Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Ligne directrice sur l’authentification en nuage

Publié : le 2024-12-02

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT48-51/2024F-PDF
ISBN: 978-0-660-74625-8

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Guideline on Cloud Authentication

Ligne directrice sur l’authentification en nuage

De : Secrétariat du Conseil du Trésor du Canada

Sur cette page

1. Introduction

▶ Dans cette section

1.1 Contexte

L’authentification est le processus de vérification de l’identité d’un utilisateur, d’un processus ou d’un appareil, souvent mené à bien avant d’autoriser l’accès aux ressources d’un système d’information [1]. Dans le contexte de l’informatique en nuage, et comme il est indiqué dans l’Orientation sur l’utilisation sécurisée des services commerciaux d’informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS), les organisations sont responsables de s’assurer que les personnes et les appareils sont identifiés et authentifiés de façon unique avant d’accorder l’accès aux renseignements et aux systèmes d’information

hébergés dans l'environnement d'un fournisseur de services d'informatique en nuage (FSIN). Une authentification efficace est essentielle pour assurer la sécurité des comptes.

1.2 Objet et champ d'application

Le présent document fournit des conseils et des recommandations sur la manière dont les utilisateurs internes, à savoir les utilisateurs privilégiés et non privilégiés du gouvernement du Canada (tels que les employés et les entrepreneurs) doivent être authentifiés lorsqu'ils accèdent aux services du gouvernement du Canada hébergés dans le nuage. Il ne traite pas de l'authentification des utilisateurs externes accédant aux services du gouvernement du Canada en ligne hébergés dans le nuage (ou ailleurs).

Il remplace le Guide sur l'authentification du nuage pour le gouvernement du Canada, daté du 23 août 2018. Au fil du temps, les recommandations qui y sont formulées pourront être mises à jour ou reprises par d'autres instruments de politique. Le cas échéant, il sera mis à jour en conséquence.

1.3 Applicabilité

Le présent document vise les organisations du gouvernement du Canada qui adoptent des services d'informatique en nuage. Certains énoncés d'applicabilité sont formulés le cas échéant (par exemple, lorsque les recommandations peuvent différer selon le modèle de prestation de services de l'organisation).

1.4 Public cible

Le présent document s'adresse aux praticiens des technologies de l'information (TI) et de la sécurité informatique qui exercent l'un des rôles suivants :

- gestionnaire de projet;
- analyste opérationnel;

- analyste des besoins;
- architecte d'entreprise, de la sécurité et des solutions;
- concepteur de systèmes et de logiciels;
- spécialiste de la conception des systèmes de sécurité;
- ingénieur des systèmes et de la sécurité des systèmes;
- intégrateur et testeur de systèmes, de logiciels et de sécurité;
- évaluateur de la sécurité.

1.5 Exigences

Voici les exigences en matière d'authentification tirées de divers instruments de politique du Conseil du Trésor.

1.5.1 Les administrateurs généraux sont responsables de déterminer les exigences en matière de sécurité et de gestion de l'identité pour tous les programmes et services ministériels, en tenant compte des incidences possibles sur les intervenants internes et externes (section 4.1.4).
Référence : Politique sur la sécurité du gouvernement [1]

1.5.2 Mettre en œuvre des mesures afin de veiller à ce que les personnes et les appareils soient identifiés et authentifiés de façon unique, à un niveau approprié d'assurance avant d'accorder l'accès à l'information dans les systèmes d'information, conformément à l'annexe A : Norme sur l'assurance de l'identité et des justificatifs de la Directive sur la gestion de l'identité (section B.2.3.1).
Référence : Annexe B : Procédures obligatoires relatives aux mesures de sécurité de la technologie de l'information de la Directive sur la gestion de la sécurité [2]

1.5.3 Les gestionnaires chargés de l'exécution des programmes et services assument la responsabilité de recourir aux services intégrés obligatoires en matière de gestion de l'identité, de gestion des

justificatifs et d'authentification électronique (section 4.1.9).
Référence : Directive sur la gestion de l'identité [3]

