Extension pour l’authentification unique Kerberos

Guide de l’utilisateur

Décembre 2019

Table des matières

Introduction

L’extension pour l’authentification unique (SSO) Kerberos facilite l’utilisation de ce type d’authentification avec les appareils Apple de votre organisation.

Authentification Kerberos simplifiée

L’extension pour l’authentification unique Kerberos simplifie le processus d’acquisition d’un ticket initial (« ticket-granting ticket », TGT) Kerberos auprès du domaine Active Directory de votre organisation, ce qui permet aux utilisateurs de s’authentifier de manière transparente à des ressources telles que sites web, apps et serveurs de fichiers. Sous macOS, l’extension pour l’authentification unique Kerberos acquiert de façon proactive un TGT Kerberos à chaque changement d’état du réseau pour s’assurer que l’utilisateur est bien prêt à s’authentifier dès que nécessaire.

Gestion des comptes Active Directory

L’extension pour l’authentification unique Kerberos aide également vos utilisateurs à gérer leur compte Active Directory. Sous macOS, elle permet aux utilisateurs de modifier le mot de passe de leur compte Active Directory et les prévient dès qu’un mot de passe est sur le point d’expirer. Les utilisateurs peuvent également modifier le mot de passe de leur compte local pour le faire concorder avec leur mot de passe Active Directory.

Prise en charge d’Active Directory

L’extension pour l’authentification unique Kerberos doit être utilisée avec un domaine Active Directory sur site. Azure Active Directory n’est pas pris en charge. Pour utiliser l’extension pour l’authentification unique Kerberos, les appareils n’ont pas besoin d’être reliés à un domaine Active Directory. Par ailleurs, les utilisateurs n’ont pas besoin de se connecter à leurs ordinateurs Mac à l’aide de comptes Active Directory ou de comptes mobiles. Apple recommande plutôt d’utiliser des comptes locaux.

Conditions requises

- iOS 13, iPadOS ou macOS Catalina.
- Un domaine Active Directory exécutant Windows Server 2008 (ou version ultérieure). L’extension pour l’authentification unique Kerberos n’est pas conçue pour être utilisée avec Azure Active Directory. Elle nécessite un domaine Active Directory sur site classique.
- Accédez au réseau sur lequel est hébergé le domaine Active Directory. L’accès à ce réseau doit s’effectuer par Wi-Fi, Ethernet ou VPN.
- Les appareils doivent être gérés à l’aide d’une solution de gestion des appareils mobiles (MDM) prenant en charge les données utiles du profil de configuration d’authentification unique (SSO) extensible. Contactez votre fournisseur de solutions MDM pour savoir s’il prend en charge les données utiles de ce profil de configuration.

Enterprise Connect

L’extension pour l’authentification unique Kerberos a vocation à remplacer Enterprise Connect. Si vous utilisez actuellement Enterprise Connect et souhaitez passer à l’extension pour l’authentification unique Kerberos, veuillez consulter la section « Faire la transition à partir d’Enterprise Connect » pour y trouver de plus amples informations.

Se lancer

Élaboration et déploiement d’un profil de configuration

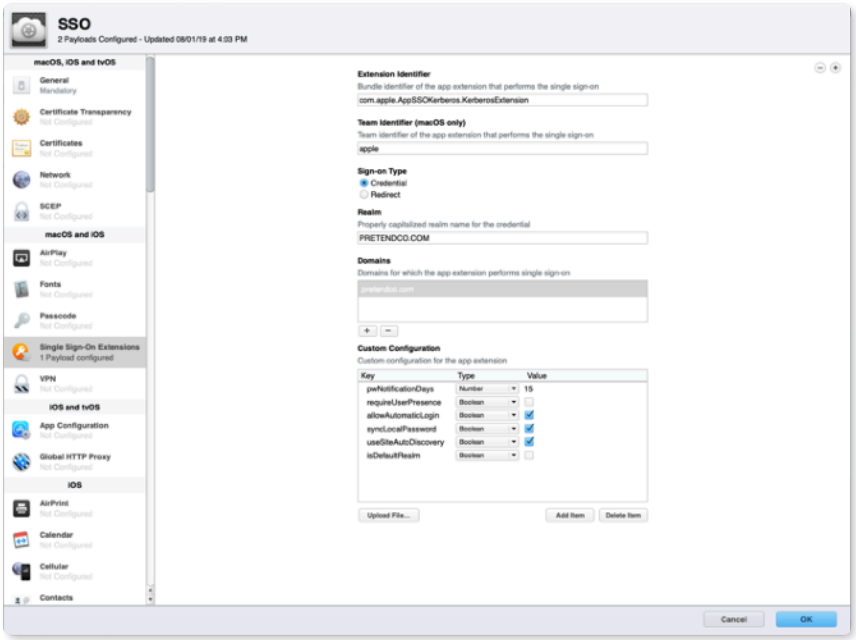
Pour utiliser l’extension pour l’authentification unique Kerberos, vous devez configurer cette dernière à l’aide d’un profil de configuration, fourni à l’appareil à partir de la solution de gestion des appareils mobiles (MDM).

Remarque : le profil de configuration doit être livré à l’appareil par la solution MDM. Sous macOS, il doit s’agir d’une inscription à la MDM approuvée par l’utilisateur et installée dans le périmètre du système. L’ajout manuel du profil n’est pas pris en charge.

