Procédure de récupération de mot de passe pour le dispositif Cisco NAC (Cisco Clean Access)

Contenu

Introduction

Ce document décrit comment récupérer un mot de passe sur un gestionnaire de Cisco Clean Access (CAM) et le serveur de Cisco Clean Access (CAS).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Procédures pas à pas

L'appliance du Cisco Network Admission Control (NAC) contient ces mots de passe administratifs intégrés de compte utilisateur :

- Utilisateur de base d'ordinateur d'installation de Clean Access Manager
- Utilisateur de base d'ordinateur d'installation de Clean Access Server
- Utilisateur d'admin de console Web de Clean Access Server

- Utilisateur d'admin de console Web de Clean Access Manager

Les trois premiers mots de passe sont au commencement placés au temps d'installation (le mot de passe par défaut est cisco123). Afin de changer ces mots de passe à une date ultérieure, accédez à l'ordinateur de Clean Access Manager ou de Clean Access Server par SSH et procédure de connexion en tant qu'utilisateur dont le mot de passe vous voulez pour changer. Employez la commande de **passwd de** Linux afin de changer le mot de passe utilisateur. Afin de récupérer le mot de passe root pour Clean Access Manager/Clean Access Server, vous pouvez employer la procédure de Linux pour démarrer au mode de seul utilisateur et pour changer le mot de passe root.

La version 3.5.x et antérieures d'appareils NAC a utilisé LILO comme programme de démarrage. Les utilisations de version 3.6.x et ultérieures FOUILLENT car le programme de démarrage et par conséquent la procédure de récupération de mot de passe est différent. Ce sont les deux procédures différentes.

Version 3.5.x et antérieures d'appareils NAC

Procédez comme suit :

1. Connectez à l'ordinateur CAM/CAS par l'intermédiaire de la console.
2. Arrêt et redémarrage l'ordinateur afin d'afficher le mode GUI.
3. Presse **CTRL-x** afin de commuter au mode texte. Ceci affiche un `démarrage :` demande.
4. **Au Linux** prompt de type **simple** afin de démarrer l'ordinateur dans le mode de seul utilisateur.
5. **Le passwd de** type et appuient sur **entrent**.
6. Changez le mot de passe root et redémarrez l'ordinateur utilisant la commande de **réinitialisation**.**Remarque:** Il est important de fournir des mots de passe sécurisé pour les comptes utilisateurs dans le système d'appareils de Cisco NAC, et de les changer de temps en temps afin de mettre à jour la sécurité des systèmes. La suite n'impose pas généralement des normes pour les mots de passe que vous choisissez, mais on lui informe que vous utilisez des mots de passe fort. C'est-à-dire, mots de passe avec au moins six caractères, lettres et numéro mélangées, et ainsi de suite. Les mots de passe fort réduisent la probabilité d'un mot de passe réussi devinant l'attaque contre votre système.

Version 3.6.x et ultérieures d'appareils NAC

Procédez comme suit :

1. Mettez l'ordinateur, l'appliance NAC, ou le serveur sous tension.
2. Appuyez sur n'importe quelle touche quand l'écran de programme de démarrage semble avec la « presse n'importe quelle clé pour écrire le menu… » message afin d'écrire le menu de VER.Le menu de VER apparaît avec un élément dans la liste :Cisco Clean Access (2.6.11-perfigo)
3. Presse **e** afin d'éditer.Ces plusieurs choix apparaissent :`root (hd0,0)`
   ```
   kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 console=ttyS0,9600n8
   Initrd /initrd-2.6.11-perfigo.img
   ```

4. Défilement à la deuxième entrée (la ligne qui commence par le `noyau…`) et presse **e** afin d'éditer la ligne.
5. Supprimez **console=ttyS0,9600n8**, ajoutez le mot **simple à l'**extrémité de la ligne, et puis l'appuyez sur **entrent**.La ligne ressemble à cet exemple :`kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 single`
6. Appuyez sur **b** afin de démarrer l'ordinateur en mode de seul utilisateur.Vous êtes présenté avec une demande de shell de racine après amorce.**Remarque:** Vous n'êtes pas incité pour un mot de passe.
7. **Au passwd** prompt de type, appuyez sur **entrent**, et suivent les instructions.
8. Après que le mot de passe soit changé, écrivez la **réinitialisation** afin de redémarrer la case.