1.5.4 Les ministères doivent identifier et authentifier les personnes et les appareils jusqu'à un certain niveau d'assurance avant d'avoir accès aux renseignements et aux services hébergés dans les services d'informatique en nuage. Ces mesures d'authentification sont conformes à la Norme sur l'assurance de l'identité et des justificatifs et s'harmonisent avec les services justificatifs d'identité et d'authentification des organisations du GC (section 6.2.3).
Référence : Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS no 2017-01) [4]

1.5.5 Les administrateurs généraux sont responsables de l'utilisation des solutions, des actifs et des services de TI pangouvernementaux ou partagés, lorsque disponibles et appropriés, afin d'éviter la redondance (section 4.4.2.3).
Référence : Politique sur les services et le numérique [5]

1.5.6 Renforcement du processus d'authentification :

> 1.5.6.1 Authentifier les utilisateurs avant de leur accorder l'accès à un système et à ses ressources, en tirant parti des services d'authentification approuvés par le gouvernement du Canada, conformément à la Directive sur la gestion de l'identité et aux lignes directrices connexes, comme le Guide sur l'authentification du nuage pour le gouvernement du Canada. Les exceptions doivent être évaluées par le Comité d'examen de l'architecture intégrée du gouvernement du Canada.
>
> 1.5.6.2 Procéder à la mise en œuvre de solides mécanismes d'authentification comme l'authentification multifactorielle (AMF) pour tous les comptes détenant un accès privilégié ou amélioré, conformément au guide ITPS.30.031 du Centre canadien pour la

cybersécurité, le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information. Des renseignements supplémentaires concernant l'approche organisationnelle du gouvernement du Canada à l'égard de l'AMF sont fournis dans le document Considérations et stratégie d'authentification multifactorielle des services organisationnels de TI du GC. Au minimum, l'AMF sert à authentifier les utilisateurs des types suivants :

1.5.6.2.1 Tous les utilisateurs ayant accès aux systèmes d'information avec une exigence du niveau d'assurance de 3 ou plus.

1.5.6.2.2 Tous les utilisateurs privilégiés qui prennent des mesures privilégiées.

1.5.6.2.3 Tous les utilisateurs de solutions d'accès à distance.

1.5.6.3 Lorsque des mots de passe sont utilisés, mettre en œuvre une politique sur les mots de passe conformément à l'*Orientation sur les mots de passe* du gouvernement du Canada.

1.5.6.4 Les systèmes sont configurés avec un verrouillage de séance ou d'écran.

1.5.6.5 Les systèmes ont une bannière de connexion approuvée qui exige des utilisateurs qu'ils reconnaissent et acceptent leurs responsabilités en matière de sécurité avant qu'on leur accorde l'accès.

Référence : Exigences de configuration relatives à la gestion des comptes de l'Annexe G : Norme sur les configurations courantes des services de la TI intégrée [6] de la Directive sur les services et le numérique [7]

1.5.7 Protéger les comptes et les identités des utilisateurs. (Mesure de protection 1).

Gérer l’accès (Mesure de protection 2).

Référence : Version 2.0 des Mesures de protection du nuage du GC [8] de l’Annexe G : Norme sur les configurations courantes des services de la TI intégrée [6] de la Directive sur les services et le numérique [7]

2. Orientations pour la mise en œuvre

▶ Dans cette section

La section 2 décrit les orientations pour la mise en œuvre à l’intention des organisations du gouvernement du Canada afin qu’elles puissent respecter les exigences des instruments de politique indiquées à la section 1.

Pour des renseignements supplémentaires et l’interprétation de cette section, communiquez avec la Division de la cybersécurité du Secrétariat du Conseil du Trésor du Canada (SCT).

2.1 Appliquer l’authentification multifactorielle à tous les utilisateurs

Pour protéger les justificatifs d’identité et empêcher l’accès non autorisé aux services d’informatique en nuage, l’accès des utilisateurs doit être protégé par une authentification multifactorielle (AMF) solide, conformément aux Exigences de configuration relatives à la gestion des comptes [6] et aux documents d’orientation connexes. Dans la mesure du possible, des options d’AMF résistantes à l’hameçonnage doivent être utilisées.