Pour effectuer la configuration à l’aide d’un profil de configuration, vous utiliserez les données utiles de l’authentification unique extensible introduites dans iOS 13, iPadOS et macOS 10.15. Le Gestionnaire de profils, qui fait partie de macOS Server, inclut la prise en charge des données utiles de l’authentification unique extensible. Si votre solution MDM ne prend pas encore en charge ces données utiles, vous pouvez peut-être élaborer le profil nécessaire dans le Gestionnaire de profils, puis l’importer dans votre solution MDM afin que celle-ci en assure la distribution. Veuillez contacter votre fournisseur de solutions MDM pour obtenir des informations complémentaires.

Pour élaborer un profil de configuration à l’aide du Gestionnaire de profils, suivez les étapes ci-dessous :

1. Connectez-vous au Gestionnaire de profils.
2. Créez un profil pour un groupe d’appareils ou pour un appareil spécifique.
3. Sélectionnez Single Sign-On Extensions dans la liste des Données utiles, puis cliquez sur le bouton d’ajout (+) pour ajouter de nouvelles données utiles.
4. Dans le champ Extension Identifier, saisissez « com.apple.AppSSOKerberos.KerberosExtension ».
5. Dans le champ Team Identifier, saisissez « apple ».



6. Sous Sign-on Type, sélectionnez Credential.

7. Dans le champ Realm, inscrivez tout en majuscules le nom de votre domaine Active Directory où résident vos comptes d'utilisateurs. N'utilisez pas le nom de votre forêt Active Directory, sauf si vos comptes d'utilisateurs résident au niveau de la forêt.
8. Sous Domains, cliquez sur le bouton d'ajout (+) pour ajouter des domaines pour toutes les ressources utilisant Kerberos. Par exemple, si vous utilisez l'authentification Kerberos avec des ressources contenues dans us.pretendco.com, ajoutez « .us.pretendco.com », sans oublier le point initial.
9. Sous Custom Configuration, ajoutez les valeurs suivantes :

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Non vérifié
allowAutomaticLogin	Boolean	Vérifié
syncLocalPassword	Boolean	Vérifié
useSiteAutoDiscovery	Boolean	Vérifié
isDefaultRealm	Boolean	Non vérifié

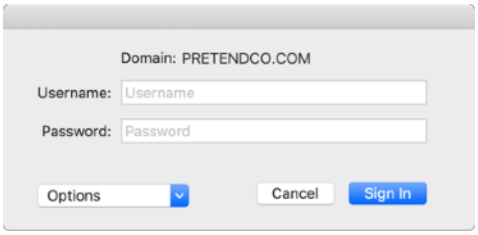
10. Cliquez sur OK pour enregistrer le nouveau profil de configuration. Celui-ci s'installera automatiquement sur l'appareil ou le groupe d'appareils sélectionné.

Configuration par l'utilisateur – iOS et iPadOS

1. Connectez votre appareil à un réseau dans lequel le domaine Active Directory de votre organisation est disponible.
2. Procédez de l'une des manières suivantes :
   - Utilisez Safari pour accéder à un site web prenant en charge l'authentification Kerberos.
   - Lancez une app prenant en charge l'authentification Kerberos.
3. Saisissez vos nom d'utilisateur et mot de passe Kerberos ou Active Directory.
4. Il vous sera demandé si vous voulez vous connecter automatiquement de manière permanente. La plupart des utilisateurs devront toucher Yes.
5. Touchez Sign In. Après une courte pause, votre app ou site web se chargera. Si vous avez choisi de vous connecter automatiquement à l'extension pour l'authentification unique Kerberos, vous n'aurez plus à fournir vos identifiants tant que vous ne changerez pas de mot de passe. Si vous n'avez pas choisi de vous connecter automatiquement, vous serez invité à saisir vos identifiants uniquement à l'expiration de vos identifiants Kerberos, généralement dans un délai de 10 heures.

Configuration par l'utilisateur – macOS

1. Vous devez vous authentifier auprès de l'extension pour l'authentification unique Kerberos. Il y a plusieurs façons de lancer ce processus :
   - Si votre Mac est connecté au réseau sur lequel votre domaine Active Directory est disponible, vous serez invité à vous authentifier immédiatement après l'installation du profil de configuration SSO extensible.
   - Si vous utilisez Safari pour accéder à un site web acceptant l'authentification Kerberos ou une app exigeant cette authentification, vous serez invité à vous authentifier.
   - Vous serez immédiatement invité à vous authentifier dès que vous connecterez votre Mac à un réseau sur lequel votre domaine Active Directory est disponible.
   - Vous pouvez sélectionner le menu supplémentaire de l'extension pour l'authentification unique Kerberos, puis cliquer sur Sign In.
2. Vous serez invité à saisir vos identifiants Kerberos. Saisissez vos nom d'utilisateur et mot de passe Kerberos ou Active Directory.



