Document/Cours - Bonnes pratiques en matière de mot de passe

Politique de mot de passe : comment appliquer les bonnes pratiques de l'ANSSI ?

Source : https://www.it-connect.fr/politique-de-mot-de-passe-comment-appliquer-les-bonnes-pratiques-de-lanssi/

24/11/2021 Florian Burnel Aucun commentaire Active Directory, anssi, Mots de passe, Sécurité

Sommaire [-]

I. Présentation

Dans cet article, je vais vous parler des bonnes pratiques de l'ANSSI en matière de politique de mot de passe, et nous verrons quelles sont les solutions techniques envisageables pour appliquer ces recommandations dans un environnement Active Directory.
Pour rédiger cet article, je me suis appuyé sur le guide publié par l'ANSSI le **08 octobre 2021** et qui s'appelle "*Recommandations relatives à l'authentification multifacteur et aux mots de passe - v2.0*".
Vous pouvez le télécharger à l'adresse suivante : ANSSI - Télécharger le guide

II. Les bonnes pratiques de l'ANSSI sur les mots de passe

Avant de rentrer dans la technique, je souhaitais vous proposer **une synthèse des bonnes pratiques de l'ANSSI au sujet des politiques de mot de passe**. Ce guide aborde d'autres sujets, comme l'authentification multifacteurs, mais ici, on va se concentrer uniquement sur l'aspect "*politique de mot de passe*".
Tout d'abord, **une politique de mot de passe définit les règles à respecter par un utilisateur** lorsqu'il souhaite définir un nouveau mot de passe pour son compte. À cela s'ajoutent **des règles de gestion des mots de passe**, comme la limite du nombre d'essais avant verrouillage du compte, la gestion de l'historique des mots de passe, etc.

A. Longueur minimale du mot de passe, en nombre de caractères

Pour les mots de passe ne devant pas être mémorisés par l'utilisateur, l'ANSSI recommande une longueur minimale beaucoup plus importante : minimum 20 caractères. Le stockage de ce précieux sésame s'effectuera dans votre gestionnaire de mots de passe.

Pour les mots de passe devant être mémorisés par l'utilisateur, ce qui est le cas du mot de passe Active Directory puisqu'il permet à l'utilisateur d'accéder à sa session Windows, l'ANSSI met à disposition le tableau suivant à la page 28 de son guide :

Niveau de sensibilité	Longueur minimale en nombre de caractères	Taille de clé équivalente en bits [5]
Faible à moyen	Entre 9 et 11	≈ 65
Moyen à fort	Entre 12 et 14	≈ 85
Fort à très fort	Au moins 15	≥ 100

TABLE 3 – Recommandations concernant les longueurs minimales des mots de passe

Source : Guide de l'ANSSI

Le niveau a choisir dépend de la sensibilité du compte concerné. Pour un compte d'un utilisateur lambda, on se situera sur les deux premiers niveaux de sensibilité. Pour les utilisateurs qui ont accès à des ressources sensibles ou des données confidentielles, on définira à minima le niveau de sensibilité "*Moyen à fort*". Et enfin, pour les administrateurs, la sensibilité sera au maximum, et donc il est recommandé de mettre en place l'authentification multifacteurs en complément. Tout cela pour dire que **la longueur minimale à imposer n'est pas une évidence et dépend du niveau de criticité du compte**.
Il faut retenir aussi qu'il est bien souvent plus pertinent d'augmenter la longueur de son mot de passe plutôt que de chercher à conserver la longueur tout en le complexifiant. Cela va permettre d'avoir une meilleure entropie sur votre mot de passe, et donc, de le rendre plus robuste, plus fort (voir cet article).

B. Ne pas imposer de longueur maximale pour les mots de passe

Imposer une longueur minimale est une excellente idée, mais à l'inverse **imposer une longueur maximale est une mauvaise idée**, ou alors elle doit être très élevée (et là pour des questions de sécurité et contrainte vis-à-vis du logiciel en lui-même). Fixer une longueur maximale revient aussi à empêcher l'utilisation de passphrase, appelée aussi "*phrase de passe*".

C. La complexité des mots de passe

En imposant des contraintes sur les types de caractères qu'un utilisateur doit utiliser pour définir un mot de passe, on définit ce que l'on appelle la règle de complexité des mots de passe. Pour cela, on met à la disposition de l'utilisateur différents jeux de caractères : les chiffres, les lettres A à Z en minuscules, les lettres de A à Z en majuscules, les caractères spéciaux, etc. Plus il y a de jeux de caractères autorisés, plus il y a de combinaisons possibles.

