Microsoft logo white text versionMicrosoft logo white text versionMise en œuvre Pro Santé Connect avec Microsoft Entra ID

Zzz

Zzz

Guide de configuration de l’accès conditionnel à destination des établissements de santé

Version 0.3 - Février 2024

Cette page est intentionnellement laissée vide.

Avertissement

Les informations contenues dans le présent document, y compris les URL et autres références à des sites Internet, sont susceptibles d'être modifiées sans préavis. Sauf indication contraire, les exemples de sociétés, d'organisations, de produits, de noms de domaine, d'adresses électroniques, de logos, de personnes, de lieux et d'événements décrits dans le présent document sont fictifs et aucune association avec une société, une organisation, un produit, un nom de domaine, une adresse électronique, un logo, une personne, un lieu ou un événement réel n'est voulue ou ne doit être déduite. Il incombe à l'utilisateur de se conformer à toutes les lois applicables en matière de droits d'auteur.

A drawing of a face

Description automatically generated

Attribution 4.0 International (CC BY 4.0)

Microsoft et tous les contributeurs vous accordent une licence pour ce document sous la licence [Creative Commons Attribution 4.0 International Public License](https://creativecommons.org/licenses/by/4.0/legalcode), Cf. fichier [LICENSE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE), et vous accordent une licence pour tout code dans le référentiel sous la licence MIT, Cf. fichier [LICENSE-CODE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE).

Microsoft, Windows, Microsoft Azure et/ou d'autres produits et services Microsoft référencés dans le document peuvent être des marques commerciales ou des marques déposées de Microsoft aux États-Unis et/ou dans d'autres pays. La licence de ce document ne vous donne pas le droit d'utiliser les noms, logos ou marques de Microsoft. Les directives générales de Microsoft en matière de marques sont disponibles à l'adresse suivante : <http://go.microsoft.com/fwlink/?LinkID=254653>.

Des informations sur la protection de la vie privée sont disponibles à l'adresse suivante : <https://privacy.microsoft.com/fr-fr/>

Microsoft et tous les contributeurs se réservent tous les autres droits, que ce soit au titre de leurs droits d'auteur, de leurs brevets ou de leurs marques respectives, que ce soit de manière implicite, par préclusion ou de toute autre manière.

Contenu

[1 Introduction 5](#_Toc158807915)

[1.1 Présentation succincte de Pro Santé Connect (PSC) 5](#_Toc158807916)

[1.2 Objectif du guide 5](#_Toc158807917)

[1.3 Non-objectifs du guide 5](#_Toc158807918)

[2 Configuration des stratégies d’accès conditionnel Microsoft Entra ID 7](#_Toc158807919)

[2.1 Prérequis pour les stratégies d’accès conditionnel 7](#_Toc158807920)

[2.2 Définition d’une stratégie d’accès conditionnel 8](#_Toc158807921)

[3 Gestion des journaux Microsoft Entra ID 12](#_Toc158807922)

[3.1 Comprendre les journaux 12](#_Toc158807923)

[3.2 Rôles pour accéder aux journaux 12](#_Toc158807924)

[3.3 Durée de rétention des journaux 12](#_Toc158807925)

[3.4 Exporter et sauvegarder les journaux 13](#_Toc158807926)

[3.5 Surveillance des activités 13](#_Toc158807927)

[3.6 Aller plus loin avec les classeurs 13](#_Toc158807928)

# Introduction

## Présentation succincte de Pro Santé Connect (PSC)

Pro Santé Connect (PSC) est le fédérateur d’identités des professionnels des secteurs sanitaire, médico-social et social enregistrés au Répertoire Partagé des Professionnels de Santé (RPPS). Ce service socle est proposé par l’Agence du Numérique en Santé (ANS) en sa qualité d’autorité compétente.

Il leur offre une manière simple, sécurisée et unifiée de se connecter à tous leurs services numériques en santé, en pouvant passer de l’un à l’autre de manière particulièrement fluide.

