Configuration de CSU pour UNIX (Solaris)

Contenu

Introduction

Le Cisco Secure ACS pour le logiciel UNIX (CSU) aide à assurer la Sécurité du réseau et dépiste l'activité des personnes qui se connectent avec succès au réseau. Le CSU agit en tant que serveur TACACS+ ou de RAYON et emploie l'Authentification, autorisation et comptabilité (AAA) pour fournir la sécurité des réseaux.

Le CSU prend en charge ces options de base de données d'enregistrer le groupe et les profils utilisateurs et l'information de comptabilité :

- SQLAnywhere (inclus avec le CSU).Cette version de Sybase SQLAnywhere n'a pas le support de client/serveur. Cependant, il est optimisé pour assurer des services essentiels d'AAA avec le CSU.**Attention :** L'option de base de données SQLAnywhere ne prend en charge pas les bases de données de profil qui dépassent 5,000 utilisateurs, réplication des données de profil parmi la base de données situe, ou le Cisco Secure distribuent la caractéristique du gestionnaire de session (DSM).
- Oracle ou système de gestion de base de données relationnelle de Sybase (RDBMS).Pour prendre en charge les bases de données Cisco Secures de profil de 5,000 utilisateurs ou plus, réplication de base de données, ou la caractéristique Cisco Secure DSM, vous devez préinstaller un serveur d'Oracle (version 7.3.2, 7.3.3, ou 8.0.3) ou de Sybase SQL (version 11)

RDBMS pour tenir vos informations de profil Cisco Secures. La réplication de base de données exige davantage de configuration RDBMS après que l'installation Cisco Secure soit complète.
- La mise à jour d'une base de données existante d'une version (2.x) précédente de CSU.Si vous améliorez d'une version 2.x plus tôt de Cisco Secure, le programme d'installation Cisco Secure améliore automatiquement la base de données de profil pour être compatible avec CSU 2.3 pour l'UNIX.
- Importer une base de données existante de profil.Vous pouvez convertir le logiciel gratuit existant TACACS+ ou les bases de données ou les fichiers plats de profil RADIUS pour l'usage avec cette version du CSU.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Secure ACS 2.3 pour l'UNIX.

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.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration CSU

Employez ces procédures pour configurer le CSU.

Commencez l'interface Cisco Secure d'administrateur

Employez cette procédure pour ouvrir une session à l'administrateur Cisco Secure.

1. De n'importe quel poste de travail avec une connexion de Web à l'ACS, lancez votre navigateur Web.
2. Entrez dans un de ces URLs pour le site Web Cisco Secure d'administrateur :Si la caractéristique de couche de socket de Sécurité sur votre navigateur n'est pas activée, entrez :`http://your_server/cs`là où le your_server est le nom d'hôte (ou le nom de domaine complet (FQDN), si le nom d'hôte et le FQDN diffèrent) du SPARCstation où vous avez installé le CSU. Vous pouvez également substituer l'adresse IP du SPARCstation au your_server.Si la caractéristique de couche de socket de Sécurité sur votre navigateur est

activée, spécifiez les « https » plutôt que le « HTTP » comme protocole de transmission d'hypertexte. Entrez :`https://your_server/cs`là où le your_server est le nom d'hôte (ou le FQDN, si le nom d'hôte et le FQDN diffèrent) du SPARCstation où vous avez installé le CSU. Vous pouvez également substituer l'adresse IP du SPARCstation au your_server.**Remarque:** L'URLs et les noms du serveur distinguent les majuscules et minuscules. Ils doivent être tapés avec les lettres majuscules et minuscules exactement comme affichés.La page de connexion CSU est affichée.
3. Saisissez votre nom d'utilisateur et votre mot de passe. Cliquez sur **Submit**.**Remarque:** Le nom d'utilisateur d'initiale par défaut est « super utilisateur. » Le mot de passe d'initiale par défaut est « changeme. » Après votre procédure de connexion initiale, vous devez changer le nom d'utilisateur et mot de passe immédiatement pour la sécurité maximale.Après que vous ouvriez une session, la page principale CSU est affichée avec la barre de menu principal le long du dessus. La page de menu principal CSU est affichée seulement si l'utilisateur fournit un nom et un mot de passe qui ont des privilèges niveau de l'administrateur. Si l'utilisateur fournit un nom et un mot de passe qui ont seulement des privilèges de niveau utilisateur, alors un écran différent est affiché.

