Intégration de Security Manager à ACS

Contenu

Introduction

Ce document décrit comment intégrer Cisco Security Manager à Cisco Secure Access Control Server (ACS).

Cisco Secure ACS fournit une autorisation de commande aux utilisateurs qui utilisent des applications de gestion, telles que Cisco Security Manager, afin de configurer des périphériques réseau gérés. La prise en charge de l'autorisation de commande est fournie par des types de jeu d'autorisations de commande uniques, appelés rôles dans Cisco Security Manager, qui contiennent un ensemble d'autorisations. Ces autorisations, également appelées privilèges, déterminent les actions que les utilisateurs ayant des rôles particuliers peuvent effectuer dans Cisco Security Manager.

Cisco Secure ACS utilise TACACS+ pour communiquer avec les applications de gestion. Pour que Cisco Security Manager puisse communiquer avec Cisco Secure ACS, vous devez configurer le serveur CiscoWorks de Cisco Secure ACS en tant que client AAA utilisant TACACS+. En outre, vous devez fournir au serveur CiscoWorks le nom d'administrateur et le mot de passe que vous

utilisez pour vous connecter à Cisco Secure ACS. Lorsque vous remplissez ces conditions, il garantit la validité des communications entre Cisco Security Manager et Cisco Secure ACS.

Lorsque Cisco Security Manager communique initialement avec Cisco Secure ACS, il demande à Cisco ACS de créer des rôles par défaut, qui apparaissent dans la section Composants du profil partagé de l'interface HTML de Cisco Secure ACS. Il exige également un service personnalisé autorisé par TACACS+. Ce service personnalisé apparaît sur la page TACACS+ (Cisco IOS®) de la section Configuration de l'interface de l'interface HTML. Vous pouvez ensuite modifier les autorisations incluses dans chaque rôle Cisco Security Manager et appliquer ces rôles aux utilisateurs et aux groupes d'utilisateurs.

Remarque : Il n'est pas possible d'intégrer CSM à ACS 5.2 car il n'est pas pris en charge.

Conditions préalables

Conditions requises

Pour utiliser Cisco Secure ACS, assurez-vous que :

- Vous définissez des rôles qui incluent les commandes requises pour exécuter les fonctions nécessaires dans Cisco Security Manager.
- La restriction d'accès au réseau (NAR) inclut le groupe de périphériques (ou les périphériques) que vous souhaitez administrer, si vous appliquez une NAR au profil.
- Les noms des périphériques gérés sont orthographiés et mis en majuscules de manière identique dans Cisco Secure ACS et dans Cisco Security Manager.

Components Used

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

- Cisco Security Manager version 3.0
- Cisco Secure ACS version 3.3

Remarque : Veillez à choisir les versions CSM et ACS compatibles avant de procéder à l'installation sur votre environnement réseau. Par exemple, Cisco a testé ACS 3.3 avec uniquement CSM 3.0 et s'est arrêté pour les versions CSM ultérieures. Il est donc recommandé d'utiliser CSM 3.0 avec ACS 3.3. Reportez-vous au tableau Matrice de compatibilité pour plus d'informations sur les différentes versions de logiciels.

Versions de Cisco Security Manager	Versions CS ACS testées
3.0.0 3.0.0 SP1	Windows 3.3(3) et 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Solutions Engine 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Solutions Engine 4.0(1) Windows 4.1(1) et 4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	Solutions Engine v4.0(1) Windows 4.1(2), 4.1(3) et 4.1(4)
3.1.1 SP1	Solutions Engine 4.0(1) Windows

	4.1(4)
3.1.1 SP2	Solutions Engine 4.0(1) Windows 4.1(4) et 4.2(0)
3.2.0	Solutions Engine 4.1(4) Windows 4.1(4) et 4.2(0)
3.2.1	Solutions Engine 4.1(4) Windows 4.2(0)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Intégrer Cisco Security Manager à Cisco Secure ACS

Cette section décrit les étapes requises pour intégrer Cisco Security Manager à Cisco Secure ACS. Certaines étapes contiennent plusieurs étapes. Ces étapes et étapes doivent être effectuées dans l'ordre. Cette section contient également des références à des procédures spécifiques utilisées pour exécuter chaque étape.