Généralement, pour s'en sortir et respecter cette notion de complexité des mots de passe, les utilisateurs vont remplacer un "a" par un "@", un "o" par un "0", ou encore ajouter un "!" à la fin du mot de passe. C'est un grand classique. On le sait tous, et on a tous fait ça un jour pour inventer un mot de passe.

Dans le cas d'une tentative d'attaque en ligne, c'est-à-dire contre un système actif, cette méthode reste encore efficace à condition que le compte ciblé soit en mesure d'être verrouillé au bout de quelques tentatives en échec. Par contre, dans le cas d'une attaque hors ligne où il est possible d'effectuer du brute force sans limites, il y a de fortes chances pour que le mot de passe soit deviné. En effet, il existe des outils et des dictionnaires capables d'imaginer ces variantes, et donc, de trouver votre mot de passe.

D. Le délai d'expiration des mots de passe

Alors que pendant longtemps, on entendait qu'il était nécessaire d'imposer aux utilisateurs de changer leur mot de passe tous les 6 mois ou une fois par an, aujourd'hui ce n'est plus aussi évident. Quel est l'intérêt de modifier son mot de passe "*Bonjour1*" par "*Bonjour2*" ? Si le mot de passe précédent fuite, il y a des chances pour que le suivant soit deviné assez facilement.
L'ANSSI précise que pour les comptes non sensibles, c'est-à-dire les comptes des utilisateurs : "*Si la politique de mots de passe exige des mots de passe robustes et que les systèmes permettent son implémentation, alors* ***il est recommandé de ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles*** *comme les comptes utilisateur.*" *[page 30 du guide]*.
Par contre, pour les comptes avec des privilèges, il est recommandé d'imposer un délai d'expiration compris **entre 1 et 3 ans**.

E. Contrôler la robustesse des mots de passe

Un mot de passe qui respecte la longueur minimale et les contraintes de complexité, est-il pour autant un mot de passe robuste ? En voilà une bonne question, et c'est un point très intéressant soulevé par l'ANSSI.
Ainsi, il est recommandé de :

- **Vérifier si votre mot de passe a déjà fait l'objet d'une fuite de données.**
  En fait, si vous définissez un mot de passe qui à première vue semble complexe, mais qu'il est présent dans un dictionnaire qui circule sur Internet ou qui est utilisé par certains outils, alors on peut douter de sa robustesse.

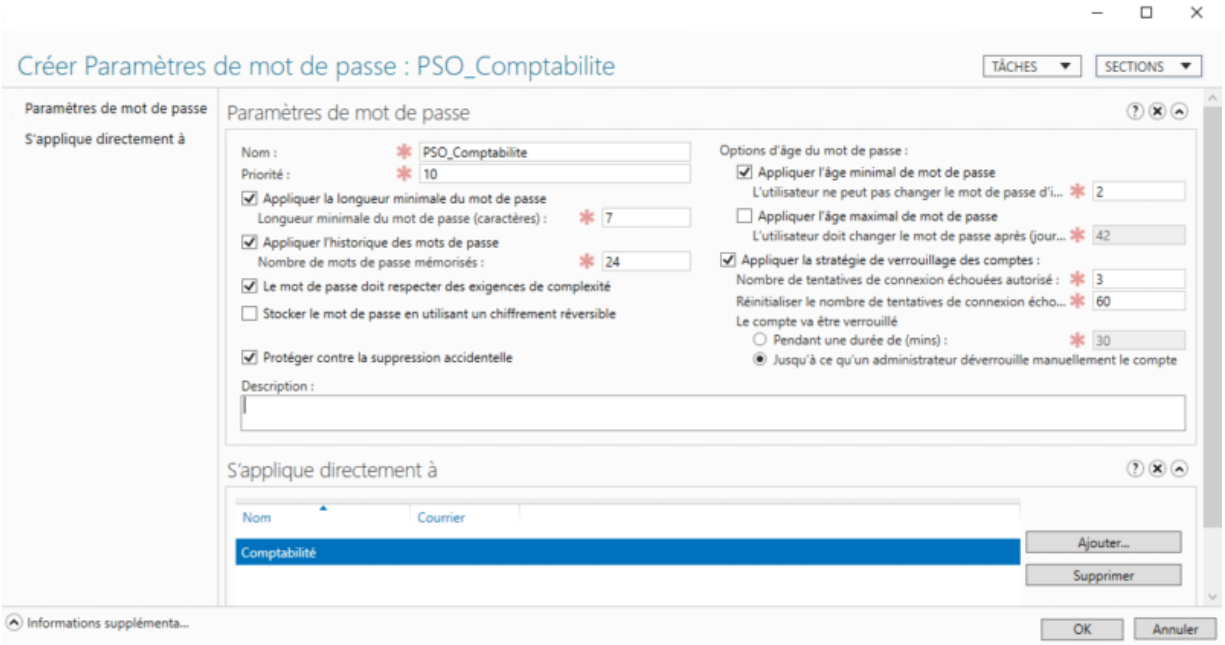
  Dans le même esprit, lorsqu'il y a une fuite de données suite à un piratage, on se retrouve avec d'énormes bases de données de mots de passe constituées à partir ces fuites. Si le nouveau mot de passe que vous venez de choisir se situe dans une fuite de données, il vaut mieux le changer immédiatement, car la probabilité qu'il soit trouvé est plus élevée. Par exemple, le site Have I Been Pwned permet de rechercher un mot de passe dans une base regroupant les données d'un ensemble de fuites d'information.
- **Bloquer les suites de caractères** ("12345", "azerty", "aaaa", "abcd", etc.)
- **Bloquer l'utilisation d'informations personnelles dans le mot de passe** (nom, prénom, date de naissance)
- **Bloquer la réutilisation d'un mot de passe déjà utilisé lors des X derniers mots de passe** (gestion de l'historique des mots de passe)