3. Il vous sera demandé si vous voulez vous connecter automatiquement. La plupart des utilisateurs devront cliquer sur Yes.
4. Cliquez sur Sign In. Après une courte pause, votre app ou site web se chargera. Si vous avez choisi de vous connecter automatiquement à l'extension pour l'authentification unique Kerberos, vous n'aurez plus à fournir vos identifiants tant que vous ne changerez pas de mot de passe. Si vous n'avez pas choisi de vous connecter automatiquement, vous serez invité à saisir vos identifiants uniquement à l'expiration de vos identifiants Kerberos, généralement dans un délai de 10 heures.
5. Si votre mot de passe est sur le point d'expirer, vous recevrez une notification vous indiquant le nombre de jours qu'il vous reste avant l'expiration. Vous pouvez cliquer sur cette notification et modifier votre mot de passe.
6. Si vous avez activé la fonctionnalité de synchronisation des mots de passe, il vous sera demandé de fournir vos mots de passe Active Directory et de compte local en cours de validité. Saisissez ces deux mots de passe, puis cliquez sur OK pour tout synchroniser. Vous verrez cette invite à la première connexion, même si vos mots de passe sont déjà synchronisés.

Changement de mots de passe – macOS

L'extension pour l'authentification unique Kerberos vous permet également de modifier votre mot de passe Active Directory :

1. Vérifiez que vous êtes bien connecté à l'extension pour l'authentification unique Kerberos.

2. Sélectionnez le menu supplémentaire de l’extension pour l’authentification unique Kerberos et choisissez Modifier le mot de passe. Vous pouvez aussi recevoir une notification vous indiquant que votre mot de passe est sur le point d’expirer.
3. Saisissez votre mot de passe actuel, puis le nouveau. Veillez à ce que votre nouveau mot de passe respecte les règles fixées par votre organisation en matière de mots de passe. Cliquez sur OK.
4. Après une courte pause, vous verrez s’afficher une boîte de dialogue vous indiquant que le mot de passe a bien été modifié. Si la fonctionnalité de synchronisation des mots de passe est activée, le mot de passe de votre compte local sera actualisé pour correspondre à votre nouveau mot de passe Active Directory.

Utilisation du menu supplémentaire de l’authentification unique Kerberos – macOS

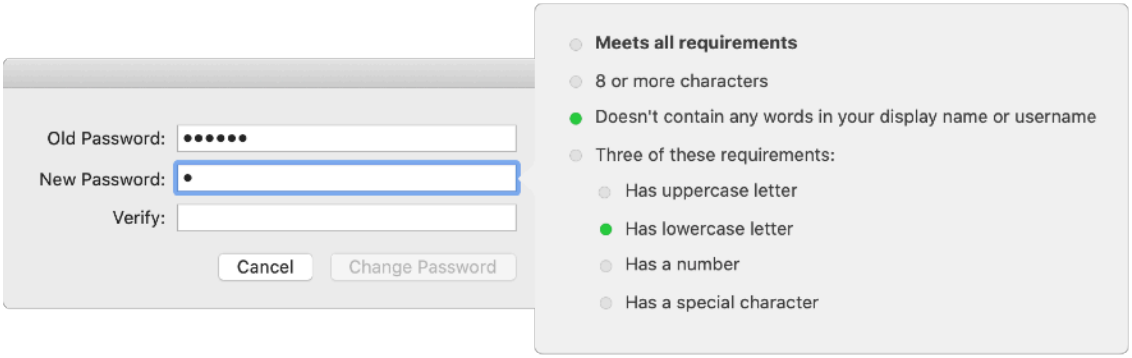
Le menu supplémentaire de l’authentification unique Kerberos offre un accès facile à des informations utiles sur votre compte et aux fonctions de l’extension. Vous le verrez apparaître sous la forme d’une clé de couleur grise ou noire dans la barre de menus, en haut à droite.

Pour connaître le statut de votre compte, vérifiez la couleur de l’icône du menu supplémentaire de l’extension pour l’authentification unique Kerberos. Si la clé est grise, c’est que vous n’êtes pas connecté à l’extension. Si elle est noire, c’est que vous êtes connecté. Après avoir sélectionné la clé, vous verrez le compte auquel vous êtes connecté ainsi que le nombre de jours qu’il vous reste avant l’expiration de votre mot de passe. Le menu vous permet également de vous connecter, de vous déconnecter et de modifier votre mot de passe.

Fonctions avancées

Test des mots de passe en direct

Dans de nombreuses configurations Active Directory, l'extension pour l'authentification unique Kerberos peut tester les nouveaux mots de passe des utilisateurs à mesure que ceux-ci les saisissent et leur indiquer les exigences qu'ils doivent respecter pour changer de mot de passe. Une fois cette fonction configurée, la vue suivante s'affichera lorsque l'utilisateur saisira son nouveau mot de passe :



Pour utiliser cette fonctionnalité, votre domaine Active Directory doit appliquer uniquement les politiques Active Directory standard en matière de mots de passe. Par défaut, Active Directory permet à un administrateur d'exiger qu'un mot de passe soit à la fois complexe et d'une certaine longueur.
Pour en savoir plus sur ce qui constitue un mot de passe complexe, consultez technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Remarque : vous risquez de ne pas pouvoir utiliser cette fonctionnalité si votre domaine utilise des DLL ou des outils tiers pour étendre la politique Active Directory standard en matière de mots de passe. Par exemple, si vous n'avez pas le droit d'utiliser dans votre mot de passe certains mots tels que votre nom d'utilisateur ou si votre mot de passe doit contenir un certain nombre de caractères spéciaux, il se peut que vous appliquiez des extensions de politiques tierces en matière de mots de passe. Si vous avez un doute, demandez des précisions à votre administrateur Active Directory.

