchronisation directe ou complète des identités avec un fournisseur d'identité (IdP pour *Identity Provider*) pour constituer une identité native en nuage.
- Bien qu'il s'agisse d'une approche possible, il est à noter qu'elle n'est pas recommandée à long terme, car elle implique des changements fondamentaux à la posture de sécurité, rendant du coup les mesures de protection énoncées dans la présente publication impossibles à mettre en œuvre. Cette approche devrait normalement être considérée comme une stratégie de transition ou de migration.

Voici quelques-unes des principales différences entre l'adoption d'une approche hybride et un déploiement complet par l'intermédiaire des services d'un FSI ou d'un IdP :

1. Les clients sont responsables du contrôle de plusieurs des facteurs environnementaux mentionnés ci-dessus et peuvent procéder à la vérification et à une mise à niveau;
2. Un client peut limiter le nombre de points de données dans les justificatifs d'identité qui sont transmis au FSI ou synchronisés avec celui-ci;
3. En faisant appel à des services fédérés, le client peut mener à bien des actions, comme centraliser le contrôle, l'examen et la vérification des justificatifs d'identité de l'organisation;

4. Au besoin, le client peut choisir de passer à un autre FSI ou d'utiliser plusieurs services et fournisseurs, puisqu'il n'a pas à confirmer le FSI et à travailler avec lui pour assurer la compatibilité de la plateforme et des services avec les autres FSI;
5. Les évaluations des risques liés à l'infrastructure AD sont plus faciles à réaliser. Comme c'est le cas pour les déploiements sur site, elles offrent une plus grande visibilité, puisque le client est toujours largement responsable de la plateforme infonuagique (IaaS, plus particulièrement) en ce qui a trait aux éléments comme l'application de correctifs.

Si votre organisation décide d'étendre ou d'autoriser une forêt entre des déploiements sur site et d'IaaS (tel qu'il est indiqué dans le profil de contrôle de sécurité), il sera nécessaire d'appliquer les changements relatifs à un déploiement sur site exclusivement. Les ATO et l'évaluation et autorisation de sécurité (EAS) découlant du déploiement sur site ne s'appliqueront plus, même si toutes les configurations sont identiques sur le plan fonctionnel, puisque l'infrastructure sous-jacente a changé. Plus particulièrement, les séparations physiques recommandées pour les serveurs AD sur site ne peuvent pas être mises en œuvre dans l'IaaS et on ne s'attend pas à ce que les autres contrôles de compensation puissent fournir une défense contre les attaques en amont du système d'exploitation. S'il est nécessaire de procéder au déploiement d'IaaS d'une fonctionnalité AD DS à des fins opérationnelles, votre organisation devrait séparer les forêts.

Au moment de considérer un nouveau déploiement ou d'envisager de créer une stratégie réseau pour votre organisation, il est important de prendre note que cette approche – et les options hybrides mentionnées précédemment – est toujours valide, mais qu'il faudra tenir compte des dépenses en capital et des coûts opérationnels continus pour chacune de ces approches. Dans le cas où les services d'un FSI ou d'un IdP sont utilisés, le client permet que la totalité de l'identité ou des justificatifs d'identité de ses utilisatrices et utilisateurs soit formée et utilisée dans ces services. Cette façon de procéder offre des avantages, car des facettes de l'application des correctifs et des mises à niveau à la solution de GIJIA sont effectuées par le FSI conformément à l'abonnement auquel souscrit votre organisation.

Cette approche implique toutefois un changement fondamental dans l'utilisation des services AD en ce sens que votre organisation est maintenant dépendante des services infonuagiques. En d'autres termes, plusieurs des recommandations formulées dans cette publication devront être revues, puisque le contrôle du matériel physique et l'étendue du contrôle sur d'autres fonctions changeront de manière radicale. En outre, la capacité de votre organisation est réduite en ce qui concerne la visibilité et le contrôle des justificatifs d'identité, car elle doit collaborer avec le fournisseur dans tous les cas où des mesures et des services additionnels, ou une utilisation des justificatifs en dehors des principales fonctions de service du fournisseur, sont requis.

6 Contenu complémentaire

6.1 Liste d'abréviations, d'acronymes et de sigles

Abréviation, acronyme ou sigle	Définition
AAD	Azure Active Directory
AD	Microsoft Active Directory
AD DS	Services d'annuaire Active Directory (Active Directory Domain Services)
AES	Norme de chiffrement avancée (Advanced Encryption Standard)
AMF	Authentification multifacteur (Multi-Factor Authentication)
API	Interface de programmation d'applications (Application Programming Interface)
CIS	Center for Internet Security
CST	Centre de la sécurité des télécommunications
DoD	Department of Defense des États-Unis
ESAE	Architecture ESAE (Enhanced Security Admin Environment)
GC	Gouvernement du Canada
GIJIA	Gestion de l'identité, des justificatifs d'identité et de l'accès
IaaS	Infrastructure-service (Infrastructure as a Service)
IdP	Fournisseur d'identité (Identity Provider)
ITSG-33	La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie
LoA	Niveau d'assurance (Level of assurance)
SA	Secteur d'activités
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
TLS	Protocole TLS (Transport Layer Security)
TPM	Module de plateforme sécurisée (Trusted Platform Module)
UEFI	Unified Extensible Firmware Interface
USB	Bus série universel (Universal Serial Bus)