2.2 Adopter des solutions d’authentification appropriées

La présente section décrit les considérations relatives aux solutions d’authentification en fonction du contexte opérationnel suivant, lequel comprend :

- des environnements hybrides où sont combinées des ressources sur site et déployées dans le nuage;
- des environnements où les ressources sont exclusivement déployées dans le nuage.

Le gouvernement du Canada étudie d'autres approches de modernisation de l'identité et les modèles connexes pour l'utilisation d'une architecture d'identité hybride. L'orientation sera mise à jour au fur et à mesure de l'évolution des travaux.

2.2.1 Pour les environnements où sont combinées des ressources sur site et déployées dans le nuage

Les organisations qui disposent de ressources sur site et déployées dans le nuage (modèle de déploiement hybride pour les données et les applications ministérielles) doivent utiliser l'authentification fédérée pour les utilisateurs non privilégiés [2].

Dans cette configuration, le processus d'authentification peut continuer de se dérouler sur site, ce qui permet à l'utilisateur de se connecter une seule fois pour accéder aux ressources sur place et déployées dans le nuage. L'authentification unique (ou simplifiée) est ainsi prise en charge, ce qui réduit la propagation des justificatifs d'identité et la réutilisation des mots de passe [3].

L'utilisation de l'authentification fédérée présente les avantages énumérés ci-dessous.

- Les politiques d'authentification ne sont pas transmises à l'externe.
- Le risque de compromettre dans le nuage les mots de passe sur site pendant le processus d'authentification de l'utilisateur est réduit au minimum, en particulier pour les organisations dont les données et services sur site sont jugés trop sensibles pour être migrés vers le nuage (voir l'annexe A-2 pour en savoir plus).
- Les opérations d'authentification sont gérées en un seul endroit, de sorte que chaque compte n'a besoin que d'un seul enregistrement, ce

qui facilite la gestion centralisée des politiques et la consignation des tentatives d'authentification.
- La fédération de l'authentification est basée sur des normes ouvertes et acceptées par l'industrie. Elle est donc indépendante de toute solution d'authentification propre (ou propriétaire) au FSIN Il n'y a aucune dépendance à l'égard d'un seul FSIN pour négocier l'accès à d'autres FSIN.

Les organisations sont censées utiliser des solutions, des biens et des services de TI intégrés ou partagés pour éviter les dédoublements, le cas échéant. À cette fin, elles peuvent utiliser les services intégrés qui prennent en charge l'authentification fédérée avec les FSIN offerts par Services partagés Canada (SPC). Il s'agit notamment des services de fédération Active Directory (AD FS) et GCPass dont la capacité sécurisée et évolutive d'authentification fédérée permet aux utilisateurs de s'authentifier pour accéder aux services d'informatique en nuage au moyen de leurs justificatifs d'identité du gouvernement du Canada.

Pour les organisations qui ne font pas partie de la portée des services de SPC et dont les ressources de TI sont limitées, une analyse des options et une évaluation des risques doivent être effectuées pour déterminer l'option d'authentification des utilisateurs la plus appropriée en fonction de leur contexte opérationnel, technique et de menace.

Se reporter à l'annexe A pour obtenir des considérations de sécurité supplémentaires liées à la protection des services de fédération.

2.2.2 Pour les environnements où les ressources sont exclusivement déployées dans le nuage

Bien qu'il y ait de nombreux avantages à traiter toute l'authentification de manière centralisée, certaines organisations qui ont déplacé toutes leurs données et applications ministérielles vers le nuage peuvent vouloir profiter des services d'identité basés sur le nuage pour l'authentification des

utilisateurs plutôt que de continuer à gérer leurs propres exigeantes d'infrastructure, en particulier pour les ministères qui ont des ressources informatiques limitées.

