Accès à distance VPN IKE/SSL ASA - Échéance et modification de mot de passe exemple pour de RAYON, TACACS, et de LDAP configuration

Contenu

Introduction

Ce document décrit les caractéristiques de modification d'échéance de mot de passe et de mot de passe sur un tunnel VPN d'Accès à distance terminé sur une appliance de sécurité adaptable Cisco (ASA). Les couvertures de document :

- Différents clients : Mobilité sécurisée de Client VPN Cisco et de Cisco AnyConnect
- Différents protocoles : TACACS, RAYON, et Protocole LDAP (Lightweight Directory Access Protocol)
- Différentes mémoires sur le Système de contrôle d'accès sécurisé Cisco (ACS) : gens du pays et Répertoire actif (AD)

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la configuration ASA par l'interface de ligne de commande (CLI)
- Connaissance de base de configuration du VPN sur une ASA
- Connaissance de base du Cisco Secure ACS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité adaptable Cisco, version 8.4 et ultérieures
- Microsoft Windows Server 2003 SP1
- Système de contrôle d'accès sécurisé Cisco, version 5.4 ou ultérieures
- Mobilité sécurisée de Cisco AnyConnect, version 3.1
- Client VPN Cisco, version 5

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

> Remarques :
>
> Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

ASA avec l'authentification locale

Une ASA avec les utilisateurs localement définis ne permet pas l'utilisation des caractéristiques de modification d'expiration du mot de passe ou de mot de passe. Un serveur externe, tel que le RAYON, TACACS, LDAP, ou Windows NT, est prié.

ACS et utilisateurs locaux

ACS prend en charge l'échéance de mot de passe et la modification de mot de passe pour les

utilisateurs localement définis. Par exemple, vous pouvez forcer les utilisateurs de création récente pour changer leur mot de passe à leur prochaine procédure de connexion, ou vous pouvez désactiver un compte une date spécifique :

Vous pouvez configurer une politique de mot de passe pour tous les utilisateurs. Par exemple, après qu'un mot de passe expire, vous pouvez désactiver le compte utilisateur (bloc il sans capacité d'ouvrir une session), ou vous pouvez offrir l'option de changer le mot de passe :

les configurations d'Utilisateur-particularité ont la priorité au-dessus des paramètres généraux.

ACS-RÉSERVé-jamais-Expirer est un attribut interne pour l'identité de l'utilisateur.

Cet attribut est activé par l'utilisateur et peut être utilisé afin de désactiver l'échéance globale configurations de compte. Avec cette configuration, un compte n'est pas désactivé même si la stratégie globale indique qu'elle devrait être :

ACS et utilisateurs de Répertoire actif

ACS peut être configuré pour vérifier les utilisateurs dans une base de données d'AD. L'échéance et la modification de mot de passe est prise en charge quand la version 2 (MSCHAPv2) de Microsoft Challenge Handshake Authentication Protocol est utilisée ; voir le guide utilisateur pour le Système de contrôle d'accès sécurisé Cisco 5.4 : Authentification dans ACS 5.4 : L'authentification Protocol et l'identité enregistrent la compatibilité pour des détails.

Sur une ASA, vous pouvez utiliser la caractéristique de gestion des mots de passe, comme décrit dans la section suivante, afin de forcer l'ASA pour utiliser MSCHAPv2.

ACS utilise l'appel de Distributed Computing Environment/protocole RPC de Protocole CIFS (Common Internet File System) (DCE/RPC) quand il entre en contact avec le répertoire du contrôleur de domaine (C.C) afin de changer le mot de passe :

L'ASA peut employer les protocoles de RAYON et TACACS+ afin d'entrer en contact avec l'ACS pour une modification de mot de passe d'AD.

ASA avec ACS par l'intermédiaire du RAYON

Le protocole RADIUS ne prend en charge pas à la façon des indigènes la modification d'échéance de mot de passe ou de mot de passe. Typiquement, le Password Authentication Protocol (PAP) est utilisé pour le RAYON. L'ASA envoie le nom d'utilisateur et mot de passe en texte brut, et le mot de passe est alors chiffré par l'utilisation du secret partagé par RAYON.

Dans un scénario typique quand le mot de passe utilisateur a expiré, ACS renvoie un message de Rayon-anomalie à l'ASA. ACS note cela :

Pour l'ASA, c'est un message simple de Rayon-anomalie, et l'authentification échoue.