Commencez le programme de configuration avancée

Commencez le programme Cisco Secure basé sur Java de configuration avancée d'administrateur à partir des pages Web l'unes des d'administrateur CSU. De la barre de menus de l'interface web CSU, cliquez sur **avancé**, et puis cliquez sur **avancé** de nouveau.

Le programme Cisco Secure de configuration avancée d'administrateur est affiché. Il pourrait probablement prendre quelques minutes pour charger.

Créez un profil de groupe

Employez le programme Cisco Secure de configuration avancée d'administrateur pour créer et configurer des profils de groupe. Cisco recommande que vous créiez des profils de groupe pour configurer des conditions requises détaillées d'AAA pour un grand nombre d'utilisateurs semblables. Après que le profil de groupe soit défini, utilisez le CSU ajoutent une page Web d'utilisateur pour ajouter rapidement des profils utilisateurs au profil de groupe. Les conditions requises avancées configurées pour le groupe s'appliquent à chaque utilisateur de membre.

Employez cette procédure pour créer un profil de groupe.

1. Dans le programme Cisco Secure de configuration avancée d'administrateur, sélectionnez l'onglet de **membres**. Dans le volet de navigateur, retirez la case de **furetage**. Les nouveaux affichages d'icône de profil de création.
2. Dans le volet de navigateur, faites un de ces derniers :Pour créer un profil de groupe sans le parent, localisez et cliquez sur [l'icône du dossier de **racine**].Pour créer votre profil de groupe en tant qu'enfant d'un autre profil de groupe, localisez le groupe que vous voulez en tant que parent et cliquez sur le.Si le groupe qui vous voulez que soit le parent est un groupe enfants, cliquez sur le répertoire de son groupe parent pour l'afficher.
3. Le clic **créent le nouveau profil**. Les nouveaux affichages de boîte de dialogue de profil.
4. Sélectionnez la case de **groupe**, introduisez le nom du groupe que vous voulez créer, et cliquez sur OK. Les nouveaux affichages de groupe dans l'arborescence.
5. Après que vous créiez le profil de groupe, assignez TACACS+ ou attributs RADIUS pour

configurer les propriétés spécifiques d'AAA.

Créez un profil utilisateur dans le mode de configuration avancée

Employez le mode Cisco Secure de configuration avancée d'administrateur pour créer et configurer un profil utilisateur. Vous pouvez faire ceci pour personnaliser les attributs de l'autorisation du profil utilisateur et liés à la comptabilité plus en détail qu'est possible avec l'ajouter par page utilisateur.

Employez cette procédure pour créer un profil utilisateur :

1. Dans le programme Cisco Secure de configuration avancée d'administrateur, sélectionnez l'onglet de **membres**. Dans le volet de navigateur, situez et retirez **parcourent**. Les nouveaux affichages d'icône de profil de création.
2. Dans le volet de navigateur, faites un de ces derniers :Localisez et cliquez sur le groupe auquel l'utilisateur appartient.Si vous ne voulez pas que l'utilisateur appartienne à un groupe, cliquez sur [l'icône du dossier de **racine**].
3. Le clic **créent le profil**. Les nouveaux affichages de boîte de dialogue de profil.
4. Assurez-vous que la case de **groupe** est retirée.
5. Écrivez le nom d'utilisateur que vous voulez créer et cliquer sur OK. Les nouveaux affichages d'utilisateur dans l'arborescence.
6. Après que vous créiez le profil utilisateur, assignez la particularité TACACS+ ou les attributs RADIUS pour configurer les propriétés spécifiques d'AAA :Pour assigner des profils TACACS+ au profil utilisateur, voyez pour assigner des attributs TACACS+ à un profil de groupe ou d'utilisateur.Pour assigner des profils RADIUS au profil utilisateur, voyez pour assigner des attributs RADIUS à un profil de groupe ou d'utilisateur.

Stratégies pour appliquer des attributs

Employez la caractéristique de profil de groupe CSU et le TACACS+ et les attributs RADIUS pour implémenter l'authentification et l'autorisation des utilisateurs du réseau par le CSU.

Attributs de plan pour des groupes et des utilisateurs

La caractéristique de profil du groupe du CSU te permet de définir un ensemble commun de conditions requises d'AAA pour un grand nombre d'utilisateurs.

Vous pouvez assigner un ensemble de TACACS+ ou de valeurs d'attribut RADIUS à un profil de groupe. Ces valeurs d'attribut assignées au groupe s'appliquent à n'importe quel utilisateur qui est un membre ou qui est ajouté en tant que membre de ce groupe.