Dans le cadre de cette expérimentation, le fédérateur d’identités PSC permet la délégation de l’authentification auprès de fournisseurs d’identités (FI) tiers. Pour plus d’informations, nous invitons le lectorat à consulter le guide « Mise en œuvre Pro Santé Connect - Guide d’intégration de PSC pour le mode sans couture à destination des établissements de santé » disponible sur le site de l’ANS : TBD.

Une telle mise en œuvre et les capacités nouvelles ainsi proposées constituent un premier niveau de livrable du projet Pro Santé Connect sans couture. Pour plus d’informations, nous invitons le lectorat à consulter la page suivante sur le site de l’ANS : TBD.

## Objectif du guide

L’objectif de ce guide est d’expliciter la mise en œuvre des politiques d’accès conditionnel attendues suite à la configuration :

1. D’un ou plusieurs moyens d’identification électroniques (MIE) conformes avec les exigences établies par l’ANS.
2. D’une délégation de l’authentification Pro Santé Connect (PSC) auprès du fournisseur d’identités (FI) tiers Microsoft Entra ID (anciennement connu sous le nom d’Azure AD).

L’accès conditionnel permet d’assurer dans le cadre de PSC sans couture le respect d’un ensemble d’exigences comme la force d’authentification requise pour accéder à PSC et la durée d’activité d’une session autorisée sur PSC.

Ces deux volets de la mise en œuvre constituent un prérequis au présent document.

## Non-objectifs du guide

La délégation de l’authentification PSC auprès du fournisseur d’identités (FI) tiers Microsoft Entra ID est couverte dans le Guide d’intégration de Pro Santé Connect à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

De même, les MIE conformes sont couverts dans le Guide de configuration des MIE et de la navigation sans couture à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

Microsoft Entra ID propose par ailleurs des mécanismes permettant une navigation sans couture dès l’ouverture de session sur un appareil Windows pour l’accès à une application ou un service numérique déléguant l’authentification à PSC. Si les prérequis pour la mise en place de ces éléments pour cette navigation sans couture ne font pas partie du cadre minimum défini par l’ANS, ceux-ci sont néanmoins couverts dans ce même guide. Nous invitons le lectorat à s’y reporter le cas échéant.

Enfin, la mise en œuvre des MIE conformes avec les exigences établies par l’ANS ainsi que cette expérience navigation sans couture peuvent être étendues à d’autres types de dispositifs comme les services de terminaux Windows. Ceci requiert la mise en œuvre additionnelle de Microsoft Entra Private Access, un produit de type ZTNA (Zero Trust Network Access) centré sur l'identité. Cette dernière est couverte dans le Guide de configuration de Microsoft Entra Private Access à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

# Configuration des stratégies d’accès conditionnel Microsoft Entra ID

Dans le cadre du respect des exigences quant à la force d’authentification requise pour bénéficier de l’authentification sans couture, Microsoft met à disposition un mécanisme appelé Accès conditionnel.

L’accès conditionnel dans Microsoft Entra ID est un moteur de stratégie intelligent qui aide les organisations à mieux contrôler les modalités d’accès des utilisateurs aux ressources d’une entreprise en :

* Appliquant des contrôles d’accès avec des stratégies adaptatives. Il s’agit de regrouper divers signaux en temps réel (contexte d’utilisateur, appareil, emplacement et niveau de risque de la session) afin de déterminer quand il convient d’autoriser l’accès, le bloquer ou le limiter, ou d’exiger des étapes de vérification supplémentaire ;
* Protégeant les données dans les applications et les services numériques. Il s’agit de surveiller et de contrôler les sessions, l’accès aux applications, aux services numériques et les données sensibles dans l’ensemble de l’organisation en temps réel sur la base du comportement des utilisateurs dans les applications et les services numériques, en local et dans le cloud ;
* Limitant l’accès des appareils vulnérables ou compromis. Il s’agit d’utiliser des stratégies d’accès conditionnel pour vérifier l’intégrité et la posture de sécurité des appareils inscrits et réserver l’accès aux ressources de votre entreprise aux seuls appareils intègres et approuvés. Les appareils Windows 10 ou ultérieur avec une jointure (hybride) à Microsoft Entra peuvent ainsi voir leur posture de sécurité vérifier.