6.2 Glossaire

Abréviation, acronyme ou sigle	Définition
Azure Active Directory (Azure AD)	Gestion d'identité et des appareils mobiles en nuage offrant des services de comptes d'utilisateur et d'authentification pour les ressources comme Microsoft 365, le portail Azure ou les applications de SaaS.
Forêt	Regroupement d'arbres AD qui partagent une configuration et un schéma communs et qui sont liés par des relations de confiance.
Multifacteur	Caractéristique d'un système d'authentification ou d'un jeton qui fait intervenir plus d'un facteur d'authentification. Les trois types de facteurs d'authentification sont les suivants : 1) quelque chose que l'utilisatrice ou l'utilisateur connaît, 2) quelque chose qu'il possède et 3) quelque chose qui le caractérise.
Niveau d'assurance (*Level of assurance*)	Degré de confiance dans le processus de filtrage utilisé pour établir l'identité d'une personne et les contrôles utilisés pour gérer les justificatifs d'identité qui leur ont été confiés.
Résistance à la personnification du vérificateur	Utilisation d'authentifiants qui permettent de résister aux tentatives des parties de confiance et des vérificateurs frauduleux qui cherchent à tromper un demandeur non averti afin qu'il s'authentifie sur le site Web d'un imposteur. Un protocole d'authentification résistant à la personnification du vérificateur DOIT établir un canal protégé et authentifié avec le vérificateur.
Résistance aux compromissions du vérificateur	Utilisation d'authentifiants qui exigent que le vérificateur stocke une copie de leur clé secrète. Il peut s'agir, par exemple, d'un authentifiant de mot de passe à usage unique qui exige que le vérificateur génère indépendamment le résultat de l'authentifiant en vue de le comparer à la valeur envoyée par le demandeur.
Services d'annuaire Active Directory (AD DS)	Serveur avec protocole allégé d'accès annuaire (LDAP) d'entreprise offrant des fonctionnalités clés comme l'identité et l'authentification, la gestion des objets informatiques, les stratégies de groupe et les approbations [23].
Services d'annuaire Azure Active Directory (Azure AD DS)	Solution de gestion des identités en nuage qui fournit des services d'annuaire gérés avec un sous-ensemble de fonctionnalités AD DS pleinement compatibles, comme la jonction de domaine, la stratégie de groupe, le protocole allégé d'accès annuaire (LDAP) et l'authentification Kerberos ou NTLM.

6.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie, décembre 2014.
2	Microsoft, Niveaux fonctionnels de domaine et de forêt, décembre 2021.
3	Microsoft, Meilleures pratiques pour la sécurisation d'Active Directory, juillet 2021.
4	Defense Information Systems Agency, Active Directory Domain Security Technical Implementation Guide (STIG), août 2022 (en anglais seulement).
5	Center For Internet Security, Center for Internet Security (CIS) Controls version 8, (en anglais seulement)
6	Center For Internet Security, CIS Microsoft Windows Server 2019 Benchmark version 1.3.0 (en anglais seulement), mars 2022.
7	Center For Internet Security, CIS Microsoft Windows Server 2019 STIG Benchmark version 1.1.0 (en anglais seulement), mars 2022.
8	Microsoft, Mettre à niveau une batterie de serveurs AD FS existante à l'aide de la base de données interne Windows, mars 2023.
9	Microsoft, Meilleures pratiques en matière de services de fédération Active Directory (AD FS), février 2023.
10	Microsoft, Active Directory Certificate Services Overview (en anglais seulement), août 2016.
11	Microsoft, Microsoft Certification Authority Guidance (en anglais seulement), août 2016.
12	Microsoft, Active Directory Rights Management Services Overview (en anglais seulement), août 2016.
13	Microsoft, Active Directory Lightweight Directory Services Overview (en anglais seulement), juillet 2012.
14	Department of Defense des États-Unis, Microsoft Windows Privileged Access Workstation (PAW) STIG Version 2 (en anglais seulement), octobre 2023.
15	Microsoft, Vue d'ensemble de Credential Guard, septembre 2023.
16	Microsoft, Groupe de sécurité Utilisateurs protégés, octobre 2021
17	Microsoft, Comment détecter, activer et désactiver SMBv1, SMBv2 et SMBv3 dans Windows, mai 2023.
18	Microsoft, Considérations relatives à la programmation du filtre de mot de passe, janvier 2021.
19	Microsoft, Recommandations pour l'activation de l'ouverture de session de carte à puce auprès d'autorités de certification tierces, août 2023.
20	Centre canadien pour la cybersécurité, Détermination de la robustesse des contrôles de périmètre (ITSP.80.032), mars 2019.
21	Microsoft, Évaluation de la sécurité du service spouleur d'impression, février 2023.
22	Microsoft, Récupération de forêt Active Directory : concevoir un plan de récupération de forêt AD, juillet 2023.
23	Microsoft, Comparer des services d'identité, octobre 2023.