Pour résoudre ce problème, l'ASA permet l'utilisation de l'ordre de **gestion des mots de passe** sous la configuration de groupe de tunnels :

```
tunnel-group RA general-attributes
 authentication-server-group ACS
```

```
password-management
```

L'ordre de **gestion des mots de passe** change le comportement de sorte que l'ASA soit forcée pour utiliser MSCHAPv2, plutôt que le PAP, dans la demande RADIUS.

L'échéance de mot de passe de supports du protocole MSCHAPv2 et le mot de passe changent. Ainsi, si un utilisateur VPN a débarqué à ce groupe de tunnels spécifique pendant la phase de Xauth, la demande RADIUS de l'ASA inclut maintenant un Ms-CHAP-défi :

Si ACS note que les besoins de l'utilisateur de changer le mot de passe, il renvoie un message de Rayon-anomalie avec MSCHAPv2 l'erreur 648.

L'ASA comprend ce message et emploie MODE_CFG afin de demander le nouveau mot de passe du Client VPN Cisco :

```
Oct 02 06:22:26 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received Password Expiration from Auth server!
```

Le Client VPN Cisco présente une boîte de dialogue qui incite pour un nouveau mot de passe :

L'ASA envoie une autre demande RADIUS avec une charge utile MS-CHAP-CPW et Ms-CHAP-NT-P.J.-picowatt (le nouveau mot de passe) :

L'ACS confirme la demande et renvoie un Rayon-recevoir avec MS-CHAP2-Success :

Ceci peut être vérifié sur ACS, qui signale un successfully '24204 changé par mot de passe :

L'ASA alors signale l'authentification réussie et continue le processus rapide du mode (QM) :

```
Oct 02 06:22:28 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

ASA avec ACS par l'intermédiaire de TACACS+

De même, TACACS+ peut être utilisé pour l'échéance et la modification de mot de passe. La caractéristique de gestion des mots de passe n'est pas nécessaire, parce que l'ASA utilise toujours TACACS+ avec un type d'authentification d'ASCII au lieu de MSCHAPv2.

Des plusieurs paquets sont permutés, et ACS demande un nouveau mot de passe :

Le Client VPN Cisco présente à une boîte de dialogue (qui diffère du dialogue utilisé par le RAYON) cette des demandes pour un nouveau mot de passe :

ACS demande la confirmation du nouveau mot de passe :

Le présent de Client VPN Cisco une case de confirmation :

Si la confirmation est correcte, ACS signale une authentification réussie :

ACS se connecte alors un événement que le mot de passe a été changé avec succès :

L'ASA met au point l'exposition le processus complet de l'échange et de l'authentification réussie :

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
```

```
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes.
Oct 02 07:44:41 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

Que la modification de mot de passe est complètement transparente pour l'ASA. C'est juste un peu plus long la session TACACS+ avec plus de demande et de paquets de réponse, qui sont analysés par le client vpn et présentés à l'utilisateur qui change le mot de passe.

ASA avec le LDAP

L'échéance et la modification de mot de passe sont entièrement prises en charge par l'AD de Microsoft et exposent au soleil le schéma de serveur LDAP.

Pour une modification de mot de passe, bindresponse = invalidCredentials » du retour de serveurs le « avec la 'erreur = cette erreur 773.' indique que l'utilisateur doit remettre à l'état initial le mot de passe. Codes d'erreur typiques incluent :

Code d'erreur	Erreur
525	Utilisateur non trouvé
52e	Qualifications non valides
530	Non laissé ouvrir une session à ce moment
531	Non laissé ouvrir une session à ce poste de travail
532	Le mot de passe a expiré
533	Compte désactivé
701	Le compte a expiré
773	L'utilisateur doit remettre à l'état initial le mot de passe
775	Compte utilisateur verrouillé

Configurez le serveur LDAP :

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.48.66.128
 ldap-base-dn CN=USers,DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
 server-type microsoft
```

Utilisez cette configuration pour le groupe de tunnels et la caractéristique de gestion des mots de passe :

```
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group LDAP
 default-group-policy MY
 password-management
```

Configurez l'utilisateur d'AD ainsi une modification de mot de passe est exigée :

Quand les essais d'utilisateur pour utiliser le Client VPN Cisco, l'ASA signale un mot de passe incorrect :

```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[111] Session Start
[111] New request Session, context 0xbd835c10, reqType = Authentication
[111] Fiber started
[111] Creating LDAP context with uri=ldap://10.48.66.128:389
[111] Connect to LDAP server: ldap://10.48.66.128:389, status = Successful
[111] supportedLDAPVersion: value = 3
[111] supportedLDAPVersion: value = 2
[111] Binding as Administrator
[111] Performing Simple authentication for Administrator to 10.48.66.128
[111] LDAP Search:
       Base DN = [CN=USers,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[111] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[111] Talking to Active Directory server 10.48.66.128
[111] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[111] Read bad password count 2
[111] Binding as cisco-test
[111] Performing Simple authentication for cisco-test to 10.48.66.128
[111] Simple authentication for cisco-test returned code (49) Invalid
credentials
[111] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 773, vece
[111] Invalid password for cisco-test
```