Les fonctionnalités d’accès conditionnel sont disponibles avec les abonnements Microsoft Entra ID P2.

## Prérequis pour les stratégies d’accès conditionnel

### Eléments de configuration

Comme indiqué en introduction, i) la délégation de l’authentification Pro Santé Connect (PSC) auprès de Microsoft Entra ID ainsi que ii) le déploiement et à la configuration d’un ou plusieurs moyens d’identification électroniques (MIE) conformes avec les exigences établies par l’ANS, constituent des prérequis pour le présent guide.

### Licences Entra ID

Le locataire de l’ES doit disposer de la licence Microsoft Entra ID P1 pour utiliser l'accès conditionnel et la fonctionnalité force d’authentification.

### Privilèges d’administration

Par ailleurs, en termes de privilèges nécessaires pour procéder à la configuration, les administrateurs interagissant avec l’accès conditionnel doivent avoir une ou plusieurs des attributions de rôles suivantes en fonction des tâches qu’ils effectuent. Pour suivre le principe du moindre privilège de la Confiance Zéro (Zero Trust), nous recommandons d’utiliser Microsoft Entra Privileged Identity Management (PIM) pour activer juste-à-temps les attributions de rôles privilégiés.

* Lire les stratégies et configurations d’accès conditionnel
  + Lecteur de sécurité (security reader) ;
  + Lecteur général (global reader).
* Créer ou modifier des stratégies d’accès conditionnel
  + Administrateur de l’accès conditionnel (conditional access administrator) ;
  + Administrateur de la sécurité (security administrator).

## Définition d’une stratégie d’accès conditionnel

Une stratégie d’accès conditionnel permet de gérer les contrôles de sécurité à l’aide de conditions sur mesure permettant de bloquer l’accès, d’exiger l’authentification multifacteur (MFA) ou d’autoriser l’accès d’un utilisateur uniquement lorsque celui-ci est nécessaire. Il s’agit ici en l’état d’imposer une authentification multifacteur (MFA).

Documentation Microsoft :

* Planifier un déploiement d’accès conditionnel: <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/plan-conditional-access> ;
* Microsoft Entra Privileged Identity Management (PIM) : <https://learn.microsoft.com/fr-fr/entra/id-governance/privileged-identity-management/pim-configure> ;
* Rôles intégrés Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference> ;

### Exigence de l’authentification multifacteur (MFA)

Pour définir une stratégie d’accès conditionnel, procéder comme suit :

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Aller sur Applications > Applications d’entreprise et cliquer sur l’application PSC.
3. Dans Sécurité > Accès conditionnel, cliquer sur Nouvelle stratégie.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

1. Afin de d’imposer le MFA pour accéder à l’application :
   1. Sous Utilisateurs, indiquer Tous les utilisateurs.
   2. Sous Octroyer, Accorder l’accès, sélectionner Exiger une authentification multifacteur.
   3. Activer la stratégie..

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Alternative : Au lieu d’exiger l’authentification mutificateur, il est possible d’exiger la force de l’authentification grâce à 3 méthodes prédéfinies. Il est également possible de configurer plus finement la force d’authentification.

### Exigence d’une force d’authentification donnée

La force d'authentification est un contrôle d'accès conditionnel qui permet aux administrateurs de spécifier quelle combinaison de méthodes d'authentification peut être utilisée pour accéder à une ressource. Cela peut varier en fonction du niveau de sensibilité de la ressource et du risque d'utilisateur, de l'emplacement, etc.

Pour spécifier une force d'authentification afin d'accéder à une ressource ou à une application, les administrateurs doivent créer une stratégie d'accès conditionnel avec le contrôle Exiger une force d'authentification.

Ils peuvent choisir parmi trois forces d'authentification intégrées ou créer une force d'authentification personnalisée.

