TACACS+ et attributs RADIUS pour divers Cisco et l'exemple de configuration de périphériques non-Cisco

Contenu

Introduction

Ce document fournit une compilation des attributs que les divers Produits de Cisco et de non-Cisco comptent recevoir d'un serveur d'Authentification, autorisation et comptabilité (AAA) ; dans ce cas, le serveur d'AAA est un serveur de contrôle d'accès (ACS). L'ACS peut renvoyer ces attributs avec un Access-recevoir pendant qu'une partie d'un profil de shell (TACACS+) ou de profil d'autorisation (RAYON).

Ce document fournit des instructions pas à pas sur la façon dont ajouter des attributs personnalisés pour écosser des profils et des profils d'autorisation. Ce document contient également une liste de périphériques et le TACACS+ et attributs RADIUS que les périphériques comptent voir retourné du serveur d'AAA. Tous les thèmes incluent des exemples.

La liste d'attributs fournis dans ce document n'est pas exhaustive ou bien fondée et peut changer à tout moment sans mise à jour en ce document.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version 5.2/5.3 ACS.

Conventions

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

Créez un profil de shell (TACACS+)

Un profil de shell est un conteneur de base d'autorisations pour l'accès TACACS+-based. Vous pouvez spécifier que TACACS+ attribue et des valeurs d'attribut devraient être retournées avec l'Access-recevoir, en plus du niveau de privilège IOS de ® de Cisco, du délai d'attente de session, et d'autres paramètres.

Terminez-vous ces étapes afin d'ajouter des attributs personnalisés à un nouveau profil de shell :

1. Procédure de connexion à l'interface ACS.
2. Naviguez des **profils** vers des **éléments de stratégie** > l'**autorisation et des autorisations** > de **périphérique gestion > shell**.
3. Cliquez sur le bouton de **création**.
4. Nommez le profil de shell.
5. Cliquez sur l'onglet d'**attributs personnalisés**.
6. Écrivez le nom d'attribut dans le domaine d'**attribut**.
7. Choisissez si la condition requise est **obligatoire** ou **facultative de la** liste déroulante de condition requise.
8. Laissez le déroulant pour la valeur d'attribut réglée à la **charge statique**. Si la valeur est statique, vous pouvez écrire la valeur dans le prochain domaine. Si la valeur est dynamique, vous ne pouvez pas écrire l'attribut manuellement ; au lieu de cela attribué est tracé à un attribut dans une des mémoires d'identité.
9. Écrivez la valeur de l'attribut dans le dernier domaine.
10. Cliquez sur le bouton d'**ajouter** afin d'ajouter l'entrée à la table.
11. Répétition pour configurer tous les attributs que vous avez besoin.
12. Cliquez sur le bouton de **soumission au** bas de l'écran.

Exemple de configuration

Périphérique : Moteur de contrôle des applications (ACE)

Attributs : `shell : <context-name>`

Valeurs : `<Role-name> <domain-name1>`

Utilisation : Le rôle et le domaine sont séparés par un caractère espace. Vous pouvez configurer un utilisateur (par exemple, USER1) pour assigner un rôle (par exemple, ADMIN) et un domaine (par exemple, MYDOMAIN) quand l'utilisateur ouvre une session à un contexte (par exemple, C1).

Créez un profil d'autorisation (le RAYON)

Un profil d'autorisation est un conteneur de base d'autorisations pour l'accès basé sur rayon. Vous pouvez spécifier que des attributs RADIUS et les valeurs d'attribut devraient être retourné avec l'Access-recevoir, en plus des VLAN, du Listes de contrôle d'accès (ACL), et d'autres paramètres.

Terminez-vous ces étapes afin d'ajouter des attributs personnalisés à un nouveau profil d'autorisation :