Les organisations doivent effectuer une analyse des options et une évaluation des risques pour déterminer la méthode d'authentification des utilisateurs la plus appropriée en fonction de leur contexte opérationnel, technique et de menace. L'évaluation doit inclure les considérations de sécurité, l'expérience utilisateur [4], les exigences d'infrastructure, la charge et le coût des opérations, la fiabilité et les répercussions en matière de reprise après sinistre, entre autres.

Bien que non exhaustives, les considérations suivantes auront une incidence sur la sélection de la méthode d'authentification la plus appropriée dans le nuage et doivent être incluses dans l'analyse susmentionnée.

- L'organisation qui exploite sa propre infrastructure de gestion des justificatifs d'identité peut bénéficier de la gestion des justificatifs d'identité à l'aide d'une plate-forme fournie par le FSIN, ce qui élimine le besoin de maintenir et d'exploiter une infrastructure distincte;
- L'organisation qui utilise plusieurs FSIN devra tenir compte du fait que chaque utilisateur peut avoir besoin de plusieurs justificatifs d'identité si des services de fédération ne sont pas utilisés. Pour éviter la propagation des justificatifs d'identité, les organisations doivent réduire au minimum le nombre de justificatifs d'identité nécessaires afin d'accéder aux services d'informatique en nuage. À l'inverse, l'organisation qui utilise un seul FSIN pour négocier l'accès à un autre FSIN devra envisager une dépendance et une résilience accrues pour tenir compte des défaillances du FSIN fournissant des services de courtage.
- Les fonctionnalités de récupération de mot de passe en libre-service prises en charge par le FSIN peuvent ne pas convenir et peuvent nécessiter d'être améliorées avant leur utilisation (voir la section 2.4

pour en savoir plus); l'organisation peut donc avoir besoin de gérer la récupération de mot de passe.
- L'incompatibilité de l'authentification principale en nuage avec les applications existantes peut nécessiter une instance ministérielle d'Active Directory (AD) sur place ou dans le nuage, même si toutes les autres données et applications sont hébergées dans le nuage.

Se reporter à l'annexe A pour des considérations de sécurité supplémentaires concernant l'authentification par synchronisation de mot de passe.

2.3 Assurer une protection adéquate des comptes administrateurs dans le nuage

Comme pour les comptes privilégiés sur site, la protection contre les accès non autorisés aux comptes privilégiés dans le nuage est essentielle et fait l'objet des configurations ci-dessous.

2.3.1 Prendre en charge l'accès privilégié aux services d'informatique en nuage grâce à des contrôles de sécurité appropriés, conformément au Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3) du Centre canadien pour la cybersécurité (CCC) [9].

2.3.2 Restreindre l'accès au personnel en fonction des principes du moindre privilège, du besoin de savoir et de la séparation des tâches.

2.3.3 Protéger l'accès aux comptes privilégiés (dans le nuage ou sur site) au moyen de solutions d'AMF solides; une AMF résistante à l'hameçonnage est fortement recommandée [5].

2.3.4 Utiliser, pour l'accès aux comptes privilégiés dans le nuage, des justificatifs d'identité qui diffèrent de ceux utilisés pour administrer les ressources sur site.

2.3.5 Réduire l'impact des attaques de justificatifs d'identité entre les environnements sur site et dans le nuage. À cette fin, s'assurer que les

utilisateurs, groupes et rôles administratifs très privilégiés dans le nuage (comme l'administrateur global et le compte racine) ne font pas partie de la portée de synchronisation à partir des environnements sur site et ne sont pas utilisés avec l'authentification unique fédérée, mais s'appuient plutôt sur l'authentification native en nuage [6]; cependant, il ne s'agit pas d'empêcher l'utilisation de la fédération pour les administrateurs moins privilégiés tels que les administrateurs d'applications ou de logiciels-services (SaaS), en particulier lorsque les avantages de la fédération l'emportent sur l'authentification native en nuage.

2.3.6 Désactiver les fonctionnalités de réinitialisation du mot de passe en libre-service dans le nuage pour les administrateurs du nuage.