III. Quelles solutions techniques ?

En prenant connaissance des différentes **recommandations de l'ANSSI en matière de politique de mot de passe**, on se rend compte que d'un point de vue technique, cela ne va pas forcément être évident à mettre en œuvre. Enfin, c'est comme tout, il suffit d'avoir les bons outils alors cela tombe bien, car nous allons en parler de ces solutions potentielles.
Ici, j'évoque le cas des mots de passe stockés dans l'Active Directory et utilisé par les utilisateurs pour une connexion à Windows. En complément ce mot de passe peut être utilisé pour se connecter sur Microsoft 365, s'il y a un outil tel que Azure AD Connect en place au sein de votre infrastructure. Le stockage des mots de passe doit être effectué de façon sécurisée et **il convient de ne pas activer le chiffrement réversible au niveau de votre Active Directory**, même si c'est demandé par la solution logicielle que vous souhaitez utiliser.

A. Les politiques de mots de passe de l'Active Directory

La première solution qui nous vient à l'esprit, c'est la politique de mots de passe native à l'Active Directory. Il y a deux types de politiques de mots de passe : **celle définie par GPO, et celle que l'on définira sous la forme d'objets appelée stratégie de mots de passe affinée.**
Si l'on compare les recommandations de l'ANSSI avec les possibilités offertes nativement par l'Active Directory, on voit rapidement qu'**on ne pourra pas appliquer toutes les recommandations**.



Exemple d'une politique de mot de passe affinée

Sur des choses basiques comme la longueur minimale ou l'âge maximal du mot de passe, ce sera gérable. Par contre, sur les recommandations plus spécifiques comme le blocage de certaines chaînes de caractères ou la vérification dans les fuites de données, ce ne sera pas possible avec la méthode native de l'Active Directory. Pour la complexité des mots de passe, il est bien possible d'imposer le fait que le mot de passe doive respecter une certaine complexité, mais cette complexité n'est pas ajustable. Dommage.

Voici un récapitulatif :

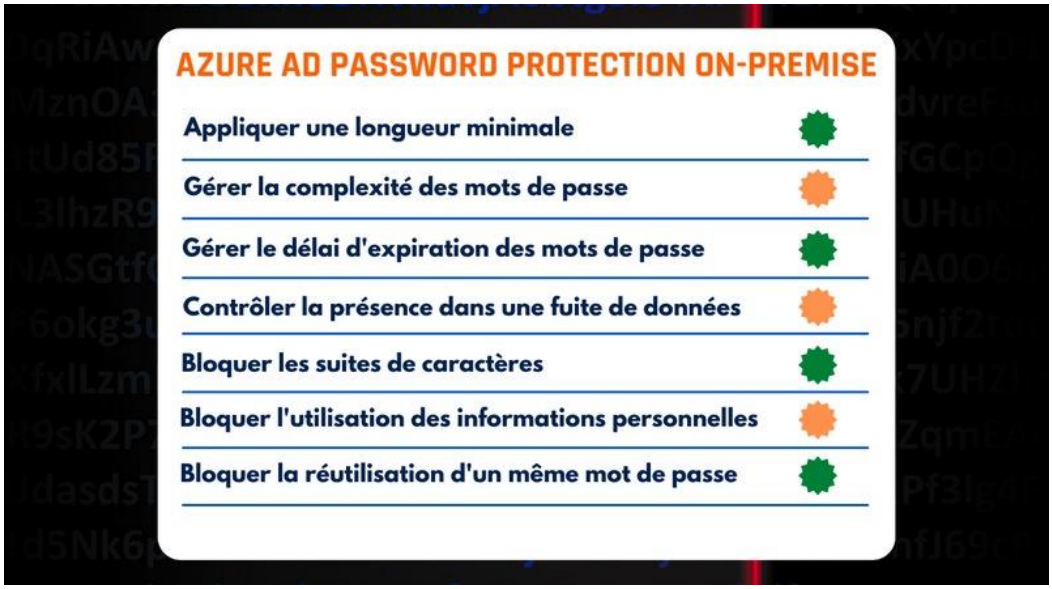
Même si cette méthode ne remplit pas toutes les cases vis-à-vis des recommandations de l'ANSSI, il vaut mieux mettre en place une stratégie de mot de passe affinée plutôt que de ne rien faire.