Utilisez la caractéristique de profil de groupe efficacement

Pour configurer le CSU pour gérer de grands nombres et divers types d'utilisateurs avec des conditions requises complexes d'AAA, Cisco recommande que vous employiez les caractéristiques du programme Cisco Secure de configuration avancée d'administrateur pour créer et configurer des profils de groupe.

Le profil de groupe doit contenir tous les attributs qui ne sont pas spécifiques à l'utilisateur. Ceci

signifie habituellement tous les attributs excepté le mot de passe. Vous pouvez alors employer l'ajouter une page utilisateur de l'administrateur Cisco Secure pour créer des profils utilisateurs simples avec des attributs de mot de passe et pour assigner ces profils utilisateurs au profil approprié de groupe. Les caractéristiques et les valeurs d'attribut définies pour un groupe particulier s'appliquent alors à ses utilisateurs de membre.

Groupes parents et groupes enfants

Vous pouvez créer une hiérarchie des groupes. Dans un profil de groupe, vous pouvez créer des profils de groupe enfants. Les valeurs d'attribut assignées au profil de groupe parent sont des valeurs par défaut pour les profils de groupe enfants.

Gestion de niveau du groupe

Un administrateur système Cisco Secure peut assigner l'état Cisco Secure individuel d'administrateur d'users group. Groupez les utilisateurs individuels d'enables d'état d'administrateur pour gérer tous les profils et profils utilisateurs de groupe enfants qui sont subalternes à leur groupe. Cependant, lui ne leur permet pas pour ne gérer aucun groupe ou les utilisateurs qui tombent en dehors de la hiérarchie de leur groupe. Ainsi, l'administrateur système partage la tâche de gérer un grand réseau à d'autres personnes sans accorder à chacun d'eux l'autorité égale.

Quels attributs est-ce que je définis pour des utilisateurs individuels ?

Cisco recommande que vous assigniez à des utilisateurs individuels les valeurs d'attribut d'authentification de base qui sont seules à l'utilisateur, tel que les attributs qui définissent le nom d'utilisateur, le mot de passe, le type de mot de passe, et le privilège de Web. Assignez les valeurs d'attribut d'authentification de base à vos utilisateurs par des CSU éditent un utilisateur ou ajoutent des pages utilisateur.

Quels attributs est-ce que je définis pour des profils de groupe ?

Cisco recommande que vous définissiez les attributs de qualification, d'autorisation, et liés à la comptabilité au niveau du groupe.

Dans cet exemple, le profil de groupe nommé des « utilisateurs en accès entrant » est assigné les paires de valeurs d'attribut Frame-Protocol=PPP et Service-Type=Framed.

Quels sont des attributs absolus ?

Un sous-ensemble du TACACS+ et des attributs RADIUS dans le CSU peut être assigné l'état absolu au niveau de profil de groupe. Une valeur d'attribut activée pour l'état absolu au niveau de profil de groupe ignore toutes les valeurs d'attribut contractuelles à un niveau de profil utilisateur de profil ou de membre de groupe enfants.

Dans les réseaux multiniveaux avec plusieurs niveaux des administrateurs de groupe, les attributs absolus permettent à un administrateur système de placer les valeurs d'attribut de groupe sélectionné qui groupent des administrateurs aux niveaux plus bas ne peuvent pas ignorer.

Attributs qui peuvent être assignés à affichage d'état absolu une case absolue dans la case

d'attributs du programme Cisco Secure de configuration avancée d'administrateur. Sélectionnez la case pour activer l'état absolu.

Les valeurs de valeurs d'attribut de groupe et d'attribut d'utilisateur peuvent-elles être en conflit ?

La résolution de conflits parmi des valeurs d'attribut a assigné aux profils de groupe parent, des profils de groupe enfants, et les profils utilisateurs de membre dépend de si les valeurs d'attribut sont absolues et si elles sont TACACS+ ou attributs RADIUS :

- TACACS+ ou valeurs d'attribut RADIUS assignées à un profil de groupe avec le dépassement absolu d'état toute valeur définie contractuelle d'attribut à un groupe enfants ou à un niveau de profil utilisateur.
- Si un état absolu de valeur d'attribut TACACS+ n'est pas activé au niveau de profil de groupe, il est ignoré par n'importe quelle valeur d'attribut contractuelle réglée à un groupe enfants ou à un niveau de profil utilisateur.
- Si un état absolu de valeur d'attribut RADIUS n'est pas activé au niveau de groupe parent, alors toute valeur définie contractuelle d'attribut à un résultat de groupe enfants dans des résultats imprévisibles. Quand vous définissez des valeurs d'attribut RADIUS pour un groupe et ses utilisateurs de membre, évitez d'assigner le même attribut à l'utilisateur et groupez les profils.