Si le domaine Active Directory de votre organisation satisfait aux exigences, vous pouvez activer la procédure de test des mots de passe en direct. Dans votre profil de configuration de l'extension pour l'authentification unique Kerberos, réglez les paramètres suivants :

Paramètre	Key	Type	Value	Facultatif
Exigence de mots de passe	pwReqComplexity	Boolean	OUI	Non
Longueur requise des mots de passe	pwReqLength	Integer	Nombre	Oui
Limite à la réutilisation des mots de passe précédents	pwReqHistory	Integer	Nombre	Oui
Âge minimum des mots de passe	pwReqMinAge	Integer	Nombre	Oui

La procédure de test des mots de passe en direct est soumise à certaines limites. Elle ne peut pas vérifier si un mot de passe a déjà été utilisé. Elle ne peut pas non plus vérifier si votre mot de passe contient votre nom tel qu'il s'affiche dans Active Directory si vous ne disposez pas déjà d'un ticket initial (TGT) Kerberos.

Cela peut se produire si c'est la première fois que vous définissez votre mot de passe ou si celui-ci a expiré. Tous les autres tests s'effectueront normalement.

Affichage des exigences en matière de mots de passe

Si vous ne pouvez pas utiliser la procédure de test des mots de passe en direct, vous pouvez configurer l'extension pour l'authentification unique Kerberos de façon à ce qu'elle affiche une chaîne de texte indiquant les exigences de votre organisation en matière de mots de passe au moment où les utilisateurs saisissent leur nouveau mot de passe. Dans votre profil de configuration de l'extension pour l'authentification unique Kerberos, réglez « pwReqText » sur une chaîne contenant le texte qui doit se présenter à un utilisateur au moment où celui-ci change de mot de passe.

Adaptation ou désactivation de la fonctionnalité de modification des mots de passe

Il se peut que certaines organisations ne puissent pas utiliser la fonctionnalité standard de modification des mots de passe fournie par l'extension pour l'authentification unique Kerberos, car elles n'autorisent pas la modification des mots de passe par rapport à Active Directory. Dans votre profil de configuration de l'extension pour l'authentification unique Kerberos, réglez « allowPasswordChanges » sur FALSE pour désactiver cette fonctionnalité.

Prise en charge des sites web de modification des mots de passe – macOS

L'extension pour l'authentification unique Kerberos peut être configurée de façon à ouvrir un site web de modification de mot de passe dans le navigateur par défaut lorsque l'utilisateur sélectionne « Modifier le mot de passe » ou lorsqu'il prend acte de l'avis d'expiration d'un mot de passe. Apple recommande de n'utiliser cette fonctionnalité qu'avec un compte local, les comptes mobiles n'étant pas pris en charge.

Dans votre profil de configuration de l'extension pour l'authentification unique Kerberos, réglez « pwChangeURL » sur l'URL de votre site web de changement de mot de passe. Une fois que les utilisateurs ont modifié leur mot de passe, ils doivent se déconnecter de l'extension Kerberos, puis se reconnecter à l'aide de leur nouveau mot de passe. Si la synchronisation des mots de passe locaux est activée, ils seront guidés dans les étapes de resynchronisation de leurs mots de passe.

Synchronisation des mots de passe – macOS

L'extension pour l'authentification unique Kerberos peut définir le mot de passe du compte local d'un utilisateur pour le faire correspondre au mot de passe de son compte Active Directory. Pour activer cette fonctionnalité, réglez « syncLocalPassword » sur TRUE dans la partie Configuration personnalisée de votre profil de configuration de l'extension pour l'authentification unique Kerberos.

Le processus de synchronisation des mots de passe comprend deux fonctions élémentaires. D'abord, lorsque l'utilisateur recourt à l'extension pour l'authentification unique Kerberos pour changer de mot de passe, cette fonctionnalité fait concorder son mot de passe local avec son mot de passe Active Directory. Si les mots de passe du compte local et du compte Active Directory se désynchronisent, l'extension pour l'authentification unique Kerberos les resynchronise de la façon suivante :

- À l'activation de la synchronisation des mots de passe et à chaque tentative ultérieure de connexion effectuée par l'extension pour l'authentification unique Kerberos, les dates auxquelles l'utilisateur a modifié ses mots de passe local et Active Directory pour la dernière fois sont comparées aux valeurs mises en cache. Si les valeurs concordent, les mots de passe sont synchronisés et aucune action n'est requise. Si, en revanche, elles ne concordent pas, l'extension pour l'authentification unique Kerberos invitera l'utilisateur à saisir ses mots de passe local et Active Directory. Une fois qu'il aura fourni son mot de passe local, l'extension pour l'authentification unique Kerberos le fera concorder avec son mot de passe Active Directory.
- Les changements de mots de passe fonctionnent de la même façon. Lorsqu'un utilisateur effectue un changement de mot de passe avec l'extension pour l'authentification unique Kerberos, son ancien mot de passe Active Directory est vérifié par rapport à celui de son compte local. Si un ancien mot de passe Active Directory et le mot de passe du compte local concordent, l'extension pour l'authentification unique Kerberos modifie les deux mots de passe. S'ils ne concordent pas, seul le mot de passe Active Directory est modifié. L'utilisateur est invité à fournir son mot de passe local lors de la tentative de connexion suivante.