- Tutoriel - Politique de mot de passe affinée

B. La solution **Password protection for Windows Server Active Directory**

Azure AD intègre une fonctionnalité baptisée "**Password protection for Windows Server Active Directory**". Cette fonctionnalité s'applique aux utilisateurs Cloud, mais aussi aux utilisateurs locaux de l'Active Directory lorsqu'il y a une synchronisation avec Azure AD Connect.
Avec **Azure AD Password Protection**, vous allez renforcer la sécurité de vos mots de passe locaux puisque vous allez pouvoir bloquer certains termes (et leurs variantes) à partir d'un dictionnaire personnalisé, limité à 1000 entrées. Par exemple, avec l'entrée "*it-connect*", les mots de passe suivants sont bloqués : "*it-connect123*", "*it-c0nnect14!*" ou encore "*1t-c0nnect14!*". Certaines substitutions ne sont pas prises en compte, car si l'on bloque "*securite*", on peut définir "*S€curite14!*" comme mot de passe.
En complément, **Microsoft dispose de sa propre liste globale de mots de passe interdits (car trop faibles)**. J'ignore combien de mots de passe contient cette liste (ce n'est pas précisé) mais certains mots de passe présents dans des fuites de données semblent fonctionner. En tout cas, un mot de passe basique comme "*Password123!*" est bien bloqué alors qu'il pourrait matcher avec la politique de sécurité. Idem pour "*Azerty123!*" qui est bien bloqué, par contre "*Motdepasse123!*" et "*123soleil*" sont autorisés. J'ai tendance à penser que l'outil de Microsoft analyse surtout les mots anglais et qu'il ne doit pas forcément se référer à une liste externe comme I Have Been Pwned.

En cumulant une politique de mot de passe affinée et la protection Password Protection en complément, on obtient la synthèse suivante :



Cette fonctionnalité est incluse dans certaines licences et vous devez couvrir vos utilisateurs. L'installation est assez simple et s'appuie sur la mise en œuvre d'agents sur vos serveurs locaux. L'outil en tant que tel est peu configurable pour le moment, ce qui est dommage.

Si vous souhaitez en savoir plus sur Password Protection, je vous invite à lire ce tutoriel :

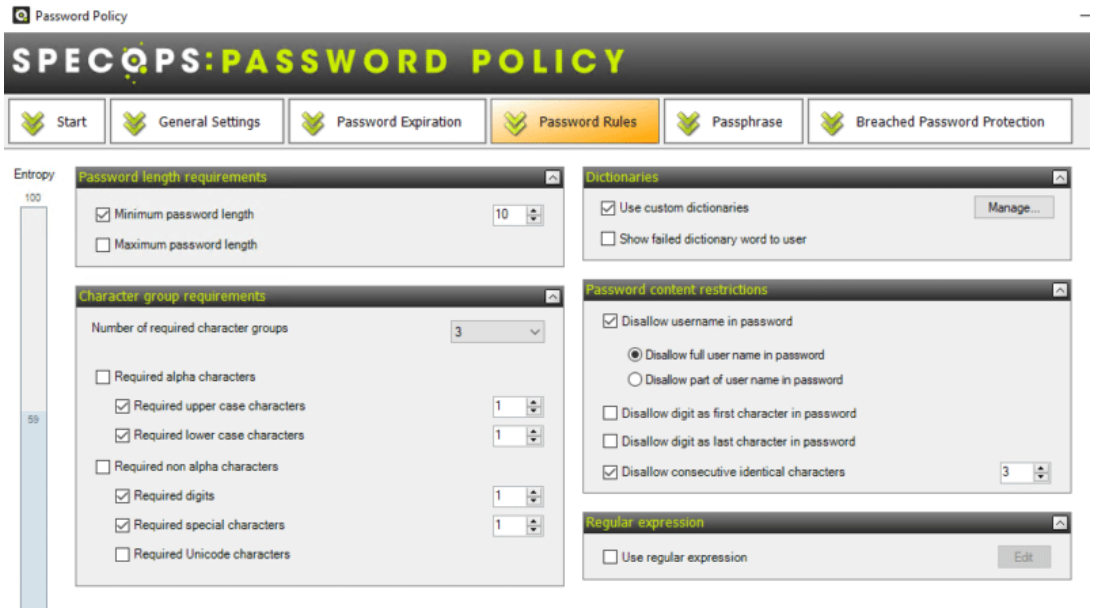
- Tutoriel - Azure AD Password Protection on-premise