Si les qualifications sont non valides, l'erreur 52e apparaît :

```
[110] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 52e, vece
```

Le Client VPN Cisco demande alors une modification de mot de passe :

Cette boîte de dialogue diffère du dialogue utilisé par TACACS ou RAYON parce qu'elle affiche la stratégie. Dans cet exemple, la stratégie est une longueur du mot de passe minimum de sept caractères.

Une fois que l'utilisateur change le mot de passe, l'ASA pourrait recevoir ce message d'échec du serveur LDAP :

```
[113] Modify Password for cisco-test successfully converted password to unicode
[113] modify failed, no SSL enabled on connection
```

La stratégie de Microsoft exige l'utilisation de Secure Sockets Layer (SSL) pour la modification de mot de passe. Changez la configuration :

```
aaa-server LDAP (outside) host 10.48.66.128
 ldap-over-ssl enable
```

LDAP de Microsoft pour le SSL

Par défaut, le LDAP de Microsoft au-dessus du SSL ne fonctionne pas. Afin d'activer cette fonction, vous devez installer le certificat pour le compte d'ordinateur avec l'extension principale correcte. Voyez comment activer le LDAP au-dessus du SSL avec une tiers autorité de certification pour plus de détails.

Le certificat peut même être un certificat auto-signé parce que l'ASA ne vérifie pas le certificat de LDAP. Voir l'ID de bogue Cisco CSCui40212, « permettent à l'ASA pour valider le certificat du serveur de LDAP, » pour une demande d'amélioration relative.

> Remarque: ACS vérifie le certificat de LDAP dans la version 5.5 et ultérieures.

Pour installer le certificat, ouvrez la console MMC, sélectionnez l'**ajout/suppression SNAP-dans**, ajoutez le certificat, et choisissez le **compte d'ordinateur** :

L'ordinateur local choisi, importent le certificat à la mémoire personnelle, et déplacent le certificat associé d'Autorité de certification (CA) à la mémoire de confiance. Vérifiez que le certificat est de confiance :

Il y a une bogue dans la version 8.4.2 ASA, où cette erreur pourrait être retournée quand vous essayez d'utiliser le LDAP au-dessus du SSL :

```
ASA(config)# debug ldap 255

[142] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[142] supportedLDAPVersion: value = 3
[142] supportedLDAPVersion: value = 2
[142] Binding as Administrator
[142] Performing Simple authentication for Administrator to 10.48.66.128
[142] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=Administrator]
       Scope   = [SUBTREE]
[142] Request for Administrator returned code (-1) Can't contact LDAP server
```

La version 9.1.3 ASA fonctionne correctement avec la même configuration. Il y a deux sessions de LDAP. La première session renvoie une panne avec le code 773 (le mot de passe a expiré), alors que la deuxième session est utilisée pour la modification de mot de passe :

```
[53] Session Start
[53] New request Session, context 0xadebe3d4, reqType = Modify Password
[53] Fiber started
[53] Creating LDAP context with uri=ldaps://10.48.66.128:636
[53] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] Binding as Administrator
[53] Performing Simple authentication for Administrator to 10.48.66.128
[53] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[53] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[53] Talking to Active Directory server 10.48.66.128
[53] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[53] Read bad password count 0
[53] Change Password for cisco-test successfully converted old password to
unicode
[53] Change Password for cisco-test successfully converted new password to
unicode
[53] Password for cisco-test successfully changed
[53] Retrieved User Attributes:

<....most attributes details ommitted for clarity>
```

```
accountExpires: value = 130256568000000000 <----- 100ns intervals since
January 1, 1601 (UTC)
```
Pour vérifier la modification de mot de passe, regardez les paquets. La clé privée du serveur LDAP peut être utilisée par Wireshark afin de déchiffrer le trafic SSL :

L'Échange de clés Internet (IKE) /Authentication, l'autorisation, et la comptabilité (AAA) met au point sur l'ASA sont très semblables à ceux présentés dans le scénario d'authentification de RAYON.