Procédez comme suit :

1. **Planifiez votre modèle d'authentification et d'autorisation administrative.**Vous devez choisir votre modèle d'administration avant d'utiliser Cisco Security Manager. Cela inclut la définition des rôles et des comptes administratifs que vous prévoyez d'utiliser.**Conseil :** Lorsque vous définissez les rôles et les autorisations des administrateurs potentiels, déterminez également s'il faut activer ou non le workflow. Cette sélection affecte la manière dont vous pouvez restreindre l'accès.
2. **Installez Cisco Secure ACS, Cisco Security Manager et CiscoWorks Common Services.**Installez Cisco Secure ACS version 3.3 sur un serveur Windows 2000/2003. Installez CiscoWorks Common Services et Cisco Security Manager sur un autre serveur Windows 2000/Windows 2003.Référez-vous à ces documents pour plus d'informations :Guide d'installation de Cisco Security Manager 3.0Guide d'installation de Cisco Secure ACS pour Windows 3.3**Remarque :** Reportez-vous au tableau Matrice de compatibilité pour plus d'informations avant de choisir les versions logicielles CSM et ACS.
3. **Exécuter des procédures d'intégration dans Cisco Secure ACS.**Définissez les utilisateurs de Cisco Security Manager en tant qu'utilisateurs ACS et affectez-les à des groupes d'utilisateurs en fonction de leur rôle planifié, ajoutez tous vos périphériques gérés (ainsi que le serveur CiscoWorks/Security Manager) en tant que clients AAA et créez un utilisateur de contrôle d'administration. Reportez-vous à Procédures d'intégration exécutées dans Cisco Secure ACS pour plus d'informations.
4. **Exécuter des procédures d'intégration dans CiscoWorks Common Services.**Configurez un utilisateur local qui correspond à l'administrateur défini dans Cisco Secure ACS, définissez le même utilisateur pour la configuration de l'identité du système et configurez ACS comme

mode de configuration AAA.Reportez-vous à Procédures d'intégration exécutées dans CiscoWorks pour plus d'informations.

5. **Attribuez des rôles aux groupes d'utilisateurs dans Cisco Secure ACS.**Attribuez des rôles à chaque groupe d'utilisateurs configuré dans Cisco Secure ACS. La procédure que vous utilisez dépend du fait que vous avez configuré des groupes de périphériques réseau (NDG).Reportez-vous à Affecter des rôles à des groupes d'utilisateurs dans Cisco Secure ACS pour plus d'informations.

Procédures d'intégration exécutées dans Cisco Secure ACS

Cette section décrit les étapes à suivre dans Cisco Secure ACS pour l'intégrer à Cisco Security Manager :

1. Définir les utilisateurs et les groupes d'utilisateurs dans Cisco Secure ACS
2. Ajouter des périphériques gérés en tant que clients AAA dans Cisco Secure ACS
3. Créer un utilisateur de contrôle d'administration dans Cisco Secure ACS

Définir les utilisateurs et les groupes d'utilisateurs dans Cisco Secure ACS

Tous les utilisateurs de Cisco Security Manager doivent être définis dans Cisco Secure ACS et se voir attribuer un rôle correspondant à leur fonction. La façon la plus simple d'y parvenir est de diviser les utilisateurs en différents groupes en fonction de chaque rôle par défaut disponible dans ACS. Par exemple, affectez tous les administrateurs système à un groupe, tous les opérateurs réseau à un autre groupe, etc. Référez-vous à Rôles par défaut Cisco Secure ACS pour plus d'informations sur les rôles par défaut dans ACS.

En outre, vous devez créer un utilisateur supplémentaire auquel est attribué le rôle d'administrateur système avec des autorisations complètes. Les informations d'identification établies pour cet utilisateur sont utilisées ultérieurement sur la page Configuration de l'identité système de CiscoWorks. Voir Définir l'utilisateur d'identité système pour plus d'informations.

Notez qu'à ce stade, vous n'affectez que des utilisateurs à différents groupes. L'affectation effective des rôles à ces groupes est effectuée ultérieurement, après l'enregistrement de CiscoWorks, de Cisco Security Manager et de toute autre application auprès de Cisco Secure ACS.

Conseil : Avant de continuer, installez CiscoWorks Common Services et Cisco Security Manager sur un serveur Windows 2000/2003. Installez Cisco Secure ACS sur un autre serveur Windows 2000/2003.

1. Connectez-vous à Cisco Secure ACS.
2. Configurer un utilisateur avec des autorisations complètes :Cliquez sur **Configuration utilisateur** dans la barre de navigation.Sur la page User Setup, saisissez un nom pour le nouvel utilisateur, puis cliquez sur **Add/Edit**.Sélectionnez une méthode d'authentification dans la liste Password Authentication sous User Setup.Saisissez et confirmez le mot de passe du nouvel utilisateur.Sélectionnez **Groupe 1** comme groupe auquel l'utilisateur est affecté.Cliquez sur **Submit** afin de créer le compte utilisateur.
3. Répétez l'étape 2 pour chaque utilisateur de Cisco Security Manager. Cisco recommande de diviser les utilisateurs en groupes en fonction du rôle attribué à chaque utilisateur :Groupe 1 -

Administrateurs systèmeGroupe 2 - Administrateurs de sécuritéGroupe 3 - Approbateurs de sécuritéGroupe 4 - Administrateurs réseauGroupe 5 - ApprobateursGroupe 6 - Opérateurs réseauGroupe 7 - Centre d'assistanceReportez-vous au tableau pour plus d'informations sur les autorisations par défaut associées à chaque rôle. Référez-vous à Personnalisation des rôles Cisco Secure ACS pour plus d'informations sur la personnalisation des rôles utilisateur.**Note :** À ce stade, les groupes eux-mêmes sont des ensembles d'utilisateurs sans définition de rôle. Vous attribuez des rôles à chaque groupe une fois le processus d'intégration terminé. Reportez-vous à Affecter des rôles à des groupes d'utilisateurs dans Cisco Secure ACS pour plus d'informations.

4. Créez un utilisateur supplémentaire et affectez cet utilisateur au groupe d'administrateurs système. Les informations d'identification établies pour cet utilisateur sont utilisées ultérieurement sur la page Configuration de l'identité système de CiscoWorks. Voir Définir l'utilisateur d'identité système pour plus d'informations.
5. Continuer avec Ajouter des périphériques gérés en tant que clients AAA dans Cisco Secure ACS.

Ajouter des périphériques gérés en tant que clients AAA dans Cisco Secure ACS

Avant de commencer à importer des périphériques dans Cisco Security Manager, vous devez d'abord configurer chaque périphérique en tant que client AAA dans votre Cisco Secure ACS. En outre, vous devez configurer le serveur CiscoWorks/Security Manager en tant que client AAA.

Si Cisco Security Manager gère les contextes de sécurité configurés sur les périphériques de pare-feu, qui incluent les contextes de sécurité configurés sur les FWSM pour les périphériques Catalyst 6500/7600, chaque contexte doit être ajouté individuellement à Cisco Secure ACS.

La méthode que vous utilisez pour ajouter des périphériques gérés dépend de la volonté de restreindre les utilisateurs à gérer un ensemble particulier de périphériques avec des groupes de périphériques réseau (NDG). Reportez-vous à l'une des sections suivantes :

- Si vous voulez que les utilisateurs aient accès à tous les périphériques, ajoutez les périphériques comme décrit dans Ajouter des périphériques en tant que clients AAA sans NDG.
- Si vous souhaitez que les utilisateurs aient accès uniquement à certains NDG, ajoutez les périphériques comme décrit dans Configurer les groupes de périphériques réseau à utiliser dans Security Manager.

Ajouter des périphériques en tant que clients AAA sans NDG

Cette procédure décrit comment ajouter des périphériques en tant que clients AAA d'un Cisco Secure ACS. Reportez-vous à la section *Configuration du client AAA* de Configuration réseau pour obtenir des informations complètes sur toutes les options disponibles.

Remarque : N'oubliez pas d'ajouter le serveur CiscoWorks/Security Manager en tant que client AAA.

1. Cliquez sur **Configuration du réseau** dans la barre de navigation de Cisco Secure ACS.
2. Cliquez sur **Ajouter une entrée** sous le tableau Clients AAA.
3. Saisissez le nom d'hôte du client AAA (jusqu'à 32 caractères) sur la page Add AAA Client. Le

nom d'hôte du client AAA doit correspondre au nom d'affichage que vous prévoyez d'utiliser pour le périphérique dans Cisco Security Manager.Par exemple, si vous avez l'intention d'ajouter un nom de domaine au nom de périphérique dans Cisco Security Manager, le nom d'hôte du client AAA dans ACS doit être **<nom_périphérique>.<nom_domaine>**.Lorsque vous nommez le serveur CiscoWorks, il est recommandé d'utiliser le nom d'hôte complet. Assurez-vous d'épeler correctement le nom d'hôte. Le nom d'hôte ne respecte pas la casse.Lorsque vous nommez un contexte de sécurité, ajoutez le nom du contexte (**_<nom_contexte>**) au nom du périphérique. Pour les FWSM, il s'agit de la convention d'attribution de noms :Lame FWSM—**<nom_châssis>_FW_<numéro_emplacement>**Contexte de sécurité—**<nom_châssis>_FW_<numéro_emplacement>_<nom_contexte>**

4. Saisissez l'adresse IP du périphérique réseau dans le champ AAA Client IP Address.
5. Saisissez le secret partagé dans le champ Key (Clé).
6. Sélectionnez **TACACS+ (Cisco IOS)** dans la liste Authentifier à l'aide.
7. Cliquez sur **Submit** afin d'enregistrer vos modifications. Le périphérique que vous avez ajouté apparaît dans la table AAA Clients.
8. Répétez les étapes 1 à 7 afin d'ajouter des périphériques supplémentaires.
9. Après avoir ajouté tous les périphériques, cliquez sur **Soumettre + Redémarrer**.
10. Continuer avec Créer un utilisateur de contrôle d'administration dans Cisco Secure ACS.

Configurer des groupes de périphériques réseau à utiliser dans Security Manager

Cisco Secure ACS vous permet de configurer des groupes de périphériques réseau (NDG) contenant des périphériques spécifiques à gérer. Par exemple, vous pouvez créer des NDG pour chaque région géographique ou des NDG correspondant à votre structure organisationnelle. Lorsqu'ils sont utilisés avec Cisco Security Manager, les NDG vous permettent de fournir aux utilisateurs différents niveaux d'autorisations, en fonction des périphériques qu'ils doivent gérer. Par exemple, avec les NDG, vous pouvez attribuer des autorisations d'administrateur système utilisateur A aux périphériques situés en Europe et des autorisations de centre d'assistance aux périphériques situés en Asie. Vous pouvez ensuite attribuer les autorisations opposées à l'utilisateur B.

Les NDG ne sont pas attribués directement aux utilisateurs. Les NDG sont plutôt affectés aux rôles que vous définissez pour chaque groupe d'utilisateurs. Chaque NDG peut être attribué à un seul rôle, mais chaque rôle peut inclure plusieurs NDG. Ces définitions sont enregistrées dans le cadre de la configuration du groupe d'utilisateurs sélectionné.

Ces rubriques décrivent les étapes de base requises pour configurer les NDG :

- Activation de la fonction NDG
- Créer des NDG
- Associer des NDG et des rôles à des groupes d'utilisateurs

Activation de la fonction NDG

Vous devez activer la fonction NDG avant de pouvoir créer des NDG et les remplir avec des périphériques.

1. Cliquez sur **Interface Configuration** dans la barre de navigation de Cisco Secure ACS.
2. Cliquez sur **Options avancées**.

3. Faites défiler la liste vers le bas, puis cochez la case **Groupes de périphériques réseau**.
4. Cliquez sur Submit.
5. Continuer avec Créer des NDG.

Créer des NDG

Cette procédure décrit comment créer des NDG et les remplir avec des périphériques. Chaque périphérique ne peut appartenir qu'à un seul NDG.

Remarque : Cisco vous recommande de créer un NDG spécial contenant le serveur CiscoWorks/Security Manager.

1. Cliquez sur **Configuration réseau** dans la barre de navigation.Tous les périphériques sont initialement placés sous Non attribué, qui contient tous les périphériques qui n'ont pas été placés dans un NDG. N'oubliez pas que Not Assigned n'est pas un NDG.
2. Créer des NDG :Cliquez sur **Ajouter une entrée**.Entrez un nom pour le NDG sur la page New Network Device Group. La longueur maximale est de 24 caractères. Les espaces sont autorisés.**Facultatif avec la version 4.0 ou ultérieure :** Saisissez une clé à utiliser par tous les périphériques du NDG. Si vous définissez une clé pour le NDG, elle remplace toutes les clés définies pour les périphériques individuels dans le NDG.Cliquez sur **Soumettre** afin d'enregistrer le NDG.Répétez les étapes a à d afin de créer plus de NDG.
3. Remplir les NDG avec les périphériques :Cliquez sur le nom du NDG dans la zone Network Device Groups.Cliquez sur **Ajouter une entrée** dans la zone AAA Clients.Définissez les détails du périphérique à ajouter au NDG, puis cliquez sur **Soumettre**. Voir Ajouter des périphériques en tant que clients AAA sans NDG pour plus d'informations.Répétez les étapes b et c afin d'ajouter le reste des périphériques aux NDG. Le seul périphérique que vous pouvez laisser dans la catégorie Non affecté est le serveur AAA par défaut.Après avoir configuré le dernier périphérique, cliquez sur **Soumettre + Redémarrer**.
4. Continuer avec Créer un utilisateur de contrôle d'administration dans Cisco Secure ACS.

Créer un utilisateur de contrôle d'administration dans Cisco Secure ACS

Utilisez la page Administration Control de Cisco Secure ACS afin de définir le compte administrateur utilisé lors de la définition du mode de configuration AAA dans CiscoWorks Common Services. Reportez-vous à Configuration du mode de configuration AAA dans CiscoWorks pour plus d'informations.

1. Cliquez sur **Administration Control** dans la barre de navigation de Cisco Secure ACS.
2. Cliquez sur **Ajouter un administrateur**.
3. Sur la page Ajouter un administrateur, saisissez un nom et un mot de passe pour l'administrateur.
4. Cliquez sur **Grant All** dans la zone Administrator Privileges afin de fournir des autorisations d'administration complètes à cet administrateur.
5. Cliquez sur **Submit** afin de créer l'administrateur.

Remarque : Référez-vous à Administrateurs et Politique d'administration pour plus d'informations sur les options disponibles lorsque vous configurez un administrateur.

Procédures d'intégration exécutées dans CiscoWorks

Cette section décrit les étapes à suivre dans CiscoWorks Common Services pour l'intégrer à Cisco Security Manager :

- Créer un utilisateur local dans CiscoWorks
- Définir l'utilisateur d'identité système
- Configurer le mode de configuration AAA dans CiscoWorks

Effectuez ces étapes après avoir terminé les procédures d'intégration effectuées dans Cisco Secure ACS. Common Services effectue l'enregistrement réel de toutes les applications installées, telles que Cisco Security Manager, Auto-Update Server et IPS Manager, dans Cisco Secure ACS.

Créer un utilisateur local dans CiscoWorks

Utilisez la page Configuration utilisateur locale de CiscoWorks Common Services afin de créer un compte utilisateur local qui duplique l'administrateur que vous avez précédemment créé dans Cisco Secure ACS. Ce compte d'utilisateur local est utilisé ultérieurement pour la configuration de l'identité du système. Pour plus d'informations, reportez-vous à la section.

Remarque : avant de continuer, créez un administrateur dans Cisco Secure ACS. Reportez-vous à Définir des utilisateurs et des groupes d'utilisateurs dans Cisco Secure ACS pour obtenir des instructions.

1. Connectez-vous à CiscoWorks avec le compte utilisateur **admin** par défaut.
2. Choisissez **Server > Security** dans Common Services, puis choisissez **Local User Setup** dans la table des matières.
3. Cliquez sur **Add**.
4. Entrez le même nom et le même mot de passe que ceux que vous avez entrés lorsque vous avez créé l'administrateur dans Cisco Secure ACS. Reportez-vous à l'étape 4 de Définir des utilisateurs et des groupes d'utilisateurs dans Cisco Secure ACS.
5. Cochez toutes les cases sous Rôles à l'exception des données d'exportation.
6. Cliquez sur **OK** pour créer l'utilisateur.

Définir l'utilisateur d'identité système

Utilisez la page Configuration de l'identité système dans CiscoWorks Common Services afin de créer un utilisateur d'approbation, appelé utilisateur d'identité système, qui active la communication entre les serveurs qui font partie du même domaine et les processus d'application qui sont situés sur le même serveur. Les applications utilisent l'utilisateur Identité système afin d'authentifier les processus sur les serveurs CiscoWorks locaux ou distants. Cela est particulièrement utile lorsque les applications doivent se synchroniser avant que les utilisateurs ne se connectent.

En outre, l'utilisateur d'identité système est souvent utilisé pour exécuter une sous-tâche lorsque la tâche principale est déjà autorisée pour l'utilisateur connecté. Par exemple, pour modifier un périphérique dans Cisco Security Manager, une communication interapplication est requise entre Cisco Security Manager et le DCR des services communs. Une fois que l'utilisateur est autorisé à effectuer la tâche de modification, l'utilisateur Identité système est utilisé afin d'appeler le DCR.

L'utilisateur d'identité système que vous configurez ici doit être identique à l'utilisateur disposant des autorisations administratives (complètes) que vous avez configurées dans ACS. Si vous ne le faites pas, vous risquez de ne pas voir tous les périphériques et politiques configurés dans Cisco

Security Manager.

Remarque : Avant de continuer, créez un utilisateur local avec le même nom et le même mot de passe que cet administrateur dans CiscoWorks Common Services. Reportez-vous à Créer un utilisateur local dans CiscoWorks pour obtenir des instructions.

1. Choisissez **Serveur > Sécurité**, puis choisissez **Gestion de confiance multiserveur > Configuration de l'identité système** dans la table des matières.
2. Saisissez le nom de l'administrateur que vous avez créé pour Cisco Secure ACS. Reportez-vous à l'étape 4 de Définir des utilisateurs et des groupes d'utilisateurs dans Cisco Secure ACS.
3. Entrez et vérifiez le mot de passe de cet utilisateur.
4. Cliquez sur Apply.

Configurer le mode de configuration AAA dans CiscoWorks

Utilisez la page Mode de configuration AAA dans CiscoWorks Common Services afin de définir votre Cisco Secure ACS comme serveur AAA, qui inclut le port requis et la clé secrète partagée. En outre, vous pouvez définir jusqu'à deux serveurs de sauvegarde.

Ces étapes permettent d'enregistrer CiscoWorks, Cisco Security Manager, IPS Manager (et éventuellement Auto-Update Server) dans Cisco Secure ACS.

1. Choisissez **Server > Security**, puis choisissez **AAA Mode Setup** dans la table des matières.
2. Cochez la case **TACACS+** sous Modules de connexion disponibles.
3. Sélectionnez **ACS** comme type AAA.
4. Saisissez les adresses IP d'un maximum de trois serveurs Cisco Secure ACS dans la zone Détails du serveur. Les serveurs secondaire et tertiaire agissent comme sauvegardes en cas de défaillance du serveur principal.**Remarque :** si tous les serveurs TACACS+ configurés ne répondent pas, vous devez vous connecter avec le compte d'administrateur CiscoWorks Local, puis redéfinir le mode AAA sur Non-ACS/CiscoWorks Local. Une fois les serveurs TACACS+ restaurés en service, vous devez redéfinir le mode AAA en ACS.
5. Dans la zone Connexion, saisissez le nom de l'administrateur que vous avez défini sur la page Administration Control de Cisco Secure ACS. Reportez-vous à Créer un utilisateur de contrôle d'administration dans Cisco Secure ACS pour plus d'informations.
6. Entrez et vérifiez le mot de passe de cet administrateur.
7. Saisissez et vérifiez la clé secrète partagée que vous avez entrée lorsque vous avez ajouté le serveur Security Manager en tant que client AAA de Cisco Secure ACS. Reportez-vous à l'étape 5 dans Ajouter des périphériques en tant que clients AAA sans NDG.
8. Cochez la case **Enregistrer toutes les applications installées avec ACS** afin d'enregistrer Cisco Security Manager et toutes les autres applications installées avec Cisco Secure ACS.
9. Cliquez sur **Apply afin de sauvegarder vos paramètres.** Une barre de progression affiche la progression de l'enregistrement. Un message s'affiche lorsque l'enregistrement est terminé.
10. Si vous intégrez Cisco Security Manager à une version ACS, redémarrez le service Cisco Security Manager Daemon Manager. Reportez-vous à Redémarrer le Gestionnaire de démons pour obtenir des instructions.**Remarque :** après CSM 3.0.0, Cisco ne teste plus ACS 3.3(x) car il est fortement corrigé et sa fin de vie (EOL) a été annoncée. Par conséquent, vous devez utiliser la version ACS appropriée pour CSM versions 3.0.1 et ultérieures. Pour plus d'informations, reportez-vous au tableau Matrice de compatibilité.

11. Reconnectez-vous à Cisco Secure ACS afin d'attribuer des rôles à chaque groupe d'utilisateurs. Reportez-vous à Affecter des rôles à des groupes d'utilisateurs dans Cisco Secure ACS pour obtenir des instructions.**Remarque :** La configuration AAA configurée ici n'est pas conservée si vous désinstallez CiscoWorks Common Services ou Cisco Security Manager. En outre, cette configuration ne peut pas être sauvegardée et restaurée après la réinstallation. Par conséquent, si vous effectuez une mise à niveau vers une nouvelle version de l'une ou l'autre des applications, vous devez reconfigurer le mode de configuration AAA et réenregistrer Cisco Security Manager avec ACS. Ce processus n'est pas nécessaire pour les mises à jour incrémentielles. Si vous installez des applications supplémentaires, telles que AUS, en plus de CiscoWorks, vous devez réenregistrer les nouvelles applications et Cisco Security Manager.

Redémarrer le Gestionnaire de démons

Cette procédure décrit comment redémarrer le Gestionnaire de démons du serveur Cisco Security Manager. Vous devez effectuer cette opération pour que les paramètres AAA que vous avez configurés prennent effet. Vous pouvez ensuite vous reconnecter à CiscoWorks avec les informations d'identification définies dans Cisco Secure ACS.

1. Connectez-vous à la machine sur laquelle le serveur Cisco Security Manager est installé.
2. Choisissez **Démarrer > Programmes > Outils d'administration > Services** afin d'ouvrir la fenêtre Services.
3. Dans la liste des services affichée dans le volet de droite, sélectionnez **Cisco Security Manager Daemon Manager**.
4. Cliquez sur le bouton **Redémarrer le service** de la barre d'outils.
5. Continuer avec Affecter des rôles à des groupes d'utilisateurs dans Cisco Secure ACS.

Attribuer des rôles à des groupes d'utilisateurs dans Cisco Secure ACS

Après avoir enregistré CiscoWorks, Cisco Security Manager et d'autres applications installées sur Cisco Secure ACS, vous pouvez attribuer des rôles à chacun des groupes d'utilisateurs que vous avez précédemment configurés dans Cisco Secure ACS. Ces rôles déterminent les actions que les utilisateurs de chaque groupe sont autorisés à effectuer dans Cisco Security Manager.

La procédure que vous utilisez pour attribuer des rôles à des groupes d'utilisateurs dépend de l'utilisation ou non des NDG :

- Affecter des rôles à des groupes d'utilisateurs sans NDG
- Associer des NDG et des rôles à des groupes d'utilisateurs

Affecter des rôles à des groupes d'utilisateurs sans NDG

Cette procédure décrit comment attribuer les rôles par défaut aux groupes d'utilisateurs lorsque les NDG ne sont pas définis. Référez-vous à Rôles par défaut Cisco Secure ACS pour plus d'informations.

Remarque : avant de continuer :

- Créez un groupe d'utilisateurs pour chaque rôle par défaut. Reportez-vous à Définir des utilisateurs et des groupes d'utilisateurs dans Cisco Secure ACS pour obtenir des instructions.
- Suivez les procédures décrites dans Procédures d'intégration exécutées dans Cisco Secure ACS et Procédures d'intégration exécutées dans CiscoWorks.

Procédez comme suit :

1. Connectez-vous à Cisco Secure ACS.
2. Cliquez sur **Configuration du groupe** dans la barre de navigation.
3. Sélectionnez le groupe d'utilisateurs pour les administrateurs système dans la liste. Reportez-vous à l'étape 2 de Définir des utilisateurs et des groupes d'utilisateurs dans Cisco Secure ACS, puis cliquez sur **Modifier les paramètres**.

Associer des NDG et des rôles à des groupes d'utilisateurs

Lorsque vous associez des NDG à des rôles à utiliser dans Cisco Security Manager, vous devez créer des définitions à deux endroits de la page Configuration du groupe :

- Zone CiscoWorks
- Zone Cisco Security Manager

Les définitions de chaque domaine doivent correspondre le plus étroitement possible. Lorsque vous associez des rôles personnalisés ou ACS qui n'existent pas dans CiscoWorks Common Services, essayez de définir le plus près possible d'un rôle équivalent en fonction des autorisations attribuées à ce rôle.

Vous devez créer des associations pour chaque groupe d'utilisateurs à utiliser avec Cisco Security Manager. Par exemple, si vous avez un groupe d'utilisateurs qui contient du personnel de support pour la région Occidentale, vous pouvez sélectionner ce groupe d'utilisateurs, puis associer le NDG qui contient les périphériques de cette région au rôle Centre d'assistance.

Remarque : avant de continuer, activez la fonction NDG et créez des NDG. Reportez-vous à Configurer des groupes de périphériques réseau à utiliser dans Security Manager pour plus d'informations.

1. Cliquez sur **Configuration du groupe** dans la barre de navigation.
2. Sélectionnez un groupe d'utilisateurs dans la liste Groupe, puis cliquez sur **Modifier les paramètres**.
3. Mapper les NDG et les rôles à utiliser dans CiscoWorks :Sur la page Group Setup (Configuration du groupe), faites défiler jusqu'à la zone CiscoWorks sous TACACS+ Settings (Paramètres TACACS+).Sélectionnez **Affecter un CiscoWorks par groupe de périphériques réseau**.Sélectionnez un NDG dans la liste Device Group.Sélectionnez le rôle auquel ce NDG doit être associé dans la deuxième liste.Cliquez sur **Ajouter une association**. L'association apparaît dans la zone Groupe de périphériques.Répétez les étapes c à e afin de créer des associations supplémentaires.**Remarque :** afin de supprimer une association, sélectionnez-la dans le groupe de périphériques, puis cliquez sur Supprimer l'association.
4. Faites défiler jusqu'à la zone Gestionnaire de sécurité Cisco et créez des associations qui correspondent le plus possible aux associations définies à l'étape 3.**Remarque :** Lorsque vous sélectionnez les rôles Approbateur de sécurité ou Administrateur de sécurité dans Cisco Secure ACS, il est recommandé de sélectionner Administrateur réseau comme rôle équivalent le plus proche de CiscoWorks.

5. Cliquez sur **Submit** afin d'enregistrer vos paramètres.
6. Répétez les étapes 2 à 5 afin de définir des NDG pour le reste des groupes d'utilisateurs.
7. Après avoir associé des NDG et des rôles à chaque groupe d'utilisateurs, cliquez sur **Soumettre + Redémarrer**.

Dépannage

1. Avant de commencer à importer des périphériques dans Cisco Security Manager, vous devez d'abord configurer chaque périphérique en tant que client AAA dans votre Cisco Secure ACS. En outre, vous devez configurer le serveur CiscoWorks/Security Manager en tant que client AAA.
2. Si vous recevez un journal des tentatives ayant échoué, l'auteur a échoué avec une erreur dans Cisco Secure ACS.
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test
   Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches
   authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   Afin de résoudre ce problème, assurez-vous que le nom du périphérique dans ACS doit être un nom de domaine complet.

Informations connexes

- Page d'assistance de Cisco Security Access Control Server pour Windows
- Page d'assistance de Cisco Security Manager
- Cisco Secure Access Control Server pour Windows
- Guide de configuration de Cisco Secure ACS 4.1
- Guide de dépannage en ligne Cisco Secure ACS, 4.1
- Avis de champs relatifs aux produits de sécurité (y compris CiscoSecure ACS pour Windows)
- Support et documentation techniques - Cisco Systems