Reprise de mot de passe GUI de WEB de CAM

Créez un nouvel utilisateur

Il n'y a aucune procédure standard pour récupérer le mot de passe administrateur. La seule procédure disponible est pour le mot de passe root CLI.

1. Connectez au CLI et émettez ces commandes :`[root@cca-3390-cam ~]# psql -h 127.0.0.1 controlsmartdb -U postgres`
   `controlsmartdb=# select * from admin_account;`Vous devriez maintenant voir une liste d'utilisateurs, semblable à ceci :`id | name | password | group_name | enable | admin_desc`
   `----+------------+------------------------------------------+------------------+--------+-----------------------`
   `0 | admin | 96208ed2256706e8d8b29c1bf58d10c4a07267b4c1 | Full-Control Admin | 1 | Primary admin account`
   `1 | localadmin | b0f3e23dcd1046d1dbf4e095186d5cb54e47963690 | GuestLobby | 1 | only local users`
   `2 | admin1 | 96208ed225670d688bs29c1bf58d10c4a07267b4c1 | Full-Control Admin | 1 | admin test user`
   `(3 rows)`
2. Vous devez voir la valeur d'id la plus élevée et l'incrémenter (dans cet exemple, la nouvelle valeur est 3).
3. Insérez le nouvel utilisateur avec la commande :`insert into admin_account(id, name, password, group_name, enable)`
   `values ('3', 'recover', 'cisco123', 'Full-Control Admin', '1');`
4. Vérifiez si l'utilisateur de récupérer est dans le DB :`controlsmartdb=# select * from admin_account;`
   `id | name | password | group_name | enable | admin_desc`
   `----+------------+------------------------------------------+------------------+--------+-----------------------`
   `0 | admin | 96208ed225670688b29c1bf58d10c4a07267b4c1 | Full-Control Admin | 1 | Primary admin account`
   `1 | localadmin | b0f3e23dcd10461db4e095186d5cb54e47963690 | GuestLobby | 1 | only local users`
   `2 | admin1 | 96208ed225670688b29c1bf58d10c4a07267b4c1 | Full-Control Admin | 1 | admin test user`
   `3 | recover | cisco123 | Full-Control Admin | 1 |`
   `(4 rows)`
5. Ouvrez une session au GUI avec ce nouvel utilisateur.

Supprimez le compte d'admin

Utilisez la commande SQL De supprimer l'utilisateur d'admin.

1. Écrivez la ligne de commande SQL :`[root@cca-3390-cam ~]#  psql -h 127.0.0.1 controlsmartdb -U postgres`
2. Supprimez l'utilisateur d'admin (id=0).`controlsmartdb=# delete from admin_account where id='0';`
   `DELETE 1`
3. Vérifiez que l'id 0 a été supprimé.`controlsmartdb=# select * from admin_account;`
```
 id |    name    |                 password                 |
group_name     | enable |    admin_desc
----+------------+------------------------------------------+-------------------+--------
+------------------
  1 | localadmin | b0f3e23dcd10461db4e095186d5cb54e47963690 |
GuestLobby          |      1 | only local users
  2 | admin1     | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | admin test user
  3 | recover    | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 |
(3 rows
```
4. Vous pouvez maintenant créer un nouvel utilisateur de « admin » le '0' d'id.`controlsmartdb=# insert into admin_account(id,name,password,group_name,enable) values('0', 'admin', 'cisco123', 'Full-Control Admin', 1);`
```
INSERT 0 1
controlsmartdb=# select * from admin_account
controlsmartdb-# ;
 id |    name    |                 password                 |
group_name     | enable |    admin_desc
----+------------+------------------------------------------+-------------------+--------
+------------------
  1 | localadmin | b0f3e23dcd10461db4e095186d5cb54e47963690 |
GuestLobby          |      1 | only local users
  2 | admin1     | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | admin test user
  3 | recover    | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 |
  0 | admin      | cisco123                                 |
Full-Control Admin |      1 |
(4 rows)
```
5. Vérifiez si le nouvel utilisateur est dans le DB.

Informations connexes

- Documentation du produit d'appareils de Cisco NAC
- Support et documentation techniques - Cisco Systems