Cette fonctionnalité impose les exigences suivantes :

- Si les utilisateurs sont connectés à leurs ordinateurs Mac par des comptes Active Directory – et non par des comptes locaux –, la synchronisation des mots de passe est désactivée. Cette fonctionnalité ne s'utilise qu'avec les comptes locaux. Si les utilisateurs se connectent à leur ordinateur Mac avec leur compte Active Directory, elle devient inutile.
- Si une politique en matière de mots de passe est appliquée aux comptes locaux (par exemple, l'utilisation d'un profil de configuration ou de la commande pwpolicy), veillez à ce que cette politique corresponde à celle utilisée pour les comptes Active Directory ou qu'elle soit moins stricte. Si la politique en matière de mots de passe pour les comptes locaux est plus stricte que celle pour Active Directory, il peut arriver que l'extension pour l'authentification unique Kerberos accepte un mot de passe répondant aux exigences Active Directory, mais qu'elle ne parvienne pas à définir le mot de passe local parce que celui-ci ne répond pas aux exigences des mots de passe locaux. Si la politique en matière de mots de passe pour les comptes locaux doit être plus stricte que celle pour Active Directory, n'utilisez pas cette fonctionnalité.
- Le nom d'utilisateur du compte local est différent du nom d'utilisateur Active Directory. Seuls les mots de passe doivent concorder.

Prise en charge des cartes à puce – macOS

L'extension pour l'authentification unique Kerberos prend en charge l'utilisation d'identités basées sur des cartes à puce pour l'authentification. Les cartes à puce doivent disposer d'un pilote CryptoTokenKit ; les pilotes basés sur TokenD ne sont pas pris en charge. macOS 10.15 prend en charge le standard PIV (Personal Identification Verification), largement utilisé par l'Administration américaine.

Avant de vous lancer, assurez-vous que votre domaine Active Directory est configuré pour prendre en charge l'authentification par carte à puce. Le processus d'activation de l'authentification par carte à puce auprès d'Active Directory n'est pas traité dans le cadre de ce document. Pour de plus amples détails, veuillez vous reporter à la documentation Microsoft.

Pour vous connecter à l'extension pour l'authentification unique Kerberos à l'aide d'une carte à puce, suivez les étapes ci-dessous :

1. Cliquez sur le menu Options, puis sélectionnez « Utiliser une carte à puce ».
2. Dès que vous voyez le bouton Identity, insérez votre carte à puce et cliquez sur ce bouton.
3. Choisissez l'identité que vous voulez utiliser pour vous authentifier, cliquez sur OK, puis sur Sign In.

4. Saisissez votre code PIN dès que vous êtes invité à le faire.

Si l'extension pour l'authentification unique Kerberos a besoin d'acquérir un TGT Kerberos, il vous sera demandé d'insérer votre carte à puce et de saisir votre code PIN. Vous trouverez plus d'informations sur la prise en charge des cartes à puce dans macOS en exécutant « man SmartCardServices » dans Terminal.

Notifications distribuées – macOS

L'extension pour l'authentification unique Kerberos publie des notifications distribuées lorsque surviennent différents types d'événements. Les apps et les services de macOS utilisent des notifications distribuées pour prévenir d'autres apps et services qu'un événement s'est produit. Ainsi, une app ou un service à l'écoute de ce type d'événement pourra prendre des mesures dès que nécessaire.

Un administrateur peut utiliser cette fonctionnalité pour prendre des mesures lorsque se produisent certains événements. Il peut, par exemple, décider d'exécuter un script à chaque fois que l'extension pour l'authentification unique Kerberos acquiert un nouvel identifiant Kerberos.

L'extension pour l'authentification unique Kerberos se contente de publier des notifications distribuées lorsque surviennent des événements spécifiques : elle ne lance aucune action. L'administrateur doit fournir un outil permettant d'être à l'affût de ces notifications et d'entreprendre des actions lorsque se produisent de tels événements.

Vous trouverez en annexe l'exemple d'un script et d'une liste de propriétés launchd (.plist) capables d'être à l'écoute des notifications et de lancer des actions en conséquence. Modifiez cet exemple en fonction des besoins de votre déploiement.

Voici les notifications distribuées publiées par l'extension pour l'authentification unique Kerberos :

Nom	À la publication
com.apple.KerberosPlugin.ConnectionCompleted	L'extension pour l'authentification unique Kerberos a exécuté son processus de connexion.
com.apple.KerberosPlugin.ADPasswordChanged	L'utilisateur a modifié le mot de passe Active Directory à l'aide de l'extension.
com.apple.KerberosPlugin.LocalPasswordSynced	L'utilisateur a synchronisé le mot de passe Active Directory et le mot de passe local.
com.apple.KerberosPlugin.InternalNetworkAvailable	L'utilisateur s'est connecté à un réseau dans lequel le domaine Active Directory configuré est disponible.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	L'utilisateur s'est connecté à un réseau dans lequel le domaine Active Directory configuré n'est pas disponible.
com.apple.KerberosExtension.gotNewCredential	L'utilisateur a acquis un nouveau TGT Kerberos.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	L'utilisateur a changé de mot de passe Active Directory, et son mot de passe local a été actualisé pour concorder avec le nouveau mot de passe Active Directory.

