Gérer et sécuriser les mots de passe des comptes administrateurs macOS

Référence Agnosys	SE/GSPM
Durée	1 jour
Certification	Non
Support de cours	En français et en anglais

Description

Dans un contexte où la sécurité des systèmes informatiques est une priorité absolue, la gestion des mots de passe des comptes administrateurs locaux sur les Mac représente un enjeu crucial pour les équipes IT. Une solution LAPS permet de faire tourner des mots de passe uniques et générés aléatoirement, garantissant ainsi une sécurité renforcée en réduisant le risque d'attaques liées à l'utilisation de mots de passe statiques et partagés entre les Mac. Au cours de cette formation, nous explorerons les bonnes pratiques pour sécuriser les mots de passe des comptes administrateurs locaux et mettrons en œuvre la solution EasyLAPS, qui permet de stocker les mots de passe en rotation dans une solution de gestion des appareils mobiles (MDM).

Pour permettre aux participants d'appliquer immédiatement les connaissances acquises pendant la formation au sein de leur organisation, les participants se verront remettre une licence EasyLAPS Essential d'une durée d'un an (support sans engagement via le canal dédié #easylaps sur le Mac Admins Slack).

Objectifs

• Découvrir les enjeux liés à la gestion des mots de passe des comptes administrateurs locaux
• Analyser l'impact de la rotation régulière des mots de passe sur la sécurité globale de macOS
• Définir la règle de complexité des mots de passe et la méthode de stockage dans la solution MDM
• Configurer et déployer EasyLAPS sur les Mac de l'organisation
• Intégrer EasyLAPS avec les plateformes de collaboration en équipe Slack et Microsoft Teams
• Diagnostiquer et résoudre les problèmes techniques pouvant survenir lors de l'utilisation d'EasyLAPS

Qui peut s’inscrire ?

Cette formation s'adresse aux responsables de la conformité qui veillent à ce que les pratiques de gestion des mots de passe respectent les normes de sécurité et les réglementations en vigueur, ainsi qu'aux administrateurs système chargés de la gestion quotidienne des systèmes macOS. Elle est également destinée aux techniciens support qui résolvent les problèmes liés à la gestion des mots de passe et aux outils de sécurité.

Pré-requis

Pour s'inscrire à cette formation, les participants doivent :
- participer activement à des projets de mise en conformité des systèmes macOS
- administrer ou supporter macOS au quotidien
- maîtriser le déploiement de profils de configuration et de paquets sur des Mac depuis la solution MDM de l'organisation.

La solution EasyLAPS est compatible avec les solutions MDM indiquées sur cette page : https://www.agnosys.com/logiciels/easylaps-management-solutions-support/

Les participants doivent s'assurer que les règles de sécurité de leur organisation autorisent les appels API entre les Mac gérés et la solution MDM, étant entendu que tous les comptes locaux doivent être des comptes standards, à l'exception du compte administrateur dont le mot de passe est mis en rotation.

Participants et matériels sous la responsabilité d'Agnosys

Cette formation est limitée à huit participants maximum.

À l'issue d'une inscription confirmée, le formateur entrera en contact avec les participants pour déterminer la solution MDM utilisée dans leur organisation. La classe sera dotée des solutions MDMs ainsi définies (sous réserve que leurs éditeurs continuent de mettre à disposition des instances permettant de réaliser des démonstrations le jour de la formation) et des Mac requis pour les démonstrations réalisées par le formateur.

Par ailleurs, chaque participant accédera à une solution MDM Mosyle Business pour la réalisation des exercices.

Matériels sous la responsabilité exclusive des participants

Chacun des participants devra être équipé sous sa responsabilité d'un Mac de test :
- équipé de la version la plus récente disponible du système d'exploitation macOS
- configuré avec un compte administrateur local supplémentaire qui ne soit pas le compte administrateur dont le mot de passe sera mis en rotation
- non inscrit dans une solution MDM
- non équipé d'une solution de sécurité interdisant un accès complet à Internet.

Ce Mac de test doit accéder à Internet via un réseau Wi-Fi basique avec authentification WPA/WPA2/WPA3.