2.3.7 Procéder, le cas échéant, à la configuration pour rendre les administrateurs « admissibles » à un rôle et demander l'activation du rôle de moindre privilège requis seulement au besoin et pour une période limitée.

2.3.8 Empêcher l'auto-approbation des demandes d'activation pour les rôles d'administrateurs très privilégiés dans le nuage (par exemple, compte racine, administrateur global) [7].

2.3.9 Appliquer, le cas échéant, un contrôle d'accès basé sur les attributs (ABAC) pour restreindre l'accès en fonction d'une combinaison de facteurs d'authentification (tels que l'AMF), d'appareils gérés, de la conformité des appareils, des risques liés à la connexion et à l'utilisateur et de l'emplacement.

2.3.10 Auditer, examiner et surveiller tous les accès et actions des utilisateurs privilégiés en fonction de la sensibilité de l'accès.

2.3.11 Mettre en œuvre les exigences applicables selon l'annexe G : Norme sur les configurations courantes des services de la TI intégrée de la Directive sur les services et le numérique [7].

2.4 Comprendre les répercussions de la réinitialisation du mot de passe en libre-service dans le nuage

Les méthodes de réinitialisation du mot de passe en libre-service donnent à l'utilisateur la possibilité de modifier ou de réinitialiser son mot de passe, sans l'intervention d'un administrateur ou d'un service de soutien. Si son compte est verrouillé ou s'il oublie son mot de passe, l'utilisateur peut suivre les instructions pour déverrouiller son compte et reprendre son travail.

Cette possibilité permet de réduire le nombre d'appels au service de soutien et la perte de productivité lorsque l'utilisateur ne peut pas se connecter à son appareil ou à une application. Cependant, la réinitialisation du mot de passe en libre-service dans le nuage doit être tout aussi sécurisée et robuste que les méthodes utilisées pour récupérer l'authentifiant principal.

À la section 2.3, il est recommandé de désactiver les fonctionnalités de réinitialisation du mot de passe en libre-service dans le nuage pour tous les administrateurs du nuage. Cette recommandation s'applique également aux comptes privilégiés, sur site ou dans le nuage. De plus, la réinitialisation du mot de passe en libre-service dans le nuage n'est pas recommandée pour les mots de passe sur site, même ceux des utilisateurs non privilégiés, car elle expose le gouvernement du Canada à un niveau de risque accru qui peut être évité grâce à la fédération.

Les solutions de rechange à la réinitialisation du mot de passe en libre-service dans le nuage passent par un ou plusieurs des éléments ci-dessous.

2.4.1 Continuer d'utiliser les méthodes de réinitialisation du mot de passe internes existantes.

2.4.2 Réinitialiser les mots de passe par vidéoconférence avec le personnel du service de soutien afin de pouvoir attester de l'identité de l'utilisateur (par exemple, au moyen d'une pièce d'identité valide délivrée par le gouvernement du Canada avec photo, comme une carte d'accès à un immeuble, par MS Teams ou un autre logiciel de

vidéoconférence, de préférence en utilisant un appareil géré par le gouvernement du Canada si possible).

2.4.3 Respecter l'Orientation sur les mots de passe [10] du gouvernement du Canada, qui inclut des recommandations pour faciliter la mémorisation des mots de passe et éliminer leur expiration (seuls les mots de passe qui ont été compromis ou qui sont soupçonnés d'avoir été compromis sont modifiés).

Pour en savoir plus sur la réinitialisation du mot de passe en libre-service d'Azure AD, se reporter au document de discussion sur les Considérations relatives à l'utilisation de la réinitialisation de mot de passe en libre-service de Microsoft Azure AD au sein du gouvernement du Canada (disponible en anglais sur demande en envoyant un courriel à TBS-Cyber Security/SCT-Cybersécurité ZZTBSCYBERS@tbs-sct.gc.ca).

2.5 Surveiller les événements d'authentification pour détecter les menaces pour la sécurité

La surveillance de la sécurité, les alertes et les rapports basés sur l'apprentissage automatique qui révèlent des modes d'accès incohérents permettent de cerner les risques pour la sécurité. Un système de surveillance active de l'identité peut rapidement détecter un comportement suspect et déclencher une alerte pour une enquête approfondie. Voici les événements à surveiller :

2.5.1 modes d'accès inhabituels;

2.5.2 attaques par force brute d'un compte particulier;

2.5.3 tentatives de connexion à partir de plusieurs emplacements;

2.5.4 connexions à partir d'appareils infectés;

2.5.5 adresses IP suspectes;

2.5.6 utilisation de protocoles d'authentification faibles ou anciens;

2.5.7 forme particulière de déplacements latéraux;

2.5.8 élévation des privilèges;

2.5.9 techniques de persistance.

Faute de savoir si des activités suspectes sont commises au moyen de justificatifs d'identité, il sera difficile d'atténuer ce type de menace. Le Guide sur la consignation d'événements [11] du gouvernement du Canada fournit des conseils supplémentaires sur les événements à configurer pour contribuer aux opérations de sécurité et à la surveillance.

3. Références

1. Secrétariat du Conseil du Trésor du Canada, « Politique sur la sécurité du gouvernement »
2. Secrétariat du Conseil du Trésor du Canada, « Directive sur la gestion de la sécurité ministérielle »
3. Secrétariat du Conseil du Trésor du Canada, « Directive sur la gestion de l'identité »
4. Secrétariat du Conseil du Trésor du Canada, « Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage », novembre 2017
5. Secrétariat du Conseil du Trésor du Canada, « Politique sur les services et le numérique »
6. Secrétariat du Conseil du Trésor du Canada, « Annexe G : Norme sur les configurations courantes des services de la TI intégrée - Exigences de configuration relatives à la gestion des comptes »
7. Secrétariat du Conseil du Trésor du Canada, « Directive sur les services et le numérique »
8. Secrétariat du Conseil du Trésor du Canada, « Mesures de protection du nuage du GC »
9. Centre canadien pour la cybersécurité, « Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3) »

10. Secrétariat du Conseil du Trésor du Canada, « Orientation sur les mots de passe »
11. Secrétariat du Conseil du Trésor du Canada, « Guide sur la consignation d'événements »
12. Microsoft, « Implémenter la synchronisation de hachage de mot de passe avec la synchronisation Microsoft Entra Connect »
13. Centre canadien pour la cybersécurité, « Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B - ITSP.40.111 »
14. Microsoft, « Synchronisation de hachage de mot de passe et FIPS »
15. National Security Agency, « Detecting Federated Authentication Abuse » (document en anglais seulement)
16. Secrétariat du Conseil du Trésor du Canada, « Cadre de référence pour la Gestion de l'identité et des justificatifs en matière d'accès du gouvernement du Canada (GIJA du GC) »
17. National Institute of Standards and Technology, « Digital Identity Guidelines (SP800-63-3) » (document en anglais seulement)

Annexe A – Considérations de sécurité supplémentaires

▶ Dans cette section

A-1 Services de fédération

Quel que soit l'environnement, la fédération dépend de la fiabilité des composants utilisés pour authentifier les utilisateurs et signer numériquement les messages (SAML ou OpenID Connect) de protocole connexe. Si ces composants sont compromis, ils peuvent être exploités pour obtenir un accès non autorisé aux ressources. Il est donc essentiel de configurer correctement tous les composants et services de fédération pour un fonctionnement sécurisé. Pour ce faire, il faut au minimum :

A-1.1 configurer les composants et services de fédération conformément aux orientations en vigueur (fournies par le fournisseur ou autrement [8]);

A-1.2 surveiller en permanence les activités anormales sur site et dans le nuage;

A-1.3 stocker les clés privées utilisées pour signer numériquement les assertions et revendications de SAML et d'OpenID Connect dans un module de sécurité matérielle validé FIPS 140- 2 ou FIPS 140- 3 de niveau 2 (avec sécurité physique de niveau 3) ou supérieur [9];

A-1.4 traiter les composants de la fédération comme des biens essentiels et adhérer aux pratiques exemplaires de l'accès sécurisé aux privilèges.