1. Procédure de connexion à l'interface ACS.
2. Naviguez vers des **éléments de stratégie** > l'**autorisation et des autorisations** > des **profils d'accès au réseau** > d'**autorisation**.
3. Cliquez sur le bouton de **création**.
4. Nommez le profil d'autorisation.
5. Cliquez sur l'onglet d'**attributs RADIUS**.
6. Sélectionnez un dictionnaire du menu déroulant de **type de dictionnaire**.
7. Afin de placer le choisi l'attribut pour le champ d'attribut RADIUS, cliquent sur le **bouton Select**. Une nouvelle fenêtre apparaît.
8. Passez en revue les attributs disponibles, faites votre sélection, et cliquez sur OK. **La valeur de type d'attribut** est placée par défaut, basé sur la sélection d'attribut que vous avez juste faite.
9. Laissez le déroulant pour la valeur d'attribut réglée à la **charge statique**. Si la valeur est statique, vous pouvez écrire la valeur dans le prochain domaine. Si la valeur est dynamique, vous ne pouvez pas écrire l'attribut manuellement ; au lieu de cela attribué est tracé à un attribut dans une des mémoires d'identité.
10. Écrivez la valeur de l'attribut dans le dernier domaine.
11. Cliquez sur le bouton d'**ajouter** afin d'ajouter l'entrée à la table.
12. Répétition pour configurer tous les attributs que vous avez besoin.
13. Cliquez sur le bouton de **soumission au** bas de l'écran.

Exemple de configuration

Périphérique : ACE

Attributs : `Cisco-poids du commerce-paires`

Valeurs : `shell : <context-name>=<Role-name> <domain-name1> <domain-name2>`

Utilisation : Chaque valeur après le signe d'égalité est séparée par un caractère espace. Vous

pouvez configurer un utilisateur (par exemple, USER1) pour assigner un rôle (par exemple, ADMIN) et un domaine (par exemple, MYDOMAIN) quand l'utilisateur ouvre une session à un contexte (par exemple, C1).

Liste de périphériques

L'agrégation entretient les Routeurs (l'ASR)

RAYON (profil d'autorisation)

Attributs : `Cisco-poids du commerce-paires`

Valeurs : `shell : #<role-name> de tasks= ", <permission> : <process> »`

Utilisation : Placez les valeurs du `<role-name> au` nom d'un rôle localement défini sur le routeur. La hiérarchie de rôle peut être décrite en termes d'arborescence, où le `#root de` rôle est en haut de l'arborescence, et le `#leaf de` rôle ajoute des commandes supplémentaires. Ces deux rôles peuvent être combinés et passés de retour si : `shell : tasks= " #root, #leaf »`.

Des autorisations peuvent également être passées de retour sur une base de processus individuel, de sorte qu'un utilisateur puisse être accordé lu, écrire, et exécuter des privilèges pour certains processus. Par exemple, afin d'accorder un utilisateur lisez et écrivez les privilèges pour le processus BGP, placent la valeur à : `shell : #root de tasks= ", le RW : BGP »`. La commande des attributs n'importe pas ; le résultat est identique si la valeur est placée `pour écosser : #root de tasks= ", le RW : shell BGP »` ou RO `: tasks= " RW : BGP, #root »`.

Exemple – ***Ajoutez l'attribut à un profil d'autorisation***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-Cisco	`cisco-av-pair`	Chaîne	`shell:tasks="#root,#leaf,rwx :bgp,r:ospf"`

Moteur de contrôle des applications (ACE)

TACACS+ (profil de shell)

Attributs : `shell : <context-name>`

Valeurs : `<Role-name> <domain-name1>`

Utilisation : Le rôle et le domaine sont séparés par un caractère espace. Vous pouvez configurer un utilisateur (par exemple, USER1) pour assigner un rôle (par exemple, ADMIN) et un domaine (par exemple, MYDOMAIN) quand l'utilisateur ouvre une session à un contexte (par exemple, C1).

Exemple – ***Ajoutez l'attribut à un profil de shell***

Attribut	Condition requise	Valeur d'attribut
`shell:C1`	Obligatoire	`Admin MYDOMAIN`

Si USER1 ouvre une session par le contexte C1, cet utilisateur est automatiquement assigné le

rôle d'ADMIN et le domaine MYDOMAIN (à condition que une règle d'autorisation ait été configurée où, une fois qu'USER1 ouvre une session, ils sont assignés ce profil d'autorisation).

Si USER1 ouvre une session par un contexte différent, qui n'est pas retourné en valeur de l'attribut que l'ACS renvoie, que l'utilisateur est automatiquement assigné le rôle par défaut (surveillance réseau) et le domaine par défaut (par défaut-domaine).