C. La solution Specops Password Policy

En termes de solution payante et proposée par un éditeur tiers, je souhaitais inclure **Specops Password Policy** (SPP) à cet article. Pourquoi ? Pour une raison simple : je connais ce logiciel et je sais qu'il répond à la majorité des recommandations de l'ANSSI, pour ne pas dire toutes.
Ce logiciel va beaucoup plus loin que la solution native intégrée à l'Active Directory, notamment pour gérer la complexité des mots de passe. En fait, vous pouvez créer des règles très précises pour imposer l'utilisation à minima de X majuscules, X minuscules, X chiffres, etc...

Concernant le blocage des suites de caractères, c'est géré par SPP, car **il y a une option pour bloquer les caractères identiques consécutifs**, et il est possible de créer des expressions régulières pour empêcher certains patterns.
Pour **bloquer la présence des informations personnelles dans le mot de passe** (nom, prénom, date de naissance), c'est un peu plus complexe. L'outil intègre une option pour **empêcher l'utilisation de l'identifiant dans le mot de passe**, ce qui dans de nombreux cas, devrait permettre de bloquer le nom et le prénom puisque c'est souvent utilisé pour construire le login Active Directory de l'utilisateur. Pour la date de naissance, cette option n'est pas prise en charge par l'outil proposé par Specops. Pour cela, **il faudrait pouvoir se référer à un attribut de l'Active Directory, pour chaque utilisateur**. Néanmoins, la solution SPP intègre **la gestion de dictionnaires personnalisés**, ce qui vous permet d'importer des dictionnaires existants, ou de créer votre propre dictionnaire : vous pouvez créer un dictionnaire avec toutes les dates de naissance de vos salariés (*cela signifie aussi qu'un utilisateur X ne pourra pas utiliser dans son mot de passe la date de naissance d'un utilisateur Y, car le dictionnaire est commun à tous les utilisateurs ciblés par la politique*).

Pour ma part, je vous recommande de créer un dictionnaire avec le nom de votre entreprise, car c'est souvent réutilisé dans les mots de passe. Enfin, à partir des mots du dictionnaire l'outil bloquera aussi les variantes (*exemple : le mot "itconnect" implique que "itc0nnect" avec un zéro sera bloqué aussi*), en prenant compte de nombreuses méthodes de substitution (plus que la solution Microsoft présentée ci-dessus).



Aperçu de Specops Password Policy

La solution de l'éditeur Specops est capable de **vérifier si votre mot de passe a été compromis** (fuite de données, collecté via les honey pots SpecOps, etc.), en s'appuyant à la fois sur une base locale et sur une base en ligne au travers d'une API. **Cette base en ligne est actualisée quotidiennement et elle contient 2,5 milliards de mots de passe.** Si c'est le cas, l'utilisateur sera notifié par e-mail/SMS et invité à changer son mot de passe de nouveau. Sur ce point, on est vraiment conforme vis-à-vis des préconisations de l'ANSSI.

Voici un récapitulatif :

Pour découvrir plus en détail ce logiciel, je vous invite à lire mon tutoriel complet au sujet de Specops Password Policy, dans lequel vous pouvez retrouver également une vidéo de démonstration (réalisée par mes soins).

- Tutoriel - Specops Password Policy

IV. Conclusion

Suite à la lecture de cet article, vous avez connaissance des recommandations de l'ANSSI en matière de politique de mot de passe, et en plus, vous avez quelques pistes à explorer afin de mettre en pratique ces recommandations sur un annuaire Active Directory. En complément de la mise en œuvre de cette politique de mot de passe, il ne faudra pas oublier de configurer le verrouillage des comptes afin de bloquer les attaques Brute Force.

Si vous connaissez d'autres solutions susceptibles de **mettre en place une politique de mot de passe qui respecte les best practices de l'ANSSI**, n'hésitez pas à poster un commentaire.