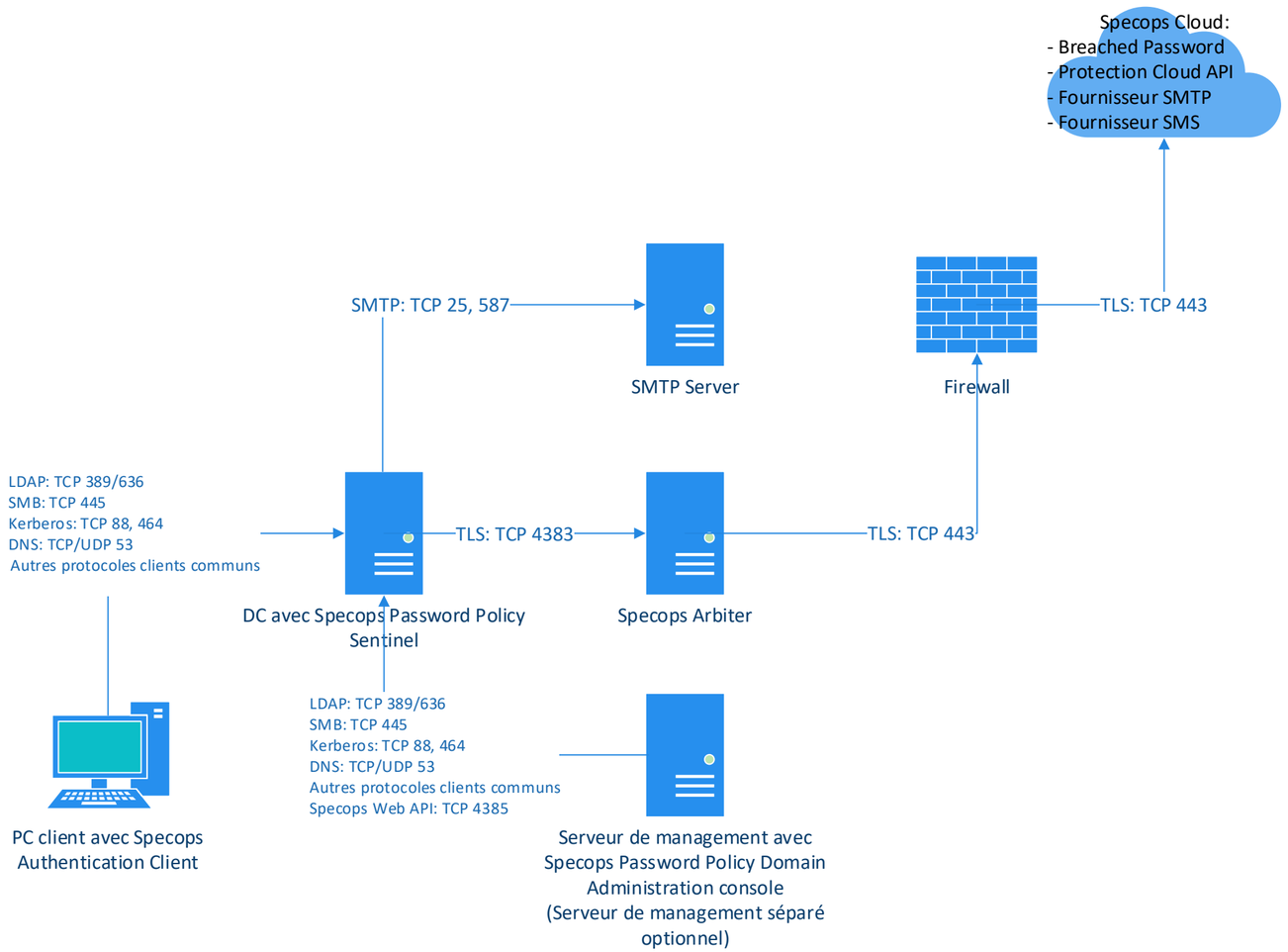
SPECOPS PASSWORD POLICY

APERÇU DES COMPOSANTS



Processus de changement de mot de passe

Les ports requis pour les communications entre le client et le DC ne changent pas lorsque Specops Password Policy est déployé dans un environnement.
*** L'application des règles de mot de passe est effectuée par les DCs avec le composant Specops Password Policy Sentinel.**
*** Le Specops Authentication Client, qui affiche en temps réel les règles de mot de passe à l'utilisateur pendant un changement de mot de passe, est facultatif.**
- Le retour d'information en temps réel sur les règles de mot de passe n'est disponible que sur Windows 10/11 x64.
- Le retour d'information sur les règles en cas de rejet du mot de passe est disponible sur les autres versions de Windows prises en charge.

1. L'utilisateur lance le changement de mot de passe sur le client en utilisant CTRL+ALT+DEL, Changer un mot de passe.

2. Le client avec le client d'authentification Specops effectue une recherche des informations de l'utilisateur Active Directory, en utilisant LDAP.

3. Le client avec le Specops Authentication Client recherche les règles de la politique de mot de passe Specops de l'utilisateur dans le fichier de configuration de la politique, en utilisant SMB, qui sont ensuite affichées à l'utilisateur.

4A. L'utilisateur tente de changer son mot de passe, qui est rejeté par un DC avec Specops Password Policy Sentinel, en utilisant Kerberos. Les règles de mot de passe rejetées sont affichées à l'utilisateur, telles que diverses exigences de complexité, dictionnaire personnalisé, mots de passe compromis (Breached Password Protection Express), en utilisant SMB.