Utilisez l'interdiction et permettez les options

Pour TACACS+, ignorez la Disponibilité des valeurs héritées de service en préfixant le mot clé **interdisent** ou **autorisent à la** spécification de service. Le mot clé d'**autorisation** permet des services spécifiés. Le mot clé d'**interdiction** rejette des services spécifiés. Avec l'utilisation de ces mots clé ensemble, vous pouvez construire « tout excepté » des configurations. Par exemple, cette configuration permet l'accès de tous les services excepté le X.25 :

```
default service = permit
prohibit service = x25
```

Assignez les attributs TACACS+ à un profil de groupe ou d'utilisateur

Pour assigner des services spécifiques et des attributs TACACS+ à un profil de groupe ou d'utilisateur, suivez ces étapes :

1. Dans le programme Cisco Secure de configuration avancée d'administrateur, sélectionnez l'onglet de **membres**. Dans le volet de navigateur, cliquez sur l'icône pour le profil de groupe ou d'utilisateur auquel des attributs TACACS+ sont assignés.
2. S'il y a lieu, dans le volet de profil, cliquez sur l'icône de **profil** pour la développer.Une liste ou une boîte de dialogue qui contiennent des attributs applicables au profil ou au service sélectionné affiche dans la fenêtre au en bas à droite de l'écran. Les informations dans cette fenêtre changent basé sur quel profil ou entretenez-vous sélectionnent dans le volet de profil.
3. Cliquez sur le service ou le protocole que vous voulez pour ajouter et cliquer sur Apply. Le service est ajouté au profil.
4. Entrez dans ou sélectionnez le texte nécessaire dans la fenêtre d'attribut.Des entrées valides sont expliquées dans les stratégies pour appliquer la section d'attributs du CSU 2.3 pour le guide de référence UNIX.**Remarque:** Si vous assignez une valeur d'attribut au niveau de profil de groupe, et l'attribut que vous spécifiez des affichages une case **absolue**, choisie

cette case pour assigner l'état d'absolu de valeur. Un état absolu de valeur affectée ne peut pas n'être ignoré par aucune valeur contractuelle assignée aux niveaux subalternes de profil ou de profil utilisateur de groupe.
5. Répétez les étapes 1 pour chaque service supplémentaire ou protocole que vous devez ajouter.
6. Quand toutes les modifications sont apportées, cliquez sur Submit.

Assignez les attributs RADIUS à un profil de groupe ou d'utilisateur

Pour assigner des attributs RADIUS spécifiques à un profil de groupe ou d'utilisateur :