Prise en charge de la ligne de commande – macOS

Les administrateurs peuvent utiliser un outil de ligne de commande appelé *app-sso* permettant de contrôler l'extension pour l'authentification unique Kerberos et d'accéder à des informations utiles. Ils peuvent, par exemple, utiliser cet outil pour initier les ouvertures de session, les changements de mots de passe et les fermetures de session. Cet outil leur permet également d'imprimer des informations utiles, comme l'utilisateur actuellement connecté, le site Active Directory actuel de l'ordinateur, le partage réseau de départ de l'utilisateur, la date d'expiration du mot de passe de l'utilisateur et toute une variété d'autres informations utiles dans la liste des propriétés ou au format JSON. Ces informations peuvent être analysées et téléchargées dans une solution de gestion de Mac à des fins d'inventaire, entre autres.

Pour plus d'informations sur l'utilisation d'app-sso, exécutez « app-sso - h » dans l'app Terminal.

Comptes mobiles – macOS

L'extension pour l'authentification unique Kerberos n'exige pas que votre Mac soit lié à Active Directory ou que l'utilisateur soit connecté au Mac avec un compte mobile. Apple vous suggère d'utiliser l'extension pour l'authentification unique Kerberos avec un compte local. Les comptes locaux fonctionnent mieux avec le modèle de déploiement recommandé pour macOS et constituent le meilleur choix pour les utilisateurs de Mac actuels, qui sont susceptibles de se connecter de façon intermittente au réseau de votre organisation. L'extension pour l'authentification unique Kerberos a été spécialement créée pour améliorer l'intégration d'Active Directory à partir d'un compte local.

Toutefois, si vous choisissez de continuer à utiliser des comptes mobiles, vous pourrez quand même utiliser l'extension pour l'authentification unique Kerberos. Cette fonctionnalité impose les exigences suivantes :

- La synchronisation des mots de passe ne fonctionne pas avec les comptes mobiles. Si vous utilisez l'extension pour l'authentification unique Kerberos pour modifier votre mot de passe Active Directory et que vous êtes connecté à votre Mac avec le compte que vous utilisez avec l'extension pour l'authentification unique Kerberos, la modification des mots de passe fonctionne de la même façon que dans le volet Utilisateurs et groupes des Préférences Système. Mais si vous effectuez un changement de mot de passe à l'extérieur (en d'autres termes, si vous modifiez votre mot de passe sur un site web ou si c'est votre service d'assistance qui le réinitialise), l'extension pour l'authentification unique Kerberos ne pourra pas resynchroniser le mot de passe de votre compte mobile avec votre mot de passe Active Directory.
- L'utilisation d'une URL de changement de mot de passe avec l'extension Kerberos et un compte mobile n'est pas prise en charge.

Mappage domaine/royaume

Il se peut qu'un administrateur ait besoin de définir un mappage domaine/royaume personnalisé pour Kerberos. Par exemple, une organisation pourrait disposer d'un royaume Kerberos nommé « ad.pretendco.com », mais avoir besoin d'utiliser l'authentification Kerberos pour des ressources se trouvant dans le domaine « fakecompany.com ».

Remarque : l'implémentation de Kerberos dans les systèmes d'exploitation Apple peut automatiquement déterminer le mappage domaine/royaume dans la plupart des situations. Il est très rare qu'un administrateur soit amené à personnaliser ces réglages.

Le mappage domaine/royaume peut être configuré pour l'extension pour l'authentification unique Kerberos en suivant les étapes ci-dessous :

1. Dans la section Configuration personnalisée du profil d'authentification unique extensible, ajoutez un objet nommé domainRealmMapping. L'objet doit être de type Dictionnaire.
2. Attribuez à la clé de ce dictionnaire le nom de votre royaume en majuscules.
3. Définissez la valeur de ce dictionnaire comme étant de type Tableau. La première valeur doit être le nom de votre royaume Kerberos, orthographié en minuscules et débutant par un point.
   La deuxième valeur doit être le nom du domaine ayant besoin d'être authentifié par rapport à ce royaume et débutant également par un point. Ajoutez autant de tableaux que nécessaire.

Pour plus d'informations, reportez-vous à la documentation Kerberos.

Faire la transition à partir d'Enterprise Connect

Présentation

L'extension pour l'authentification unique Kerberos a vocation à remplacer Enterprise Connect, outil similaire qu'utilisent de nombreuses organisations. La plupart des organisations passant d'Enterprise Connect à l'extension pour l'authentification unique Kerberos suivront les étapes ci-dessous :

1. Élaborer un profil de configuration pour l'extension pour l'authentification unique Kerberos offrant des fonctionnalités identiques à celles de votre profil Enterprise Connect actuel.
2. Désinstaller Enterprise Connect.
3. Déployer le profil de configuration de l'extension pour l'authentification unique Kerberos.
4. Inviter les utilisateurs à se connecter à l'extension pour l'authentification unique Kerberos.

Le passage à l'extension pour l'authentification unique Kerberos n'est pas requis pour faire évoluer les ordinateurs Mac de votre organisation vers macOS 10.15. Enterprise Connect fonctionne comme prévu avec macOS 10.15, mais les organisations doivent quand même prévoir, à terme, une transition à partir d'Enterprise Connect.