LDAP et avertissement avant expiration

Pour le LDAP, vous pouvez utiliser une caractéristique qui envoie un avertissement avant qu'un mot de passe expire. L'ASA avertit l'utilisateur pendant 90 jours avant l'expiration du mot de passe avec cette configuration :

```
tunnel-group RA general-attributes
 password-management password-expire-in-days 90
```
Ici le mot de passe expire dans 42 jours, et les essais d'utilisateur pour ouvrir une session :

```
ASA# debug ldap 255
<some outputs removed for clarity>

[84] Binding as test-cisco
[84] Performing Simple authentication for test-cisco to 10.48.66.128
[84] Processing LDAP response for user test-cisco
[84] Message (test-cisco):
[84] Checking password policy
[84] Authentication successful for test-cisco to 10.48.66.128
[84] now: Fri, 04 Oct 2013 09:41:55 GMT, lastset: Fri, 04 Oct 2013 09:07:23
GMT, delta=2072, maxage=1244139139 secs
[84] expire in: 3708780 secs, 42 days
[84] Password expires Sat, 16 Nov 2013 07:54:55 GMT
[84] Password expiring in 42 day(s),threshold 90 days
```
L'ASA envoie un avertissement et offre l'option pour une modification de mot de passe :

Si l'utilisateur choisit de changer le mot de passe, il y a une demande pour un nouveau mot de passe, et la procédure normale de modification de mot de passe commence.

ASA et L2TP

Les exemples précédents ont présenté la version 1 (IKEv1) d'IKE et un IPSec VPN.

Pour le Layer 2 Tunneling Protocol (L2TP) et IPSec, le PPP est utilisé comme transport pour l'authentification. MSCHAPv2 est exigé au lieu du PAP pour une modification de mot de passe au travail :

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```
Pour l'authentification étendue dans L2TP à l'intérieur de la session PPP, MSCHAPv2 est négocié :

Quand le mot de passe utilisateur a expiré, une panne avec le code 648 est retournée :

Une modification de mot de passe est nécessaire alors. Le reste du processus est très semblable au scénario pour le RAYON avec MSCHAPv2.

Voir le L2TP au-dessus d'IPsec entre PC et PIX/ASA 7.2 de Windows 2000/XP utilisant l'exemple principal pré-partagé de configuration pour des détails supplémentaires sur la façon dont configurer L2TP.

Client de VPN SSL ASA

Les exemples précédents se sont rapportés à IKEv1 et au Client VPN Cisco, qui est la fin de vie (EOL).

La solution recommandée pour un Accès à distance VPN est une mobilité sécurisée de Cisco AnyConnect, qui utilise la version 2 (IKEv2) d'IKE et des protocoles SSL. La modification et l'échéance caractéristiques de mot de passe fonctionnent exactement la même chose pour le Cisco AnyConnect qu'elles ont fait pour le Client VPN Cisco.

Pour IKEv1, le changement et l'échéance données de mot de passe ont été permutés entre l'ASA et le client vpn de la phase 1.5 (config de Xauth/mode).

Pour IKEv2, il est semblable ; le mode de config utilise des paquets CFG_REQUEST/CFG_REPLY.

Pour le SSL, les données sont en session du Transport Layer Security de datagramme de contrôle (DTLS).

La configuration est identique pour l'ASA.

C'est un exemple de configuration avec le Cisco AnyConnect et le protocole SSL avec un serveur LDAP au-dessus de SSL :

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host win2003-mga.test-cisco.com
 ldap-base-dn CN=Users,DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
 ldap-over-ssl enable
 server-type microsoft

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy MY internal
group-policy MY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group LDAP
 default-group-policy MY
```

```
 password-management
tunnel-group RA webvpn-attributes
 group-alias RA enable
 without-csd

ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0
```

Une fois le mot de passe correct (qui a expiré) est fourni, essai de Cisco AnyConnect pour se connecter et demande un nouveau mot de passe :

Les logs indiquent que des identifiants utilisateurs ont été écrits deux fois :

Des logs plus détaillés sont disponibles dans l'outil de génération de rapports diagnostique d'AnyConnect (DART).

Portail web SSL ASA

Le même processus de procédure de connexion se produit dans le portail web :

La mêmes expiration du mot de passe et processus de modification se produit :

Change Password d'utilisateur ACS

S'il n'est pas possible de changer le mot de passe au-dessus du VPN, vous pouvez utiliser le service Web dédié du Change Password d'utilisateur ACS (UCP). Voir le guide du programmateur de logiciel pour le Système de contrôle d'accès sécurisé Cisco 5.4 : Utilisant les services Web UCP.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6 : Configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité
- Support et documentation techniques - Cisco Systems