L'exploitation des services d'identité sur place pourrait conduire à un accès non autorisé aux environnements dans le nuage. Par conséquent, il est recommandé d'exclure de la fédération les comptes très privilégiés du service d'identité dans le nuage et les applications publiques des logiciels-services axées sur l'informatique en nuage pour les conserver en tant que comptes « exclusivement dans le nuage » afin de limiter les déplacements latéraux d'un environnement sur place compromis vers le nuage et d'en réduire l'impact.

À la section 2.2.1 du présent document, les organisations sont encouragées à utiliser les services de fédération intégrés existants du gouvernement du Canada. Toutefois, en des circonstances exceptionnelles, elles peuvent choisir de déployer une solution de fédération sur mesure pour répondre à certaines exigences opérationnelles ou ministérielles qui peuvent ne pas être disponibles dans les solutions intégrées. Dans ce scénario, les organisations doivent s'assurer que la solution d'authentification :

A-1.5 offre une expérience utilisateur positive;

A-1.6 est conforme aux exigences de sécurité applicables, y compris celles indiquées dans la présente section;

A-1.7 est conforme aux pratiques exemplaires de l'industrie;

utilise les capacités d'authentification existantes dans la mesure du possible pour réduire au minimum la multiplication de solutions sur mesure;

A-1.8 est conforme aux exigences des politiques et directives pertinentes du gouvernement du Canada, y compris les exigences indiquées dans le présent document.

Les organisations doivent communiquer avec la Division de la cybersécurité du SCT avant d'utiliser une solution d'authentification sur mesure axée sur l'informatique en nuage.

A-2 Authentification par synchronisation du mot de passe

L'authentification par synchronisation du mot de passe, telle que la fonctionnalité de synchronisation par hachage de mot de passe de Microsoft prise en charge par Active Directory (AD) de Microsoft Azure [12], est une autre option de configuration pour l'authentification.

Pour les organisations qui entrent dans la catégorie mentionnée à la section 2.2.2 du présent document, les éléments ci-dessous décrivent des considérations supplémentaires lors de l'utilisation de l'authentification par synchronisation du mot de passe.

A-2.1 Utiliser des mécanismes de hachage et de cryptage lors de la synchronisation des mots de passe, ce qui est primordial pour préserver la confidentialité et l'intégrité des justificatifs d'identification des comptes, conformément au document d'orientation Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B - ITSP.40.111 [13] du Centre canadien pour la cybersécurité.

A-2.2 S’assurer que l’AMF est appliquée à tous les utilisateurs avant d’activer la synchronisation des mots de passe.

A-2.3 Exclure la synchronisation des comptes qui ne doivent pas nécessairement être utilisés dans le nuage, y compris les comptes de service utilisés sur site ou sur des serveurs basés sur l’infrastructure-service (IaaS), ou les comptes administratifs très sensibles utilisés pour administrer des serveurs sur site ou des serveurs basés sur l’IaaS (tels que les comptes des administrateurs de domaine et des administrateurs globaux, et les comptes racines et tout compte d’accès équivalent à celui de l’administrateur de domaine).

A-2.4 S’assurer que la réinitialisation de mot de passe en libre-service et la réécriture du mot de passe sont désactivées (voir les directives à la section 2.4 du présent document).

A-2.5 Prendre des mesures pour synchroniser les comptes AD sur site expirés avec Azure AD. L’attribut d’expiration du compte des comptes Windows AD n’est pas synchronisé avec Azure AD. Par conséquent, un compte AD sur site expiré configuré pour l’authentification par synchronisation du mot de passe sera toujours actif dans Azure AD. Si la fonctionnalité d’expiration du compte est utilisée, il est recommandé aux organisations de mettre en œuvre un flux de travail du bureau de service ou un processus automatisé pour désactiver également le compte Azure AD de l’utilisateur (utiliser l’applet de commande Set-AzureADUser).