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter.
3. Aller sur Protection > Méthodes d’authentifications > Points forts d’authentification. 3 forces d’authentification sont configurées par défaut :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Afin de créer des forces d’authentification personnalisées :

1. Cliquer sur Nouvelle force d’authentification.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

1. Préciser un nom descriptif pour la nouvelle force d’authentification.
2. Fournir une description si souhaité.
3. Sélectionne comme l’une des méthodes disponibles autorisée MFA anti-hameçonnage > Authentification basée sur un certificat (multifacteur). Cette force peut être étendue le cas échéant aux méthodes Windows Hello Entreprise et Clé de sécurité FIDO2. La prise en charge des moyens d’identification électronique (MIE) PSC conforme est décrite dans le Guide de configuration de l’authentification unique à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.
4. Cliquer Suivant et passez en revue la configuration de la stratégie.

Une fois la force d'authentification déterminée, une stratégie d'accès conditionnel doit être créer pour exiger cette force d'authentification lors de l’accès à une ressource.

Remarque : Les stratégies d'accès conditionnel sont uniquement évaluées après l'authentification initiale. Par conséquent, la force d'authentification ne restreint pas l'authentification initiale d'un utilisateur.

Documentation Microsoft :

* Force d’authentification de l’accès conditionnel : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-authentication-strengths>.

### Stratégie d’accès conditionnel et authentification périodique

La fréquence de connexion, aussi connu sous le nom de réauthentification périodique, des utilisateurs définit la période avant qu'un utilisateur ne soit invité à se reconnecter lorsqu'il tente d'accéder à une ressource. Par défaut, Microsoft Entra ID demande une réauthentification tous les 90 jours. Cependant, cette fréquence peut être ajustée pour répondre aux besoins spécifiques de votre organisation. Les administrateurs peuvent sélectionner une période de temps ou choisir de demander une réauthentification à chaque fois.

Prérequis :

Pour bénéficier la fonctionnalité réauthentification périodique, l’ES doit :

* Posséder des licences Microsoft Entra ID P1 ou P2 ;
* Avoir mis en place une stratégie d'accès conditionnel nécessitant une authentification multifacteur.

Créer une fréquence de connexion personnalisée :

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter.
3. Aller surProtection > Accès Conditionnel.
4. Cliquer sur Créer une nouvelle stratégie.
5. Préciser un nom pour la stratégie. Il est recommandé de définir une convention de nommage significative pour les noms des stratégies.
6. Choisir toutes les conditions requises pour l'environnement cible, y compris l’application PSC et d’autres ressources cibles.
7. Sous Contrôles d'accès > Session, sélectionner la fréquence de connexion. Choisir la réauthentification périodique et entrer une valeur en heures – Le maximum est de 4 heures pour PSC.
8. Sauvegarder la stratégie.

Documentation Microsoft :

* Configurer la gestion de session d’authentification avec l’accès conditionnel :  
  <https://learn.microsoft.com/fr-fr/entra/identity/conditional-access/howto-conditional-access-session-lifetime#user-sign-in-frequency>

### Autres stratégies

Des stratégies additionnelles sont susceptibles de s’ajouter à l’exigence précédente à l’avenir.

# Gestion des journaux Microsoft Entra ID

Ce chapitre vous aidera à comprendre comment utiliser et gérer les journaux Microsoft Entra ID.

## Comprendre les journaux

 Le suivi et l'audit des activités et événements de votre annuaire est essentiel pour détecter les menaces, identifier les anomalies, résoudre les problèmes et répondre tout simplement aux demandes d'audit.   
Microsoft Entra ID fournit deux types de journaux d'activité : les journaux de connexion et les journaux d'audit.

1. Journaux de connexion : ces journaux contiennent des informations sur les tentatives de connexion réussies et échouées des utilisateurs et des applications à votre annuaire Entra ID ;
2. Journaux d’audit : ces journaux contiennent des informations sur les opérations effectuées dans votre annuaire Entra ID, telles que la création, la modification ou la suppression d'utilisateurs, de groupes, d'applications ou de règles.