Qui ne doit pas faire la transition

L'extension pour l'authentification unique Kerberos répondra aux besoins de l'immense majorité des organisations qui utilisent Enterprise Connect. Il se peut, toutefois, qu'une organisation satisfaisant aux critères suivants ne puisse pas faire la transition à partir d'Enterprise Connect ou ne puisse la faire que partiellement :

- Une organisation disposant actuellement d'ordinateurs Mac exécutant macOS 10.14 (ou version antérieure) doit continuer à exécuter Enterprise Connect sur ces systèmes et ne faire passer à l'extension pour l'authentification unique Kerberos que les ordinateurs Mac exécutant macOS 10.15.
  L'extension pour l'authentification unique Kerberos et le profil de configuration qui lui est associé ne fonctionneront que sur les ordinateurs Mac exécutant macOS 10.15. Installez macOS 10.15 sur ces ordinateurs pour tirer parti de l'extension pour l'authentification unique Kerberos.
- Une organisation utilisant un outil de gestion des Mac qui ne prend pas en charge l'inscription auprès de la MDM approuvée par l'utilisateur.
- Une organisation n'utilisant pas d'outil de gestion.
- Une organisation utilisant le niveau fonctionnel Active Directory de Windows Server 2003 (ou version ultérieure).

Création d'un profil de configuration pour l'extension pour l'authentification unique Kerberos

Vous allez devoir créer un profil de configuration pour l'extension pour l'authentification unique Kerberos semblable à celui d'Enterprise Connect. Nombre de Preference Keys de votre profil de configuration Enterprise Connect actuel ont un équivalent dans un profil pour l'extension pour l'authentification unique Kerberos. Commencez par examiner le tableau ci-dessous, indiquant les correspondances entre les Preference Keys Enterprise Connect et leurs équivalents dans l'extension pour l'authentification unique Kerberos :

Enterprise Connect	Extension pour l'authentification unique Kerberos	Notes
adRealm	Realm	Le nom du royaume doit être écrit en majuscules.
Automatic login (enabled by default)	allowAutomaticLogin	Ajouter à la section Configuration personnalisée. Doit être réglé sur True pour que la connexion automatique fonctionne.
disablePasswordFunctions	allowPasswordChange	Ajouter à la section Configuration personnalisée. Régler sur False pour désactiver les changements de mot de passe.
passwordChangeURL	pwChangeURL	Ajouter à la section Configuration personnalisée.
passwordExpireOverride	pwExpireOverride	Ajouter à la section Configuration personnalisée.
passwordNotificationDays	pwNotificationDays	Ajouter à la section Configuration personnalisée.
prepopulatedUsername	principalName	Ajouter à la section Configuration personnalisée.
pwReqComplexity	pwReqComplexity	Ajouter à la section Configuration personnalisée.
pwReqHistory	pwReqHistory	Ajouter à la section Configuration personnalisée.
pwReqLength	pwReqLength	Ajouter à la section Configuration personnalisée.
pwReqMinimumPasswordAge	pwReqMinAge	Ajouter à la section Configuration personnalisée.
pwReqText	pwReqText	Ajouter à la section Configuration personnalisée. Fournir une chaîne de texte à afficher plutôt qu'un chemin vers un fichier RTF.
syncLocalPassword	syncLocalPassword	Ajouter à la section Configuration personnalisée.

Remarque : certaines Preference Keys de votre profil de configuration Enterprise Connect ne sont peut-être pas mentionnées ici. Il se peut qu'elles renvoient à des fonctionnalités qui ne sont plus prises en charge ou ne sont plus nécessaires dans l'extension pour l'authentification unique Kerberos.

Désinstallation d'Enterprise Connect

L'exécution concomitante de l'extension pour l'authentification unique Kerberos et d'Enterprise Connect sur le même ordinateur n'est pas prise en charge. Après avoir effectué la transition vers l'extension pour l'authentification unique Kerberos, désinstallez Enterprise Connect. Vous aurez besoin de droits d'administrateur pour effectuer la désinstallation. Pour désinstaller Enterprise Connect, suivez les étapes ci-dessous :

Enterprise Connect 2.0 (et versions ultérieures)

1. Déchargez l'agent Enterprise Connect en lançant l'app Terminal et exécutant « launchctl unload /Library/LaunchAgents/com.apple.ecAgent » en tant qu'utilisateur actuellement connecté.
2. Quittez le menu supplémentaire d'Enterprise Connect en lançant l'app Terminal et en saisissant « killall Enterprise\ Connect\ Menu » dans l'app Terminal.
3. Supprimez l'app Enterprise Connect du dossier Applications.
4. Supprimez la liste de propriétés Enterprise Connect launchd .plist de /Library/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 (et versions antérieures)

1. Quittez Enterprise Connect en saisissant « killall Enterprise\ Connect » dans l'app Terminal.
2. Supprimez l'app Enterprise Connect du dossier Applications.

Vous trouverez, en annexe, un exemple de script permettant de supprimer n'importe quelle version d'Enterprise Connect.

Déclencheurs de scripts Enterprise Connect

Enterprise Connect peut exécuter des scripts lorsque surviennent certains événements : par exemple, à l'issue de son processus de connexion ou lorsque l'utilisateur effectue un changement de mot de passe. L'extension pour l'authentification unique Kerberos gère les scripts différemment d'Entreprise Connect. Elle n'exécute pas directement les scripts. Dès que survient un événement, elle publie une notification distribuée, qu'un autre processus peut capter, avant d'exécuter un script. Pour plus de détails, consultez la section « Fonctions avancées » de ce document.

Déclencheurs de scripts Enterprise Connect et leurs équivalents sous forme de notifications distribuées dans l'extension pour l'authentification unique Kerberos :

Enterprise Connect	Extension pour l'authentification unique Kerberos
auditScriptPath	com.apple.KerberosPlugin.InternalNetworkAvailable
connectionCompletedScriptPath	com.apple.KerberosPlugin.ConnectionCompleted
passwordChangeScriptPath	com.apple.KerberosPlugin.ADPasswordChanged

Partages réseau

L'extension pour l'authentification unique Kerberos ne prend pas en charge la gestion des partages réseau, comme le dossier de départ réseau de l'utilisateur. Cette fonctionnalité peut être remplacée en grande partie par des scripts.

Annexe

Profil de gestion des appareils : ExtensibleSingleSignOnKerberos

developer.apple.com/documentation/devicemanagement/extensiblesinglesignonkerberos?language=objc

Documentation de référence pour le protocole de gestion des appareils mobiles

developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf

Profil de gestion des appareils : ExtensibleSingleSignOnKerberos.ExtensionData

developer.apple.com/documentation/devicemanagement/extensiblesinglesignonkerberos/extensiondata?language=objc

Exemple de script – Traitement des notifications distribuées

L'extension pour l'authentification unique Kerberos publie toute une variété de notifications distribuées dès que surviennent différents événements : par exemple, lorsque l'utilisateur change de mot de passe ou que le réseau d'entreprise est mis en ligne. En tant qu'administrateur, vous pouvez utiliser un script ou une app pour guetter ces notifications et entreprendre des actions une fois qu'elles ont été publiées, comme exécuter un script ou une commande shell.

Voici un exemple de script capable d'exécuter des scripts ou des commandes lorsque sont publiées des notifications. Il doit être exécuté comme LaunchAgent pour s'exécuter en tant qu'utilisateur connecté ou comme LaunchDaemon pour s'exécuter en tant que racine. Le script comprend obligatoirement les deux paramètres suivants :

- **-notification** est le nom de la notification distribuée dont vous voulez être à l'écoute. Vous trouverez des exemples en page 11.
- **-action** est l'action que vous voulez exécuter lorsque la notification distribuée est publiée. Par exemple : « sh /path/to/script.sh ».

Pour exécuter le script, vous devez installer les outils de ligne de commande destinés aux développeurs. Un programme d'installation de ces outils est à votre disposition sur le site Apple Developer.

```
#!/usr/bin/swift

import Foundation

class NotifyHandler {

    // Action we want to run, like a shell command or a script
    public var action = String()

    // Runs every time we receive the specified distributed
    // notification
    @objc func gotNotification(notification: NSNotification){
        let task = Process()
        task.launchPath = "/bin/zsh"
        task.arguments = ["-c", action]
        task.launch()
    }
}

// MAIN

let scriptPath: String = CommandLine.arguments.first!

// -notification is the name of the notification you are listening for
guard let notification = UserDefaults.standard.string(forKey: "notification") else {
    print("\(scriptPath): No notification passed, exiting…")
    exit(1)
}
```

```
// -action is the action you want to run. This can be a shell

// command, script, etc.
guard let action = UserDefaults.standard.string(forKey: "action") else {
    print("\(scriptPath): No action passed, exiting…")
    exit(1)
}

let nh = NotifyHandler()
nh.action = action

print("Action is \(nh.action) and notification is \(notification)")

// Listen for the specified notification
DistributedNotificationCenter.default().addObserver(
    nh,
    selector: #selector(nh.gotNotification),
    name: NSNotification.Name(rawValue: notification),
    object: action)

RunLoop.main.run()
```

Exemple de script – Désinstallation d'Enterprise Connect

Cet exemple de script permet de supprimer n'importe quelle version d'Enterprise Connect. Exécutez-le depuis une solution de gestion des Mac ou de façon manuelle. Le script doit être exécuté avec les privilèges de racine.

```
#!/bin/zsh

# Unload the Kerberos helper from versions of EC prior to 1.6
if [[ -e /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist ]]; then
  launchctl bootout system /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist
  rm /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist
fi

# Remove the privileged helper from versions of EC prior to 1.6
if [[ -e /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper ]]; then
  rm /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper
fi

# Remove the authorization db entry from versions of EC prior to 1.6
/usr/bin/security authorizationdb read com.apple.Enterprise-Connect.writeKDCs > /dev/null

if [[ $? -eq 0 ]]; then
  security authorizationdb remove com.apple.Enterprise-Connect.writeKDCs
fi

if [[ -e /Library/LaunchAgents/com.apple.ecAgent.plist ]]; then
  # Enterprise Connect 2.0 or greater is installed
  # Unload ecAgent for logged in user and remove from launchd

  loggedInUser=$(scutil <<< "show State:/Users/ConsoleUser" | awk '/Name :/ && ! /loginwindow/ { print $3 }')
  loggedInUID=$(id -u $loggedInUser)

  launchctl bootout gui/$loggedInUID /Library/LaunchAgents/com.apple.ecAgent.plist
  rm /Library/LaunchAgents/com.apple.ecAgent.plist

  # Quit the menu extra
  killall "Enterprise Connect Menu"
fi

# Finally, remove the Enterprise Connect app bundle
rm -rf /Applications/Enterprise\ Connect.app
```