A-2.6 Utiliser le paramètre de mot de passe par défaut « ne jamais expirer »; cette mesure est conforme à l’Orientation sur les mots de passe du gouvernement du Canada [10] et ne doit pas être remplacée.

A-2.7 S’assurer que MD5 est activé conformément à la documentation Microsoft applicable [10][14].

De plus, les organisations qui utilisent les services AD FS pour se fédérer avec Microsoft Azure AD doivent savoir que l'authentification par synchronisation du mot de passe peut être activée pour prendre en charge certaines fonctionnalités de sécurité telles que la détection des fuites de justificatifs d'identité. L'utilisation de l'authentification par synchronisation du mot de passe à cette fin n'est pas exclue dans la présente Ligne directrice. En d'autres termes, il est possible de mettre en œuvre l'authentification fédérée au moyen des services AD FS et de permettre que l'authentification par synchronisation du mot de passe prenne en charge la détection des fuites de justificatifs d'identité (mais pas pour l'authentification des utilisateurs).

De plus, à des fins de résilience, les organisations qui exploitent leur propre infrastructure des services AD FS peuvent envisager d'utiliser l'authentification par synchronisation du mot de passe comme sauvegarde pour leur méthode d'authentification principale (fédération). Cependant, comme il est indiqué à la section 2.2.1 du présent document, l'avantage d'utiliser l'authentification fédérée pour les environnements hybrides est de réduire au minimum le risque d'exposition des informations d'identification sur site dans le nuage pendant le processus d'authentification de l'utilisateur.

Les organisations doivent, en fonction de leur contexte opérationnel, technique et de menace, effectuer une analyse des options et une évaluation des risques qui prennent en compte les compromis entre sécurité et disponibilité. Si une organisation choisit d'utiliser l'authentification par synchronisation de mot de passe comme sauvegarde, les utilisateurs qui se sont connectés directement à Azure AD devront réinitialiser leurs mots de passe, une fois que les composants de l'infrastructure des services AD FS auront été rétablis.

1 Conformément au Cadre de référence pour la Gestion de l'identité et des justificatifs en matière d'accès du gouvernement du Canada (GIJA du GC) [16] et aux Digital Identity Guidelines NIST SP800-63-3[17] (document en anglais seulement).

2 Voir la section 2.3 pour des conseils supplémentaires concernant les utilisateurs privilégiés.

3 Les principaux FSIN tels qu'Amazon Web Services (AWS), Google Cloud Platform (GCP) et Microsoft Azure prennent en charge la fédération au moyen des services de fédération Active Directory, de sorte que la même infrastructure peut être utilisée pour prendre en charge l'authentification des utilisateurs auprès de plusieurs FSIN.

4 Par exemple, réduire au minimum le nombre de justificatifs d'identité nécessaires pour accéder aux services d'informatique en nuage.

5 Les justificatifs d'identité utilisés pour accéder aux comptes d'accès d'urgence (parfois appelés comptes « de secours ») peuvent être basés uniquement sur un identifiant utilisateur ou un mot de passe très solide et strictement contrôlé. Il est fortement recommandé d'utiliser un contrôle par deux personnes pour empêcher l'accès non autorisé à ces comptes spéciaux.

6 Consulter le bulletin Detecting Abuse of Authentication Mechanisms [15] de la National Security Agency (NSA) pour obtenir de plus amples renseignements et des justifications.

7 Par exemple, l'approbation du gestionnaire peut être requise pour les rôles très privilégiés.

8 Des orientations précises relatives à la fédération avec Azure AD sont fournies dans le bulletin Detecting Abuse of Authentication Mechanisms [15] de la National Security Agency (NSA).

9 Consulter le bulletin Detecting Abuse of Authentication Mechanisms [15] de la NSA pour obtenir de plus amples renseignements et des justifications.

10 Il ne s’agit pas ici de valider MD5 ni de remettre en question les directives du gouvernement du Canada sur la cryptographie. MD5 est tout simplement une fonction de mise en œuvre de Microsoft.

Date de modification :
2024-12-02