## Rôles pour accéder aux journaux

Pour accéder aux journaux d’activité, il est nécessaire de disposer d'un rôle approprié.

Les rôles Microsoft Entra ID permettent de définir des niveaux d'accès appropriés pour les utilisateurs et les groupes d’utilisateurs. Ces rôles comprennent notamment l'administrateur global, le lecteur global, l'administrateur de sécurité et l'administrateur du support utilisateur.

Il existe différents types de rôles qui donnent des niveaux de permissions variables:

* Le rôle Administrateur global vous donne le niveau de permission le plus élevé. Vous pouvez accéder à tous les journaux de connexion et d'audit, ainsi qu'à toutes les autres fonctionnalités de Microsoft Entra ID ;
* Le rôle Lecteur global vous donne le niveau de permission le plus bas. Vous pouvez accéder aux journaux de connexion et d'audit en lecture seule, mais vous ne pouvez pas effectuer d'autres opérations dans Microsoft Entra ID ;
* Le rôle Administrateur de sécuritévous donne un niveau de permission intermédiaire. Vous pouvez accéder aux journaux de connexion et d'audit en lecture-écriture, ainsi qu'à certaines fonctionnalités liées à la sécurité, telles que la gestion des alertes, des rapports et des stratégies ;
* Le rôle Administrateur du support utilisateurvous donne un niveau de permission similaire à celui de l'administrateur de sécurité, mais limité aux utilisateurs dont vous êtes le responsable hiérarchique. Vous pouvez accéder aux journaux de connexion et d'audit en lecture-écriture pour ces utilisateurs, ainsi qu'à certaines fonctionnalités liées au support utilisateur, telles que la réinitialisation des mots de passe ou la gestion des appareils ;

## Durée de rétention des journaux

Les journaux d'activité sont conservés pendant une durée limitée dans le centre d’administration de Microsoft Entra. La durée de rétention dépend du type de journal et du niveau de licence Microsoft Entra ID dont dispose l’ES.

Les journaux de connexion sont conservés pendant 7 jours pour les licences gratuites, 30 jours pour les licences Microsoft Entra ID P1 et P2. Les journaux d'audit sont conservés pendant 7 jours pour les licences gratuites et 30 jours pour les licences Microsoft Entra ID P1 et P2. Pour une conservation plus longue, il est possible d’exporter et de sauvegarder les journaux.

## Exporter et sauvegarder les journaux

Pour conserver les journaux d'activité au-delà de la durée de rétention du portail Azure, il est nécessaire de les exporter vers un autre emplacement.

Il est possible :

* D’afficher les journaux d’activité et les rapports dans le Portail Azure ;
* D’accéder aux journaux d’activité via l’API Microsoft Graph ;
* De diffuser en continu les journaux d’activité vers un Event Hub ;
* D’intégrer les journaux d’activité aux journaux d’activité Azure Monitor ;
* De superviser l’activité en temps réel avec Microsoft Sentinel.

S’assurer que les procédures de sauvegarde sont bien documentées.

Consulter les ressources suivantes pour en savoir plus sur la récupération des journaux d'activité.

Documentation Microsoft :

* Comment accéder aux journaux d'activité dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/monitoring-health/howto-access-activity-logs>.

## Surveillance des activités

Pour identifier la compromission potentielle d'une application, ici en particulier l’application PSC, il est essentiel de surveiller les événements suivants :

1. Modifications en dehors des horaires normaux ;
2. Modifications des identifiants d'application ;
3. Modifications des autorisations des applications ;
4. Attribution de principaux services à des rôles Microsoft Entra ID ou à des rôles de contrôle d'accès basé sur les rôles Azure (RBAC) ;
5. Autorisations très privilégiées accordées aux applications – en particulier celles relatives à l’application PSC - ;
6. Modifications sur Azure Key Vault (si applicable) ;
7. Consentement de l'utilisateur final pour les applications ;
8. Modifications de la configuration de l'application, y compris les modifications d'URI.