4B. L'utilisateur réussit à changer son mot de passe, qui est accepté par un DC avec Specops Password Policy Sentinel, en utilisant Kerberos.

5. Après un changement de mot de passe réussi, et lorsque la protection Breached Password Protection Complete est activée, la vérification par rapport à la base cloud des mots de passe compromis commence immédiatement après le changement de mot de passe. Ce processus se termine généralement en 3 à 5 secondes. Le DC qui a traité le changement de mot de passe utilise les 4 premiers caractères du hash du mot de passe pour télécharger une liste de correspondances potentielles commençant par ces 4 premiers caractères.
La connexion du DC à l'API Specops Breached Password Protection Cloud est effectuée via l'arbiter Specops, qui agit comme un serveur passerelle.
- Le DC se connecte à l'Arbiter Specops en utilisant TLS : TCP 4383.
- L'arbiter de Specops se connecte à l'API Cloud de Specops en utilisant TLS : TCP 443.

6A. Le DC utilise la liste réduite des correspondances potentielles pour effectuer la comparaison finale. Le hash complet du nouveau mot de passe est comparé à la liste réduite. S'il y a une correspondance, le mot de passe est noté comme un mot de passe compromis. L'utilisateur peut être paramétré pour changer de mot de passe à la prochaine connexion, et être notifié par e-mail et/ou SMS.

6B. Le DC utilise la liste réduite des correspondances potentielles pour effectuer la comparaison finale. Le hash complet du nouveau mot de passe est comparé à la liste réduite. S'il n'y a pas de correspondance, le processus est terminé et l'utilisateur peut continuer à utiliser le nouveau mot de passe.

7. Si d'autres applications de synchronisation Active Directory sont utilisées, aucune configuration supplémentaire n'est généralement nécessaire. Les applications de synchronisation AD détecteront les mots de passe mis à jour dans Active Directory et effectueront la synchronisation si nécessaire.

Communications Email/SMS

Lorsque les notifications par e-mail sont activées :
*** Si un serveur SMTP personnalisé est sélectionné pour l'envoi des e-mails, le DC génère le message e-mail et l'envoie via le serveur SMTP configuré.**
La communication entre le DC et le serveur SMTP est nécessaire pour les notifications par e-mail :
- Pour les notifications par courriel, telles que :
  Notifications d'expiration de mot de passe
  Notifications de l'administrateur

Le DC avec le rôle FSMO de l'émulateur PDC génèrera les messages électroniques ci-dessus, donc ce DC devra être autorisé à relayer via le serveur SMTP personnalisé.
- Pour les notifications par e-mail Breached Password Protection Complete, n'importe quel DC pourrait générer ces messages e-mail, donc tous les DCs devraient être autorisés à relayer via le serveur SMTP personnalisé.

*** Si le service en ligne Specops est sélectionné pour l'envoi de messages électroniques, le DC génère le message électronique et le transmet au cloud Specops via le Specops Arbiter, où le message est envoyé via le fournisseur SMTP du cloud Specops.**
Les courriels proviennent du serveur SMTP : 168.245.19.207

Lorsque les notifications par SMS sont activées :
*** Le DC génère le message SMS et le transmet au Specops Cloud via le Specops Arbiter, où le SMS est envoyé via le fournisseur SMS de Specops Cloud.**

Gestion des communications

Les ports requis pour les communications entre le serveur de management et le DC ne changent pas lorsque la politique de mot de passe Specops est déployée dans un environnement, à l'exception des communications vers le DC avec le rôle PDC Emulator Active Directory FSMO. Le DC avec le rôle PDC Emulator FSMO aura Specops Password Policy Sentinel Web API d'activé, par défaut. L'API Web permet d'exécuter certaines fonctions à partir d'un serveur de management, telles qu'envoyer des emails de test après la configuration des paramètres SMTP et réaliser des analyses manuelles via Breached Password Protection Express, qui devraient autrement être exécutées localement sur le DC avec le rôle PDC Emulator FSMO. Les serveurs de management se connectent à l'API Web sur ce DC en utilisant TLS : TCP 4385, en plus des protocoles clients courants.
*** La console d'administration de domaine Specops Password Policy peut être installée sur les DCs et/ou d'autres serveurs de management, selon les besoins.**
*** Il est recommandé d'installer la console d'administration de Specops Password Policy et la console de gestion de stratégies de groupe Microsoft sur le même serveur de management. Cela permet aux administrateurs d'afficher et de modifier les paramètres de la politique de mot de passe Specops contenus dans les stratégies de groupe.**
*** La politique de mot de passe Specops est appliquée à l'aide d'objets de stratégie de groupe liés aux utilisateurs dans Active Directory. Les stratégies de groupe peuvent être liées au domaine ou à des OU spécifiques. Le filtrage de sécurité peut également être utilisé pour appliquer les stratégies de groupe aux groupes de sécurité ou aux utilisateurs.**
*** L'appartenance au groupe Domain Admins est nécessaire pour gérer la politique de mot de passe Specops, par défaut. Un groupe optionnel peut être créé, Specops Password Policy Admins, pour permettre la gestion par des comptes n'appartenant pas au groupe Domain Admins. Les permissions peuvent être déléguées pour la gestion des stratégies de groupe.**