RAYON (profil d'autorisation)

Attributs : `Cisco-poids du commerce-paires`

Valeurs : `shell : <context-name>=<Role-name> <domain-name1> <domain-name2>`

Utilisation : Chaque valeur après le signe d'égalité est séparée par un caractère espace. Vous pouvez configurer un utilisateur (par exemple, USER1) pour assigner un rôle (par exemple, ADMIN) et un domaine (par exemple, MYDOMAIN) quand les journaux de l'utilisateur dans un contexte (par exemple, C1).

Exemple – ***Ajoutez l'attribut à un profil d'autorisation***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-Cisco	`cisco-av-pair`	Chaîne	`shell:C1=ADMIN MYDOMAIN`

Si USER1 ouvre une session par le contexte C1, cet utilisateur est automatiquement assigné le rôle d'ADMIN et le domaine MYDOMAIN (à condition que une règle d'autorisation ait été configurée où, une fois qu'USER1 ouvre une session, ils sont assignés ce profil d'autorisation).

Si USER1 ouvre une session par un contexte différent, qui n'est pas retourné en valeur de l'attribut que l'ACS renvoie, que l'utilisateur est automatiquement assigné le rôle par défaut (surveillance réseau) et le domaine par défaut (par défaut-domaine).

Modélisateur de paquet de BlueCoat

RAYON (profil d'autorisation)

Attributs : `Packeteer-AVPair`

Valeurs : `access=<level>`

Utilisation : `le <level>` est le niveau d'accès à accorder. L'accès de toucher est équivalent à lecture/écriture, alors que l'accès d'aspect est équivalent à en lecture seule.

Le VSA de BlueCoat n'existe pas dans les dictionnaires ACS par défaut. Afin d'utiliser l'attribut de BlueCoat dans un profil d'autorisation, vous devez créer un dictionnaire de BlueCoat et ajouter les attributs de BlueCoat à ce dictionnaire.

Créez le dictionnaire :

1. Naviguez vers l'**administration système** > la **configuration** > les **dictionnaires** > les **protocoles** > le **RAYON** > le **VSA de RAYON**.
2. Cliquez sur **Create**.

3. Écrivez les détails du dictionnaire :Nom : BlueCoatID de constructeur : 2334Préfixe d'attribut : Packeteer-
4. Cliquez sur **Submit**.

Créez un attribut dans le nouveau dictionnaire :

1. Naviguez vers l'**administration système** > la **configuration** > les **dictionnaires** > les **protocoles** > le **RADIU** S > **RAYON LE VSA** > **BlueCoat**.
2. Cliquez sur **Create**.
3. Écrivez les détails de l'attribut :Attribut : `Packeteer-AVPair`Description : Utilisé afin de spécifier le niveau d'accèsID d'attribut du constructeur : 1Direction : SORTANTMultiple permis : FauxIncluez l'attribut dans le log : VérifiéType d'attribut : Chaîne
4. Cliquez sur **Submit**.

Exemple – ***Ajoutez l'attribut à un profil d'autorisation (pour l'accès en lecture seule)***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-BlueCoat	`Packeteer-AVPair`	Chaîne	`access=look`

Exemple – ***Ajoutez l'attribut à un profil d'autorisation (pour l'accès en lecture-écriture)***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-BlueCoat	`Packeteer-AVPair`	Chaîne	`access=touch`

Commutateurs de brocard

RAYON (profil d'autorisation)

Attributs : `Tunnel-Private-Group-ID`

Valeurs : `U:<VLAN1>` ; `T:<VLAN2>`

Utilisation : Placez `<VLAN1> à la` valeur des données VLAN. Placez `<VLAN2> à la` valeur de la Voix VLAN. Dans cet exemple, les données VLAN sont VLAN 10, et la Voix VLAN est VLAN 21.

Exemple – ***Ajoutez l'attribut à un profil d'autorisation***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-IETF	`Tunnel-Private-Group-ID`	Chaîne étiquetée	`U:10;T:21`

Cisco Unity Express (CUE)

RAYON (profil d'autorisation)

Attributs : `Cisco-poids du commerce-paires`

Valeurs : `fndn : groups=<group-name>`

Utilisation : `le <group-name>` est le nom du groupe avec les privilèges que vous voulez accorder à l'utilisateur. Ce groupe doit être configuré sur le Cisco Unity Express (CUE).

Exemple – ***Ajoutez l'attribut à un profil d'autorisation***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-Cisco	`cisco-av-pair`	Chaîne	`fndn:groups=Administrators`

Infoblox

RAYON (profil d'autorisation)

Attributs : `Infoblox-Groupe-information`

Valeurs : `<group-name>`

Utilisation : `le <group-name>` est le nom du groupe avec les privilèges que vous voulez accorder à l'utilisateur. Ce groupe doit être configuré sur le périphérique d'Infoblox. Dans cet exemple de configuration, le nom de groupe est MyGroup.

Le VSA d'Infoblox n'existe pas dans les dictionnaires ACS par défaut. Afin d'utiliser l'attribut d'Infoblox dans un profil d'autorisation, vous devez créer un dictionnaire d'Infoblox et ajouter les attributs d'Infoblox à ce dictionnaire.

Créez le dictionnaire :

1. Naviguez vers l'**administration système** > la **configuration** > les **dictionnaires** > les **protocoles** > le **RAYON** > le **VSA de RAYON**.
2. Cliquez sur **Create**.
3. Cliquez sur la petite flèche à côté des **options de constructeur avancées par utilisation**.
4. Écrivez les détails du dictionnaire :Nom : InfobloxID de constructeur : 7779Taille de champ de longueur de constructeur : 1Taille de champ de type de constructeur : 1
5. Cliquez sur **Submit**.

Créez un attribut dans le nouveau dictionnaire :

1. Naviguez vers l'**administration système** > la **configuration** > les **dictionnaires** > les **protocoles** > le **RAYON** > le **RAYON LE VSA** > **Infoblox**.
2. Cliquez sur **Create**.
3. Écrivez les détails de l'attribut :Attribut : `Infoblox-Groupe-information`ID d'attribut du constructeur : 009Direction : SORTANTMultiple permis : FauxIncluez l'attribut dans le log : VérifiéType d'attribut : Chaîne
4. Cliquez sur **Submit**.

Exemple – ***Ajoutez l'attribut à un profil d'autorisation***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-Infoblox	`Infoblox-Group-Info`	Chaîne	`MyGroup`

Système de prévention d'intrusion (IPS)

RAYON (profil d'autorisation)

Attributs : `IPS-rôle`

Valeurs : `name> de <role`

Utilisation : `Le name> de <role de` valeur peut être des n'importe quels des quatre rôles de l'utilisateur de Système de prévention d'intrusion (IPS) : visualiseur, opérateur, administrateur, ou service. Référez-vous au guide de configuration pour votre version d'IPS pour les détails des autorisations accordées à chaque rôle de l'utilisateur de type.

- Guide de configuration de gestionnaire de périphériques de Système de protection contre les intrusions Cisco IPS 7.0
- Guide de configuration de gestionnaire de périphériques de Système de protection contre les intrusions Cisco IPS 7.1

Exemple – ***Ajoutez l'attribut à un profil d'autorisation***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-Cisco	`cisco-av-pair`	Chaîne	`ips-role:administrator`

Genévrier

TACACS+ (profil de shell)

Attributs : `autoriser-commandes` ; `autoriser-configuration` ; `gens du pays-utilisateur-nom` ; `refuser-commandes` ; `refuser-configuration` ; `autorisations utilisateur`

Valeurs : `<allow-commands-regex>` ; `<allow-configuration-regex>` ; `<local-username>` ; `<deny-commands-regex>` ; `<deny-configuration-regex>`

Utilisation : Placez la valeur du `<local-username>` (c'est-à-dire, la valeur de l'attribut de gens du pays-utilisateur-nom) à un nom d'utilisateur qui existe localement sur le périphérique de genévrier. Par exemple, vous pouvez configurer un utilisateur (par exemple, USER1) pour assigner la même grille utilisateur qu'un utilisateur (par exemple, JUSER) qui existe localement sur le périphérique de genévrier quand vous placez la valeur de l'attribut de gens du pays-utilisateur-nom à JUSER. Les valeurs des autoriser-commandes, de l'autoriser-configuration, des refuser-commandes, et des attributs de refuser-configuration peuvent être écrites dans le format d'expression régulière. Les valeurs que ces attributs sont placés à sont en plus des commandes opérationnelles/mode de configuration autorisées par les bits d'autorisations de classe de la procédure de connexion de l'utilisateur.

Exemple – ***Ajoutez les attributs à un profil 1 de shell***

Attribut	Condition requise	Valeur d'attribut
`allow-commands`	Facultatif	`"(request system) | (show rip`

		neighbor)"
allow-configuration	Facultatif	
local-user-name	Facultatif	sales
deny-commands	Facultatif	"<^clear"
deny-configuration	Facultatif	

Exemple – ***Ajoutez les attributs à un profil 2 de shell***

Attribut	Condition requise	Valeur d'attribut
allow-commands	Facultatif	"monitor | help | show | ping | traceroute"
allow-configuration	Facultatif	
local-user-name	Facultatif	engineering
deny-commands	Facultatif	"configure"
deny-configuration	Facultatif	

Commutateurs de Nexus

RAYON (profil d'autorisation)

Attributs : `Cisco-poids du commerce-paires`

Valeurs : `shell:roles="<role1> <role2>"`

Utilisation : Placez les valeurs de `<role1>` et de `<role2> aux` noms des rôles localement définis sur le commutateur. Quand vous ajoutez de plusieurs rôles, séparez-les avec un caractère espace. Quand de plusieurs rôles sont passés de retour du serveur d'AAA au commutateur de Nexus, le résultat est que l'utilisateur a accès aux commandes définies par l'union de chacun des trois rôles.

Les rôles intégrés sont définis en configurant des comptes utilisateurs et RBAC.

Exemple – ***Ajoutez l'attribut à un profil d'autorisation***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
Rayon-Cisco	cisco-av-pair	Chaîne	shell:roles="network-admin vdc-admin vdc-operator"

Lit de la rivière

TACACS+ (profil de shell)

Attributs : `service` ; `gens du pays-utilisateur-nom`

Valeurs : `rbt-exécutif` ; `<username>`

Utilisation : Afin d'accorder l'accès en lecture seule d'utilisateur, la valeur de `<username>` doit être placée pour surveiller. Afin d'accorder l'accès en lecture-écriture d'utilisateur, la valeur de `<username>` doit être placée à l'admin. Si vous avez un autre compte défini en plus de l'admin et du

moniteur, configurez ce nom à retourner.

Exemple – ***Ajoutez les attributs à un profil de shell (pour l'accès en lecture seule)***

Attribut	Condition requise	Valeur d'attribut
`service`	Obligatoire	`rbt-exec`
`local-user-name`	Obligatoire	`monitor`

Exemple – ***Ajoutez les attributs à un profil de shell (pour l'accès en lecture-écriture)***

Attribut	Condition requise	Valeur d'attribut
`service`	Obligatoire	`rbt-exec`
`local-user-name`	Obligatoire	`admin`

Contrôleur LAN Sans fil (WLC)

RAYON (profil d'autorisation)

Attributs : `Type de service`

Valeurs : `(6) administratif`/Nas-`demande (7)`

Utilisation : Afin d'accorder à l'utilisateur l'accès lecture/écriture au contrôleur LAN Sans fil (WLC), la valeur doit être administrative ; pour l'accès en lecture seule, la valeur doit être Nas-demande.

Pour des détails, voir l'authentification de serveur de RAYON des utilisateurs de Gestion sur l'exemple Sans fil de configuration du contrôleur LAN (WLC)

Exemple – ***Ajoutez l'attribut à un profil d'autorisation (pour l'accès en lecture seule)***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-IETF	`Service-Type`	Énumération	`NAS-Prompt`

Exemple – ***Ajoutez l'attribut à un profil d'autorisation (pour l'accès en lecture-écriture)***

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-IETF	`Service-Type`	Énumération	`Administrative`

Gestionnaire de réseau de Data Center (DCNM)

DCNM doit être redémarré après que la méthode d'authentification soit changée. Autrement, il peut assigner le privilège d'opérateur réseau au lieu du réseau-admin.

Rôle DCNM	Cisco-POIDs du commerce-paires de RAYON	Cisco-POIDs du commerce-paires de Tacacs
Utilisateur	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`

Administrateur	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

Informations connexes

- Support et documentation techniques - Cisco Systems
- Terminal Access Controller Access Control System
- Service RADIUS (Remote Authentication Dial-In User Service)
- Demandes de commentaires (RFC)