## Aller plus loin avec les classeurs

À l’aide des paramètres de diagnostic dans Microsoft Entra ID, il est possible d’intégrer les journaux à Azure Monitor afin que l’activité de connexion et la piste d’audit des modifications au sein du locataire de l’ES puissent être analysées avec d’autres données Azure.

Ainsi, les classeur d’Azure Log Analytics permettent de surveiller les activités de consentement et de permissions dans Microsoft Entra ID. Le classeur « Consent Insights » offre une vue des applications en fonction du nombre de demandes de consentement échouées.

Prérequis :

* Un locataire Microsoft Entra ID P1 ou P2 ;
* Un abonnement Azure. Si besoin, un essai gratuit peut être demandé : <https://azure.microsoft.com/free/>.
* Un espace de travail Log Analytics dans un abonnement Azure. Se référer à Créer un espace de travail Log Analytics : <https://learn.microsoft.com/fr-fr/azure/azure-monitor/logs/quick-create-workspace?tabs=azure-portal> ;
* Autorisations d’accès aux données dans l’espace de travail Log Analytics. Se référer à Gestion de l’accès des espaces Log Analytics : <https://learn.microsoft.com/fr-fr/azure/azure-monitor/logs/manage-access?tabs=portal>.

### Accès aux classeur de Log Analytics

Pour accéder aux classeurs

1. Depuis un navigateur, aller sur la vue d’ensemble Identité du Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView>.
2. Se connecter.
3. Aller à Surveillance et intégrité > Classeurs.
4. Chercher le rapport "Sensitive Operations Report".

### Types de classeurs à considérer

 Les classeurs les plus importants sont :

* Rapport sur les modifications des méthodes d'authentification des applications et des principaux de services :
  + Surveille les nouvelles informations d'identification ajoutées, les modifications d'informations d'identification, etc.
  + Contexte : les attaquants cherchent à établir une persistance dans votre environnement en créant des accès malveillants sur des applications et des principaux de services existants. Ils utilisent ensuite ces informations d'identification pour s'authentifier en tant qu'application cible ou principal de service, leur accordant ainsi l'accès à toutes les ressources pour lesquelles ils disposent de permissions.

Eléments importants à surveiller :

* + - Toutes les nouvelles informations d'identification ajoutées aux applications et principaux de services, y compris le type d'informations d'identification ;
    - Principaux acteurs et nombre de modifications d'informations d'identification qu'ils ont effectuées ;
    - Chronologie de toutes les modifications d'informations d'identification.
* Rapport sur les nouvelles autorisations accordées aux principaux de services :
  + Liste les autorisations accordées et enquête sur toute autorisation excessive.
  + Contexte : les attaquants cherchent à obtenir un principal de service ou une application disposant d'un ensemble d'autorisations à haut privilège pour accéder à votre environnement. S'ils n'y parviennent pas, ils essaient d'ajouter des autorisations à d'autres principaux de service ou applications pour obtenir cet accès.

Eléments importants à surveiller :

* + - Liste des autorisations accordées aux principaux de services existants ;
    - Enquêter sur toute autorisation excessive accordée à des services tels que Microsoft Graph, etc.
* Rapport sur les mises à jour des rôles et des membres de groupe :
  + Surveille les modifications apportées aux adhésions, les additions aux rôles et groupes à haut privilège, etc.
  + Contexte : parfois, Les attaquants ne peuvent pas ou ne veulent pas ajouter de nouvelles autorisations aux principaux de services ou aux applications existantes. Dans ce cas, ils ajoutent de nouvelles autorisations aux rôles ou aux groupes de répertoire existants.

Eléments importants à surveiller :

* + - Liste de toutes les modifications apportées aux adhésions des principaux de services ;
    - Liste de toutes les additions aux rôles et aux groupes à haut privilège ;
    - Surveillance des principaux de services en tant que membres de rôles de répertoire (rôles d'administration) ou de groupes.

Ceci conclut le présent guide.