1. Assignez un dictionnaire de RAYON au profil de groupe :Àla page de membres du programme Cisco Secure de configuration avancée d'administrateur, cliquez sur l'icône de **groupe** ou d'**utilisateur**, puis cliquez sur l'icône de **profil** dans le volet de profils. Dans le volet d'attributs, les affichages de menu Options.Sur le **menu Options**, cliquez sur le nom du dictionnaire de RAYON que vous voulez que le groupe ou l'utilisateur l'utilise. (Par exemple, RAYON - Cisco.) Cliquez sur **Apply**.
2. Ajoutez les éléments requis de contrôle et répondez les attributs au profil RADIUS :**Remarque:** Les éléments de contrôle sont des attributs exigés pour l'authentification, telle que l'user-id et le mot de passe. Les attributs de réponse sont des attributs envoyés au serveur d'accès à distance (NAS) après que le profil ait passé la procédure d'authentification, telle que le protocole tramé. Pour des listes et des explications des éléments de contrôle et des attributs de réponse, référez-vous aux paires de valeurs d'attribut de RAYON et à la Gestion de dictionnaire dans le CSU 2.3 pour le guide de référence UNIX.Dans la fenêtre de profil, cliquez sur le RAYON - icône du dossier de dictionaryname. (Vous devez probablement cliquer sur le profil + le symbole pour développer le répertoire de RAYON.) Les éléments de contrôle et l'affichage d'options d'attributs de réponse dans la fenêtre de groupe d'attribut.Pour utiliser un ou plusieurs de ces attributs, cliquez sur les attributs que vous voulez utiliser, puis cliquez sur Apply. Vous pouvez ajouter plus d'un attribut à la fois.Cliquez sur **+** symbole pour le RAYON - dictionaryname pour développer le répertoire.**Remarque:** Si vous sélectionnez l'option RADIUS-Cisco11.3, assurez-vous que la version de logiciel 11.3.3(T) ou ultérieures de Cisco IOS® est installée sur votre NASs se connectant et ajoutez les nouvelles lignes de commande à vos configurations de NAS. Référez-vous à activer entièrement le dictionnaire RADIUS-Cisco11.3 dans le CSU 2.3 pour le guide de référence UNIX.
3. Spécifiez les valeurs pour les éléments ajoutés de contrôle et répondez les attributs :**Attention :** Pour le protocole RADIUS, l'héritage est additif par opposition à hiérarchique. (Le protocole TACACS+ utilise l'héritage hiérarchique). Par exemple, si vous assignez les mêmes attributs de réponse aux profils d'utilisateur et de groupe, l'autorisation échoue parce que le NAS reçoit deux fois le nombre d'attributs. Il ne semble pas raisonnable des attributs de réponse. N'assignez pas le même attribut d'élément ou de réponse de contrôle au groupe et aux profils utilisateurs.Cliquez sur les **éléments de contrôle** ou **répondez les attributs**, ou cliquez sur chacun des deux. Une liste d'éléments de contrôle et de valeurs d'attributs applicables de réponse apparaît dans la fenêtre droite inférieure. Cliquez sur **+** symbole pour développer le répertoire.Cliquez sur les valeurs que vous voulez assigner, puis cliquez sur Apply. Pour plus d'informations sur les valeurs, référez-vous aux paires de valeurs d'attribut de RAYON et à la Gestion de dictionnaire dans le CSU 2.3 pour le guide de référence UNIX.**Remarque:** Si vous assignez une valeur d'attribut au niveau de profil de groupe, et

l'attribut que vous spécifiez des affichages une case absolue, choisie cette case pour assigner l'état d'absolu de valeur. Un état absolu de valeur affectée ne peut pas n'être ignoré par aucune valeur contractuelle assignée aux niveaux subalternes de profil ou de profil utilisateur de groupe.Quand vous avez terminé apporter des modifications, cliquez sur Submit.

4. Pour utiliser un ou plusieurs de ces attributs, cliquez sur les attributs que vous voulez utiliser, puis cliquez sur Apply. Vous pouvez appliquer plus d'un attribut à la fois.

Assignez les niveaux de privilège de contrôle d'accès

L'administrateur de super utilisateur emploie l'attribut de privilège de Web pour assigner un niveau de privilège de contrôle d'accès aux utilisateurs Cisco Secures.

1. Dans le programme Cisco Secure de configuration avancée d'administrateur, cliquez sur l'utilisateur dont le privilège de contrôle d'accès vous voulez assigner, puis cliquez sur l'icône de profil dans le volet de profils.
2. Dans le menu Options, cliquez sur le **privilège de Web** et sélectionnez une de ces valeurs.**0** - Refuse à l'utilisateur tous les privilèges de contrôle d'accès qui incluent la capacité de changer le mot de passe Cisco Secure de l'utilisateur.**1** - Accorde l'accès client à la page Web de CSUser. Ceci permet aux utilisateurs Cisco Secures pour changer leurs mots de passe Cisco Secures. Pour des informations sur la façon changer des mots de passe, référez-vous aux fonctions de niveau utilisateur (changeant un mot de passe) en utilisateur simple et Gestion ACS.**12** - Accorde les privilèges d'administrateur de groupe d'utilisateurs.**15** - Accorde les privilèges d'administrateur système d'utilisateur.**Remarque:** Si vous sélectionnez n'importe quelle option de privilège de Web autre que 0, vous devez également spécifier un mot de passe. Pour répondre au critère d'utilisation d'un mot de passe de privilège de Web, un espace simple est d'une façon minimum acceptable.

Début et arrêt CSU

Habituellement, débuts CSU automatiquement quand vous commencez ou redémarrez le SPARCstation où il est installé. Cependant, vous pouvez commencer le CSU manuellement, ou le fermer sans arrêter le SPARCStation entier.

Procédure de connexion en tant que [racine] au SPARCStation où vous avez installé le CSU.

Pour commencer le CSU manuellement, type :

```
# /etc/rc2.d/S80CiscoSecure
```

Pour arrêter le CSU manuellement, type :

```
# /etc/rc0.d/K80CiscoSecure
```

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

- Cisco Secure ACS pour la page de support UNIX
- Page d'assistance TACACS+
- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems