Cisco Secure ACS : Restrictions d'accès au réseau avec des clients AAA pour les utilisateurs et les groupes d'utilisateurs

Contenu

Introduction

Ce document décrit comment configurer les restrictions d’accès au réseau (NAR) dans la version 4.x du Cisco Secure Access Control Server (ACS) avec des clients AAA (y compris les routeurs, le PIX, l’ASA et les contrôleurs sans fil) pour des utilisateurs et des groupes d’utilisateurs.

Conditions préalables

Conditions requises

Ce document est créé avec la supposition que des clients de Cisco Secure ACS et d'AAA sont configurés et fonctionnent correctement.

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Secure ACS 3.0 et plus tard.

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 utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Restrictions d'accès au réseau

Cette section décrit NARs, et fournit le mode d'emploi détaillé de configurer et gérer NARs partagé.

Cette section contient ces sujets :

Au sujet des restrictions d'accès au réseau

Un NAR est une définition, que vous faites dans ACS, des conditions supplémentaires que vous devez remplir avant qu'un utilisateur puisse accéder au réseau. ACS applique ces conditions à l'aide des informations à partir des attributs que vos clients d'AAA envoient. Bien que vous puissiez installer NARs de plusieurs manières, tous sont basés sur les informations d'attribut assorties qu'un client d'AAA envoie. Par conséquent, vous devez comprendre le format et le contenu des attributs que vos clients d'AAA envoient si vous voulez utiliser NARs efficace.

Quand vous installez un NAR, vous pouvez choisir si le filtre fonctionne franchement ou négativement. C'est-à-dire, dans le NAR vous spécifiez si permettre ou refuser l'accès au réseau, basé sur les informations envoyées des clients d'AAA une fois comparé à l'information enregistrée dans le NAR. Cependant, si un NAR ne rencontre pas les informations suffisantes pour fonctionner, il se transfère sur l'accès refusé. Cette table affiche ces conditions :

	Basé sur IP	**Non-IP basé**	**Les informations insuffisantes**
Autorisation	Access a accordé	Access a refusé	Access a refusé
Refusez	Access a refusé	Access a accordé	Access a refusé

ACS prend en charge deux types de filtres NAR :

- **filtres basés sur IP** — le NAR basé sur IP filtre la limite accès basé sur sur les adresses IP du client d'utilisateur et du client d'AAA. Voyez le pour en savoir plus environ basé sur IP de section de filtres NAR.
- **filtres basés sur Non IP** — le NAR basé sur Non IP filtre la limite accès basé sur sur la comparaison simple de chaîne d'une valeur envoyée du client d'AAA. La valeur peut être nombre de l'identification de ligne d'appel (CLI), le nombre de Service d'identification du numéro composé réacheminé (RDNIS), une adresse MAC, ou une valeur différente qui provient du client. Pour ce type de NAR à fonctionner, la valeur dans la description NAR doit

exactement apparier ce qui est envoyé du client, qui inclut Qu'est ce que format est utilisé. Par exemple, le téléphone le numéro (217) 555-4534 n'apparie pas 217-555-4534. Voyez le pour en savoir plus environ basé sur Non IP de section de filtres NAR.

Vous pouvez définir un NAR pour, et appliquez lui, à un utilisateur ou un groupe d'utilisateurs spécifique. Voyez les restrictions d'accès au réseau de positionnement pour un utilisateur ou placez les restrictions d'accès au réseau pour un pour en savoir plus de sections de groupe d'utilisateurs. Cependant, dans la section partagée de composants de profil d'ACS vous pouvez créer et nommer un NAR partagé sans citer directement n'importe quel utilisateur ou groupe d'utilisateurs. Vous donnez au NAR partagé un nom qui peut être mis en référence dans d'autres parties de l'interface web ACS. Puis, quand vous installez des utilisateurs ou des groupes d'utilisateurs, vous pouvez n'en sélectionner aucun, un, ou des restrictions partagées par multiple être appliqué. Quand vous spécifiez l'application de NARs partagé par multiple à un utilisateur ou à un groupe d'utilisateurs, vous choisissez un de deux critères d'accès :

- Tous les filtres sélectionnés doivent laisser.
- N'importe quel un filtre sélectionné doit laisser.

Vous devez comprendre la commande de priorité qui est liée aux différents types de NARs. C'est la commande du filtrage NAR :

1. NAR partagé au niveau utilisateur
2. NAR partagé au niveau du groupe
3. NAR non partagé au niveau utilisateur
4. NAR non partagé au niveau du groupe

Vous devriez également comprendre que le **refus de l'accès à n'importe quel niveau a la priorité au-dessus des configurations à un autre niveau qui ne refusent pas l'accès**. C'est l'une exception dans ACS à la règle que les configurations de niveau utilisateur ignorent des configurations de niveau du groupe. Par exemple, un utilisateur particulier pourrait n'avoir aucune restriction NAR au niveau utilisateur qui s'appliquent. Cependant, si cet utilisateur appartient à un groupe qui est limité par un NAR partagé ou non partagé, l'utilisateur est refusé l'accès.

NARs partagé sont maintenus dans la base de données interne ACS. Vous pouvez employer les caractéristiques de sauvegarde ACS et de restauration pour sauvegarder, et les restaurez. Vous pouvez également répliquer le NARs partagé, avec d'autres configurations, vers ACSs secondaire.

Au sujet des filtres basés sur IP NAR

Pour les filtres basés sur IP NAR, ACS utilise les attributs comme affichés, qui dépend du protocole AAA de la demande d'authentification :

- **Si vous utilisez TACACS+** — Le champ de `rem_addr du` corps de paquet de début TACACS+ est utilisé.**Note**: Quand une demande d'authentification est expédiée par proxy à un ACS, n'importe quel NARs pour des demandes TACACS+ sont appliqués à l'adresse IP du serveur d'AAA d'expédition, pas à l'adresse IP du client d'AAA de commencement.
- **Si vous utilisez l'IETF de RAYON** — `Le calling-station-id` (attribut 31) doit être utilisé.**Note**: les filtres basés sur IP NAR fonctionnent seulement si ACS reçoit attributs de calling-station-id de rayon les 31) (. Le calling-station-id (31) doit contenir une adresse IP valide. S'il ne fait pas, il tombera plus d'aux règles DNIS.

Les clients d'AAA qui ne fournissent pas des informations suffisantes d'adresse IP (par exemple, quelques types de Pare-feu) ne prennent en charge pas la pleine fonctionnalité NAR.

D'autres attributs pour des restrictions **basées sur IP**, par protocole, incluent les champs NAR comme affichés :

- **Si vous utilisez TACACS+** — Les champs NAR dans ACS utilisent ces valeurs :**Client d'AAA** — La Nas-IP-adresse est prise de l'adresse source dans le socket entre ACS et le client TACACS+.**Port** — Le champ de port est pris du corps de paquet de début TACACS+.

Au sujet des filtres basés sur Non IP NAR

Un filtre basé sur non IP NAR (c'est-à-dire, un filtre DNIS/CLI-based NAR) est une liste d'appeler ou de point permis ou refusé d'emplacements d'accès que vous pouvez employer pour limiter un client d'AAA quand vous n'avez pas une connexion basée sur IP établie. La caractéristique basée sur non IP NAR utilise généralement le nombre CLI et le numéro de DNIS.

Cependant, quand vous écrivez une adresse IP au lieu du CLI, vous pouvez utiliser le filtre basé sur non IP ; même lorsque le client d'AAA n'utilise pas une version logicielle de Cisco IOS® qui prend en charge le CLI ou le DNIS. Dans une autre exception à écrire un CLI, vous pouvez écrire une adresse MAC pour permettre ou refuser l'accès. Par exemple, quand vous utilisez un client d'AAA de Cisco Aironet. De même, vous pourriez écrire l'adresse MAC de Cisco Aironet AP au lieu du DNIS. Le format de ce que vous spécifiez dans la case CLI — CLI, adresse IP, ou adresse MAC — doit apparier le format de ce que vous recevez de votre client d'AAA. Vous pouvez déterminer ce format de votre journal de traçabilité de RAYON.

Les attributs pour des restrictions DNIS/CLI-based, par protocole, incluent les champs NAR comme affichés :

- **Si vous utilisez TACACS+** — Les champs NAR répertoriés utilisent ces valeurs :**Client d'AAA** — `La Nas-IP-adresse` est prise de l'adresse source dans le socket entre ACS et le client TACACS+.**Port** — Le champ de `port` dans le corps de paquet de début TACACS+ est utilisé.**CLI** — Le champ de rem-`adr` dans le corps de paquet de début TACACS+ est utilisé.**DNIS** — Le champ de rem-`adr` pris du corps de paquet de début TACACS+ est utilisé. Dans des cas en lesquels les données de rem-adr commencent par le slash (/), le champ DNIS contient les données de rem-adr sans slash (/).**Note**: Quand une demande d'authentification est expédiée par proxy à un ACS, n'importe quel NARs pour des demandes TACACS+ sont appliqués à l'adresse IP du serveur d'AAA d'expédition, pas à l'adresse IP du client d'AAA de commencement.
- **Si vous utilisez le RAYON** — Les champs NAR répertoriés utilisent ces valeurs :**Client d'AAA** — `La Nas-IP-adresse` (l'attribut 4) ou, si la Nas-IP-adresse n'existe pas, le Nas-`identifiant` (attribut RADIUS 32) est utilisé.**Port** — `Le Nas-port` (l'attribut 5) ou, si le Nas-port n'existe pas, le Nas-port-`ID` (attribut 87) est utilisé.**CLI** — `Le calling-station-id` (attribut 31) est utilisé.**DNIS** — `L'appeler-station-ID` (attribut 30) est utilisé.

Quand vous spécifiez un NAR, vous pouvez employer un astérisque (*) comme masque pour n'importe quelle valeur, ou en tant qu'élément de n'importe quelle valeur pour établir une plage. Toutes les valeurs ou conditions dans une description NAR doivent être remplies pour que le NAR limite l'accès. Ceci signifie que les valeurs contiennent un booléen ET.

Ajoutez un NAR partagé

Vous pouvez créer un NAR partagé qui contient beaucoup de restrictions d'accès. Bien que l'interface web ACS n'impose pas des limites au nombre de restrictions d'accès dans un NAR

partagé ou à la longueur de chaque restriction d'accès, vous devez adhérer à ces limites :

- La combinaison des champs pour chaque élément de ligne ne peut pas dépasser 1024 caractères.
- Le NAR partagé ne peut pas avoir plus de 16 KO des caractères. Le nombre d'éléments de ligne pris en charge dépend de la longueur de chaque élément de ligne. Par exemple, si vous créez un CLI/DNIS-based NAR où les noms de client d'AAA sont 10 caractères, les numéros de port sont 5 caractères, les entrées CLI sont 15 caractères, et les entrées DNIS sont 20 caractères, vous peuvent ajouter 450 éléments de ligne avant que vous atteigniez la limite du KO 16.

Note: Avant que vous définissiez un NAR, assurez-vous que vous avez établi les éléments que vous avez l'intention de utiliser dans ce NAR. Par conséquent, vous devez avoir spécifié tous les NAFs et NDGs, et avoir défini tous les clients appropriés d'AAA, avant que vous leur fassiez une partie de la définition NAR. Voyez environ le pour en savoir plus de section de restrictions d'accès au réseau.

Terminez-vous ces étapes afin d'ajouter un NAR partagé :

1. Dans la barre de navigation, le clic **a partagé des composants de profil**.La fenêtre partagée de composants de profil apparaît.
2. **Restrictions d'accès au réseau de** clic.
3. Cliquez sur **Add**.La fenêtre de restriction d'accès au réseau apparaît.
4. Dans la case de nom, écrivez un nom pour le nouveau NAR partagé.**Note**: Le nom peut contenir jusqu'à 31 caractères. On ne permet pas la conduite et les espaces de remorquage. Les noms ne peuvent pas contenir ces caractères : crochet de gauche ([), crochet droit (]), virgule (,), ou slash (/).
5. Dans la case de description, écrivez une description du nouveau NAR partagé. La description peut être jusqu'à 30,000 caractères.
6. Si vous voulez permettre ou refuser accès basé sur sur l'adressage IP :Cochez la case **basée sur IP de descriptions d'accès de définir**.Afin de spécifier si vous répertoriez les adresses qui sont permises ou refusées, du Tableau définit la liste, sélectionnent la valeur applicable.Sélectionnez ou écrivez les informations applicables dans chacune de ces cases :**Client d'AAA** — Sélectionnez **tous les clients d'AAA**, ou le nom du NDG, ou le NAF, ou le client individuel d'AAA, auquel l'accès est permis ou refusé.**Port** — Entrez dans le nombre du port auquel vous voulez permettre ou refuser l'accès. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser l'accès à tous les ports sur le client sélectionné d'AAA.**Adresse IP de Src** — Écrivez l'adresse IP pour filtrer sur en exécutant des restrictions d'accès. Vous pouvez employer l'astérisque (*) comme masque pour spécifier toutes les adresses IP.**Note**: Le nombre total de caractères dans la liste de client d'AAA, et le port et les cases d'adresse IP de Src, ne doivent pas dépasser 1024. Bien qu'ACS reçoive plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer le NAR et l'ACS ne pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**.Le client, le port, et les informations d'adresse d'AAA apparaissent comme élément de ligne dans la table.Répétez les étapes c et d afin d'inscrire les éléments de ligne basés sur IP supplémentaires.
7. Si vous voulez permettre ou refuser accès basé sur sur appeler l'emplacement ou les valeurs autres que des adresses IP :Cochez la case de **restrictions d'accès basée par CLI/DNIS de définir**.Afin de spécifier si vous répertoriez les emplacements qui sont permis ou refusé du Tableau définit la liste, sélectionnez la valeur applicable.Afin de spécifier les clients auxquels

ce NAR s'applique, sélectionnez une de ces valeurs de la liste de client d'AAA :Le nom du NDGLe nom du client particulier d'AAATous les clients d'AAA**Conseil** : Seulement NDGs que vous avez déjà configuré sont répertoriés.Afin de spécifier les informations sur lesquelles ce NAR devrait filtrer, écrivez les valeurs dans des ces cases, comme applicable :**Conseil** : Vous pouvez écrire un astérisque (*) comme masque pour spécifier **tous** comme valeur.**Port** — Entrez dans le nombre du port sur lequel pour filtrer.**CLI** — Introduisez le nombre CLI sur lequel pour filtrer. Vous pouvez également utiliser cette case pour limiter accès basé sur sur des valeurs autres que CLIs, tel qu'une adresse IP ou une adresse MAC. Voyez environ le pour en savoir plus de section de restrictions d'accès au réseau.**DNIS** — Introduisez le nombre étant commuté à sur ce que de filtrer.**Note**: Le nombre total de caractères dans la liste de client d'AAA et les cases de port, CLI, et DNIS ne doit pas dépasser 1024. Bien qu'ACS reçoive plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer le NAR et l'ACS ne pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**.Les informations qui spécifient l'élément de ligne NAR apparaissent dans la table.Répétez les étapes c à e afin d'inscrire les éléments de ligne basés sur non IP supplémentaires NAR.Cliquez sur Submit afin de sauvegarder la définition partagée NAR.ACS enregistre le NAR partagé et le répertorie dans la table de **restrictions d'accès au réseau**.

Éditez un NAR partagé

Terminez-vous ces étapes afin d'éditer un NAR partagé :

1. Dans la barre de navigation, le clic **a partagé des composants de profil**.La fenêtre partagée de composants de profil apparaît.
2. **Restrictions d'accès au réseau de** clic.La table de restrictions d'accès au réseau apparaît.
3. Dans la colonne de nom, cliquez sur le NAR partagé que vous voulez éditer.La fenêtre de restriction d'accès au réseau apparaît et affiche des informations pour le NAR sélectionné.
4. Éditez le nom ou la description du NAR, comme applicable. La description peut être jusqu'à 30,000 caractères.
5. Afin d'éditer un élément de ligne dans la table basée sur IP d'Access-restrictions :Double-cliquer l'élément de ligne que vous voulez éditer.Les informations pour l'élément de ligne sont enlevées de la table et écrites dans les cases sous la table.Éditez les informations, selon les besoins.**Note**: Le nombre total de caractères dans la liste de client d'AAA et le port et de cases d'adresse IP de Src ne doit pas dépasser 1024. Bien qu'ACS puisse recevoir plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer un tels NAR et ACS ne pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**.Les informations éditées pour cet élément de ligne sont écrites à la table basée sur IP d'Access-restrictions.
6. Afin de retirer un élément de ligne de la table basée sur IP d'Access-restrictions :Sélectionnez l'élément de ligne.Sous la table, le clic **retirent**.L'élément de ligne est retiré de la table basée sur IP d'Access-restrictions.
7. Afin d'éditer un élément de ligne dans la table d'Access-restrictions CLI/DNIS :Double-cliquer l'élément de ligne que vous voulez éditer.Les informations pour l'élément de ligne sont enlevées de la table et écrites dans les cases sous la table.Éditez les informations, selon les besoins.**Note**: Le nombre total de caractères dans la liste de client d'AAA et les cases de port, CLI, et DNIS ne doit pas dépasser 1024. Bien qu'ACS puisse recevoir plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer un tels NAR et ACS ne

pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**Les informations éditées pour cet élément de ligne sont écrites à la table d'Access-restrictions CLI/DNIS.
8. Afin de retirer un élément de ligne de la table d'Access-restrictions CLI/DNIS :Sélectionnez l'élément de ligne.Sous la table, le clic **retirent**.L'élément de ligne est retiré de la table d'Access-restrictions CLI/DNIS.
9. Cliquez sur Submit afin de sauvegarder les modifications que vous avez apportées.ACS ressaisit le filtre avec les nouvelles informations, qui les prennent effet immédiatement.

Supprimez un NAR partagé

Note: Assurez-vous que vous retirez l'association d'un NAR partagé sur n'importe quel utilisateur ou groupez avant que vous supprimiez ce NAR.

Terminez-vous ces étapes afin de supprimer un NAR partagé :

1. Dans la barre de navigation, le clic **a partagé des composants de profil**.La fenêtre partagée de composants de profil apparaît.
2. **Restrictions d'accès au réseau de** clic.
3. Cliquez sur le nom du NAR partagé que vous voulez supprimer.La fenêtre de restriction d'accès au réseau apparaît et affiche des informations pour le NAR sélectionné.
4. Au bas de la fenêtre, cliquez sur Delete.Une boîte de dialogue vous avertit que vous êtes sur le point de supprimer un NAR partagé.
5. Cliquez sur OK afin de confirmer que vous voulez supprimer le NAR partagé.Le NAR partagé sélectionné est supprimé.

Placez les restrictions d'accès au réseau pour un utilisateur

Vous employez la table de restrictions d'accès au réseau dans la région de paramètres avancés de l'installation utilisateur pour placer NARs de trois manières :

- Appliquez NARs partagé existant de nom.
- Définissez les restrictions basées sur IP d'accès pour permettre ou refuser l'accès client à un client spécifié d'AAA ou aux ports spécifiés sur un client d'AAA quand une connexion IP a été établie.
- Définissez les restrictions d'accès CLI/DNIS-based pour permettre ou refuser l'accès client basé sur le CLI/DNIS qui est utilisé.**Note**: Vous pouvez également employer la zone de restrictions d'accès CLI/DNIS-based pour spécifier d'autres valeurs. Voyez le pour en savoir plus de section de restrictions d'accès au réseau.

Typiquement, vous définissez NARs (partagé) de la section partagée de composants de sorte que vous puissiez s'appliquer ces restrictions à plus d'un groupe ou utilisateur. Voyez l'ajouter un pour en savoir plus partagé de section NAR. Vous devez avoir sélectionné la case de **restrictions d'accès au réseau de niveau utilisateur** sur la page options avancée de la section de configuration d'interface pour que cet ensemble d'options apparaisse dans l'interface web.

Cependant, vous pouvez également employer ACS pour définir et appliquer un NAR pour un seul utilisateur de la section User Setup. Vous devez avoir activé les **restrictions d'accès au réseau de niveau utilisateur** plaçant sur la page options avancée de la section de configuration d'interface pour que des options de filtre basées sur IP de seul utilisateur et des options de filtre du seul utilisateur CLI/DNIS-based apparaissent dans l'interface web.

Note: Quand une demande d'authentification est expédiée par proxy à un ACS, n'importe quel NARs pour des demandes de Terminal Access Controller Access Control System (TACACS+) sont appliqués à l'adresse IP du serveur d'AAA d'expédition, pas à l'adresse IP du client d'AAA de commencement.

Quand vous créez des restrictions d'accès sur une base par utilisateur, ACS n'impose pas des limites au nombre de restrictions d'accès et n'impose pas une limite à la longueur de chaque restriction d'accès. Cependant, il y a des limites strictes :

- La combinaison des champs pour chaque élément de ligne ne peut pas dépasser 1024 caractères de longueur.
- Le NAR partagé ne peut pas avoir plus de 16 KO des caractères. Le nombre d'éléments de ligne pris en charge dépend de la longueur de chaque élément de ligne. Par exemple, si vous créez un CLI/DNIS-based NAR où les noms de client d'AAA sont 10 caractères, les numéros de port sont 5 caractères, les entrées CLI sont 15 caractères, et les entrées DNIS sont 20 caractères, vous peuvent ajouter 450 éléments de ligne avant que vous atteigniez la limite du KO 16.

Terminez-vous ces étapes afin de placer NARs pour un utilisateur :

1. Exécutez les étapes 1 à 3 d'ajouter un compte utilisateur de base.L'installation utilisateur éditent la fenêtre s'ouvre. Le nom d'utilisateur que vous ajoutez ou éditez apparaît en haut de la fenêtre.
2. Afin de s'appliquer un NAR partagé précédemment configuré à cet utilisateur :**Note**: Afin d'appliquer un NAR partagé, vous devez l'avoir configuré sous des restrictions d'accès au réseau dans la section partagée de composants de profil. Voyez l'ajouter un pour en savoir plus partagé de section NAR.Cochez le **seul permettent l'accès au réseau quand** case.Afin de spécifier si un ou tout le NARs partagé doit s'appliquer pour qu'on permette à l'utilisateur l'accès, sélectionnez un, comme applicable :Tout le résultat sélectionné NARS dans l'autorisation.Résultats sélectionnés quelconques un NAR dans l'autorisation.Sélectionnez un nom partagé NAR dans la liste de NARs, et puis cliquez sur --> (bouton de flèche à droite) pour entrer le nom dans la liste sélectionnée de NARs.**Conseil** : Afin de visualiser les détails de serveur du NARs partagé que vous avez sélectionné pour s'appliquer, vous peut cliquer sur **IP NAR** ou **vue CLID/DNIS NAR de vue**, comme applicable.
3. Afin de définir et appliquer un NAR, pour cet utilisateur particulier, qui permet ou refuse cet accès client basé sur l'adresse IP, ou adresse IP et port :**Note**: Vous devriez définir la plupart de NARs de la section partagée de composants de sorte que vous puissiez les appliquer à plus d'un groupe ou utilisateur. Voyez l'ajouter un pour en savoir plus partagé de section NAR.Dans la table de restrictions d'accès au réseau, dessous par restrictions définies par l'utilisateur d'accès au réseau, cochez la case **basée sur IP de restrictions d'accès de définir**.Afin de spécifier si la liste ultérieure spécifie les adresses IP permises ou refusées, du Tableau définit la liste, choisissent un :**Appeler permis/point des emplacements d'AccessAppeler refusé/point des emplacements d'Access**Sélectionnez ou écrivez les informations dans des ces cases :**Client d'AAA** — Sélectionnez **tous les clients d'AAA**, ou le nom d'un groupe de périphériques réseau (NDG), ou le nom du client individuel d'AAA, auquel pour permettre ou refuser l'accès.**Port** — Entrez dans le nombre du port auquel pour permettre ou refuser l'accès. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser l'accès à tous les ports sur le client sélectionné d'AAA.**Adresse** — Introduisez l'adresse IP ou les adresses pour l'utiliser en exécutant des restrictions d'accès. Vous pouvez utiliser l'astérisque (*) comme masque.**Note**: Le nombre total de caractères

dans la liste de client d'AAA, et le port et les cases d'adresse IP de Src ne doivent pas dépasser 1024. Bien qu'ACS reçoive plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer le NAR et l'ACS ne pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**.Le client, le port, et les informations d'adresse spécifiés d'AAA apparaît dans la table au-dessus de la liste de client d'AAA.

4. Afin de permettre ou refuser cet accès client basé sur appeler l'emplacement ou les valeurs autres qu'une adresse IP établie :Cochez la case de **restrictions d'accès basée par CLI/DNIS de définir**.Afin de spécifier si la liste ultérieure spécifie des valeurs permises ou refusées, du Tableau définit la liste, choisissent un :**Appeler permis/point des emplacements d'AccessAppeler refusé/point des emplacements d'Access**Terminez-vous les cases comme affichées :**Note**: Vous devez faire une entrée dans chaque case. Vous pouvez utiliser l'astérisque (*) comme masque pour l'ensemble ou une partie d'une valeur. Le format que vous utilisez doit apparier le format de la chaîne que vous recevez de votre client d'AAA. Vous pouvez déterminer ce format de votre journal de traçabilité de RAYON.**Client d'AAA** — Sélectionnez **tous les clients d'AAA**, ou le nom du NDG, ou le nom du client individuel d'AAA, auquel pour permettre ou refuser l'accès.**PORT** — Entrez dans le nombre du port auquel pour permettre ou refuser l'accès. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser l'accès à tous les ports.**CLI** — Introduisez le nombre CLI auquel pour permettre ou refuser l'accès. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser accès basé sur sur une partie du nombre.**Conseil** : Utilisez l'entrée CLI si vous voulez limiter accès basé sur sur d'autres valeurs telles qu'une adresse MAC de client de Cisco Aironet. Voyez environ le pour en savoir plus de section de restrictions d'accès au réseau.**DNIS** — Introduisez le numéro de DNIS auquel pour permettre ou refuser l'accès. Employez cette entrée pour limiter accès basé sur sur le nombre dans lequel l'utilisateur introduira. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser accès basé sur sur une partie du nombre.**Conseil** : Utilisez la sélection DNIS si vous voulez limiter accès basé sur sur d'autres valeurs telles qu'une adresse MAC de Cisco Aironet AP. Voyez environ le pour en savoir plus de section de restrictions d'accès au réseau.**Note**: Le nombre total de caractères dans la liste de client d'AAA et les cases de **port**, **CLI** et **DNIS** ne doit pas dépasser 1024. Bien qu'ACS reçoive plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer le NAR et l'ACS ne pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**.Les informations qui spécifient le client d'AAA, le port, le CLI, et le DNIS apparaissent dans la table au-dessus de la liste de client d'AAA.
5. Si vous êtes de finition configurant les options de compte utilisateur, cliquez sur Submit afin d'enregistrer les options.

Placez les restrictions d'accès au réseau pour un groupe d'utilisateurs

Vous employez la table de restrictions d'accès au réseau dans le Group Setup pour appliquer NARs de trois manières distinctes :

- Appliquez NARs partagé existant de nom.
- Définissez les restrictions basées sur IP d'accès de groupe pour permettre ou refuser l'accès à un client spécifié d'AAA ou aux ports spécifiés sur un client d'AAA quand une connexion IP a été établie.
- Définissez le groupe NARs CLI/DNIS-based pour permettre ou refuser l'accès à, ou chacun

des deux, le nombre CLI ou le numéro de DNIS utilisé.**Note**: Vous pouvez également employer la zone de restrictions d'accès CLI/DNIS-based pour spécifier d'autres valeurs. Voyez environ le pour en savoir plus de section de restrictions d'accès au réseau.

Typiquement, vous définissez NARs (partagé) de la section partagée de composants de sorte que ces restrictions puissent s'appliquer à plus d'un groupe ou utilisateur. Voyez l'ajouter un pour en savoir plus partagé de section NAR. Vous devez cocher la case de **restriction d'accès au réseau partagée par niveau du groupe** sur la **page options avancée de la** section de configuration d'interface pour que ces options apparaissent dans l'interface web ACS.

Cependant, vous pouvez également employer ACS pour définir et appliquer un NAR pour un seul groupe de la **section Installation de groupe**. Vous devez vérifier la configuration de **restriction d'accès au réseau de niveau du groupe** sous la page options avancée de la section de configuration d'interface pour que des options de filtre basées sur IP de seul groupe et des options de filtre simples du groupe CLI/DNIS-based apparaissent dans l'interface web ACS.

Note: Quand une demande d'authentification est expédiée par proxy à un serveur ACS, n'importe quel NARs pour des demandes RADIUS sont appliqués à l'adresse IP du serveur d'AAA d'expédition, pas à l'adresse IP du client d'AAA de commencement.

Terminez-vous ces étapes afin de placer NARs pour un groupe d'utilisateurs :

1. Dans la barre de navigation, **Group Setup de** clic.La fenêtre choisie de Group Setup s'ouvre.
2. De la liste de groupe, sélectionnez un groupe, et puis cliquez sur Edit les **configurations**.Le nom du groupe apparaît en haut de la fenêtre de configurations de groupe.
3. Afin de s'appliquer un NAR partagé précédemment configuré à ce groupe :**Note**: Afin d'appliquer un NAR partagé, vous devez l'avoir configuré sous des restrictions d'accès au réseau dans la section partagée de composants de profil. Voyez l'ajouter un pour en savoir plus partagé de section NAR.Cochez le **seul permettent l'accès au réseau quand** case.Afin de spécifier si un ou tout le NARs partagé doit s'appliquer pour un membre du groupe pour permettre l'accès, vérifiez une de ces options :Tous sélectionnés ont partagé le résultat NARS dans l'autorisation.N'importe quel un NAR partagé sélectionné a comme conséquence l'autorisation.Sélectionnez un nom partagé NAR dans la liste partagée NAR, et puis cliquez sur --> (bouton de flèche à droite) pour entrer le nom dans la liste partagée sélectionnée de NARs.**Conseil** : Afin de visualiser les détails de serveur du NARs partagé que vous avez appliqué, vous pouvez cliquer sur **IP NAR** ou **vue CLID/DNIS NAR de vue**, comme applicable.
4. Afin de définir et appliquer un NAR pour ce groupe d'utilisateurs particulier, ce permet ou refuse l'accès à ce groupe basé sur l'adresse IP, ou l'adresse IP et le port :**Note**: Vous devriez définir la plupart de NARs de la section partagée de composants de sorte que les restrictions puissent s'appliquer à plus d'un groupe ou utilisateur. Voyez l'ajouter un pour en savoir plus partagé de section NAR.Dans par accès au réseau défini par groupe les restrictions que la section des restrictions d'accès au réseau ajournent, cochent la case **basée sur IP de restrictions d'accès de définir**.Afin de spécifier si la liste ultérieure spécifie les adresses IP permises ou refusées, du Tableau définit la liste, choisit **appeler permis/point des emplacements d'Access** ou **appeler refusé/point des emplacements d'Access**.Sélectionnez ou écrivez les informations dans des ces cases :**Client d'AAA** — Sélectionnez tous les clients d'AAA ou le nom du NDG ou le nom du client individuel d'AAA auquel vous voulez permettre ou refuser l'accès.**Port** — Entrez dans le nombre du port auquel pour permettre ou refuser l'accès. Vous pouvez employer l'astérisque (*) comme

masque pour permettre ou refuser l'accès à tous les ports sur le client sélectionné d'AAA.**Adresse** — Introduisez l'adresse IP ou les adresses pour filtrer sur en exécutant des restrictions d'accès. Vous pouvez utiliser l'astérisque (*) comme masque.**Note**: Le nombre total de caractères dans la liste de client d'AAA et le port et de cases d'adresse IP de Src ne doit pas dépasser 1024. Bien qu'ACS reçoive plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer le NAR et l'ACS ne pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**.Spécifié le client, le port, et les informations d'adresse d'AAA apparaît dans la **liste de contrôle d'accès NAR**.

5. Afin de permettre ou refuser l'accès à ce groupe d'utilisateurs basé sur appeler l'emplacement ou les valeurs autres qu'une adresse IP établie :Cochez la case de **restrictions d'accès du définir CLI/DNIS-based**.Afin de spécifier si la liste ultérieure spécifie des valeurs permises ou refusées, du Tableau définit la liste, choisissent un :**Appeler permis/point des emplacements d'AccessAppeler refusé/point des emplacements d'Access**De la liste de client d'AAA, choisissez **tous les clients d'AAA**, ou le nom du NDG ou le nom du client particulier d'AAA auquel pour permettre ou refuser l'accès.Terminez-vous ces cases :**Note**: Vous devez écrire une entrée dans chaque case. Vous pouvez utiliser l'astérisque (*) comme masque pour l'ensemble ou une partie d'une valeur. Le format que vous utilisez doit apparier le format de la chaîne que vous recevez de votre client d'AAA. Vous pouvez déterminer ce format de votre journal de traçabilité de RAYON.**PORT** — Entrez dans le nombre du port auquel pour permettre ou refuser l'accès. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser l'accès à tous les ports.**CLI** — Introduisez le nombre CLI auquel pour permettre ou refuser l'accès. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser accès basé sur sur une partie du nombre ou de tous nombres.**Conseil** : Le CLI est également la sélection à l'utiliser si vous voulez limiter accès basé sur sur d'autres valeurs, telles qu'une adresse MAC de client de Cisco Aironet. Voyez environ le pour en savoir plus de section de restrictions d'accès au réseau.**DNIS** — Introduisez le numéro de DNIS pour limiter accès basé sur sur le nombre dans lequel l'utilisateur introduira. Vous pouvez employer l'astérisque (*) comme masque pour permettre ou refuser accès basé sur sur une partie du nombre ou de tous nombres.**Conseil** : DNIS est également la sélection si vous voulez limiter accès basé sur sur d'autres valeurs, telles qu'une adresse MAC de Cisco Aironet AP. Voyez environ le pour en savoir plus de section de restrictions d'accès au réseau.**Note**: Le nombre total de caractères dans la liste de client d'AAA, et les cases de port, CLI, et DNIS ne doivent pas dépasser 1024. Bien qu'ACS reçoive plus de 1024 caractères quand vous ajoutez un NAR, vous ne pouvez pas éditer le NAR et l'ACS ne pouvez pas exactement s'appliquer l'aux utilisateurs.Le clic **entrent**.Les informations qui spécifient le client d'AAA, le port, le CLI, et le DNIS apparaissent dans la liste.
6. Cliquez sur Submit afin de sauvegarder les configurations de groupe que vous avez juste faites.Référez-vous aux modifications d'économie au pour en savoir plus de configurations de groupe d'utilisateurs.

Informations connexes

- Page de support de Cisco Secure Access Control Server
- Support et documentation techniques - Cisco Systems