Sujets traités

Introduction à la gestion des mots de passe des comptes administrateurs locaux

– Création d'un compte administrateur local via l'inscription automatisée des appareils
– Élévation de privilèges depuis un compte administrateur local
– Attributs Open Directory d'un compte administrateur local
– Jeton sécurisé (Secure Token) et propriété du volume
– Statut cryptographique d'un compte administrateur local

Travaux pratiques :
– Préparation du Mac pour les exercices
– Accès à la console d'administration de Mosyle Business
– Inscription du Mac dans Mosyle Business
– Vérification du statut cryptographique des comptes locaux existants

Bonnes pratiques de gestion des mots de passe des comptes administrateurs locaux

– Résultat d'une véritable rotation du mot de passe (par opposition à une réinitialisation)
– Format du mot de passe : mot de passe ou phrase de passe
– Combien de temps pour trouver un mot de passe en 2024 selon sa complexité ?
– Règles de complexité et historique du mot de passe
– Déclaration d'un profil de configuration pour la sécurisation des mots de passe

Travaux pratiques :
– Création et distribution d'un profil de configuration de type mots de passe
– Vérification des réglages imposés par le profil de configuration

Configuration d'EasyLAPS

– Vue d'ensemble des ressources fournies, à créer et à déployer
– Les différentes étapes de l'implémentation
– Les logiques de stockage du mot de passe dans la solution MDM
– Obtention des outils tiers requis
– Installation de EasyLAPS Toolkit
– Création des clés de chiffrement
– Édition d'un fichier de configuration conformément au Dictionnaire
– Définition du format et de la règle de complexité des mots de passe uniques
– Génération des informations d'authentification API dans la solution MDM

Travaux pratiques :
– Téléchargement et installation des outils tiers requis
– Téléchargement de EasyLAPS Toolkit et EasyLAPS Core
– Installation de EasyLAPS Toolkit
– Création des clés de chiffrement
– Édition d'un fichier de configuration pour une implémentation avec Mosyle Business

Déploiement d'EasyLAPS

– Conversion des fichiers de configuration en profils de configuration personnalisés
– Les cas particuliers de Jamf Pro et de VMware Workspace ONE
– Construction du paquet EasyLAPS Content
– Références pour la signature du paquet selon la solution MDM utilisée
– Déclaration d'un profil de configuration pour prévenir la désactivation d'EasyLAPS
– Provisionnement de la solution MDM

Travaux pratiques :
– Conversion du fichier de configuration en profil de configuration personnalisé
– Construction du paquet EasyLAPS Content
– Création et distribution d'un profil de configuration de type Background Item Management
– Chargement et déploiement des ressources EasyLAPS

Exploitation d'EasyLAPS

– Observation d'une rotation de mot de passe réussie dans la solution MDM
– Déchiffrement d'un mot de passe stocké sous forme chiffrée dans la solution MDM
– Affichage du mot de passe depuis le Self Service de Jamf Pro
– Mise en œuvre de l'assistant cryptographique

Travaux pratiques :
– Visualisation du mot de passe en rotation dans la fiche d'inventaire du Mac
– Observation du fonctionnement de l'assistant cryptographique

Intégrations spécifiques

– Références pour la mise en œuvre des webhooks avec Slack et Microsoft Teams
– Configuration d'EasyLAPS pour l'envoi de webhooks
– Exploration de l'intégration Proxy
– Exploration des intégrations spécifiques avec FileWave, Jamf Pro, Microsoft Intune et VMware Workspace ONE

Travaux pratiques :
– Mise à jour de la configuration d'EasyLAPS pour l'envoi de webhooks via Microsoft Teams
– Observation des webhooks reçus dans Microsoft Teams

Maintenance d'EasyLAPS

– Renouvellement de la licence du produit
– Références pour la mise à jour du produit
– Consultation du fichier de suivi
– Activation manuelle ou automatisée des fonctions de journalisation
– Affichage des journaux d'activité
– Exécution manuelle d'une rotation
– Exploration de la matrice des erreurs
– Collecte du mot de passe pour des développements internes

Travaux pratiques :
– Identification des éléments à copier d'un précédent EasyLAPS Toolkit vers un nouvel EasyLAPS Toolkit
– Activation manuelle de la journalisation de type débogage verbeux
– Consultation des journaux de débogage verbeux
– Exécution manuelle d'EasyLAPS avec les différentes options disponibles en CLI
– Collecte du mot de passe en CLI
– Inscription au canal dédié #easylaps sur le Mac Admins Slack

Consultants Network

jamf SERVICES Partner

01 64 53 25 25 www.agnosys.com contact@agnosys.fr