L'intégration de version 5.4 ACS avec Motorola s'envole l'exemple de la configuration 5.X (AP)

Contenu

Introduction

Ce document fournit à un exemple de configuration une version 5.4 du Cisco Secure Access Control Server (ACS) pour prendre en charge l'Authentification, autorisation et comptabilité (AAA) TACACS+ sur les contrôleurs Sans fil et les Points d'accès de Motorola. Dans ce document, des attributs et les valeurs de constructeur-particularité de Motorola sont assignés aux groupes sur l'ACS afin de déterminer chaque rôle et autorisation d'accès d'utilisateur. Les attributs et les valeurs sont assignés au groupe avec des services définis par l'utilisateur et aux protocoles activés sur chaque groupe.

Conditions préalables

Conditions requises

La version 5.x ACS devrait être connectée aux ailes 5.x de Motorola.

Composants utilisés

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

- Version 5.4 ACS
- Ailes 5.2

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.

Configurez

Configuration ACS

Types de périphérique

Voici un exemple de la façon définir des périphériques de l'aile 5 comme types de périphérique sur une version 5.x de Cisco Secure ACS. Les types de périphérique permettent des périphériques à grouper en version 5.x de Cisco Secure ACS, qui est utilisée quand vous définissez des stratégies d'autorisation de périphérique.

Sur le GUI ACS, naviguez vers des **ressources de réseau > des groupes de périphériques réseau > le type de périphérique**, et le clic **créent**.

Écrivez un **nom** et une **description**, et sélectionnez un **parent**. Cliquez sur **Submit**.

Ceci crée un **groupe de périphériques réseau** pour des périphériques de solutions de Motorola.

Périphériques de réseau et clients d'AAA

Voici un exemple de la façon ajouter un périphérique de l'aile 5 en tant que client d'AAA sur la version 5.x de Cisco Secure ACS.

Sur le Cisco Secure ACS, naviguez vers des **ressources de réseau > des périphériques de réseau et des clients d'AAA**, et le clic **créent** :

Écrivez un **nom** pour le contrôleur sans-fil, et sélectionnez un **emplacement**. Assignez le **type de périphérique** créé dans la section précédente, et vérifiez la case à cocher **TACACS+**. Écrivez un **secret partagé**, et cliquez sur la case d'option à côté de l'option appropriée d'**adresse IP**. Dans cet exemple, la **plage IP par le masque** est sélectionnée, et le sous-réseau d'ipv4 que les contrôleurs sans-fil sont connectés à (**192.168.20.0/24**) est défini. Cliquez sur Submit une fois que vous

écrivez toutes les informations.

Ceci définit le contrôleur sans-fil comme **périphériques de réseau et clients d'AAA** :

Groupes d'identité

Dans cet exemple, deux groupes, MotorolaRO Désigné et MotorolaRW, sont définis. Des utilisateurs assignés au groupe de MotorolaRO sont assignés au rôle de moniteur et aux autorisations accordées d'accès au Web, alors que des utilisateurs assignés au groupe de MotorolaRW sont assignés au rôle de super utilisateur et accordaient toute l'autorisation d'accès.

Naviguez vers des **utilisateurs et l'identité enregistre > des groupes d'identité > créent** :

Écrivez un **nom** et une **description** pour seulement le groupe d'Access lu, et cliquez sur Submit.

Créez un deuxième groupe. Écrivez un **nom** et une **description** pour le groupe d'Access lecture/écriture, et cliquez sur Submit.

Vous avez maintenant créé deux **groupes d'identité**.

Profils de shell

Voici un exemple de la façon définir des profils de shell sur une version 5.x de Cisco Secure ACS. Dans cet exemple, deux écossent les profils, le RO et le MOTO RW MOTO Désigné, sont définis avec les attributs qui déterminent le rôle et l'autorisation d'accès que chaque utilisateur de Gestion est assigné. Le nom de chaque profil de shell doit apparier le nom du service d'authentification TACACS+ défini dans la stratégie d'AAA TACACS+.

Naviguez des **profils** vers des **éléments de stratégie > l'autorisation et des autorisations > de périphérique gestion > shell**. Cliquez sur **Create**.

Sur l'**onglet Général**, définissez les services requis et les protocoles TACACS+ pour ajouter. Vous pouvez utiliser les services et les protocoles en cours ou créer vos propres moyens. Cet exemple définit des services et des protocoles sous le nom du RO MOTO afin de fournir seulement Access lu pour s'envoler 5 périphériques :

Sur les **fonctionnalités usuelles** tabulez, placez le **privilège maximum à la charge statique**, et sélectionnez une valeur de **1.**

Sur l'onglet d'**attributs personnalisés**, dans les domaines d'**attribut** et de **valeur d'attribut**, définissez les attributs à assigner à l'utilisateur. Dans cet exemple, seulement des utilisateurs lus sont assignés au rôle de moniteur et aux autorisations accordées d'accès au Web. Cliquez sur **Submit**.

Créez un nouveau **profil de shell**. Sur l'**onglet Général**, définissez les services requis et les protocoles TACACS+ pour ajouter. Vous pouvez utiliser les services et les protocoles en cours ou créer vos propres moyens. Cet exemple définit des services et des protocoles, MOTO Désignés RW, qui fournissent Access lecture/écriture pour des périphériques de l'aile 5 :

Sur les **fonctionnalités usuelles** tabulez, placez le **privilège maximum à la charge statique**, et sélectionnez une valeur de **1.**

Sur l'onglet d'**attributs personnalisés**, dans les domaines d'**attribut** et de **valeur d'attribut**, définissez les attributs à assigner à l'utilisateur. Dans cet exemple, des utilisateurs lecture/écriture sont assignés au rôle de super utilisateur et ont accordé toute l'autorisation d'accès. Cliquez sur **Submit**.

Vous avez maintenant créé des **profils de shell** nommés le RO et le MOTO RW MOTO.

Profils d'autorisation de périphérique

Voici un exemple de la façon définir des stratégies d'autorisation de périphérique sur une version 5.x de Cisco Secure ACS. Les stratégies d'autorisation de périphérique déterminent le profil de shell chaque Gestion que l'utilisateur est assigné basé sur le type de périphérique qui demande l'authentification, l'emplacement, et l'adhésion à des associations d'identité. Dans cet exemple, deux stratégies d'autorisation de périphérique, MotorolaRO Désigné et MotorolaRW, sont définies.

Sur le Cisco Secure ACS, naviguez **pour accéder à des stratégies > l'admin > l'autorisation de périphérique de par défaut > personnalisent** :

Ajoutez les conditions de personnaliser nommés **Identity Group**, **NDG : Emplacement**, **NDG : Type de périphérique**, et **Protocol**. Sous personnalisez les résultats, ajoutez le **profil de shell**, et cliquez sur OK :

Cliquez sur **Create**. Dans la zone d'**identification**, entrez dans **MotorolaRO**, et sélectionnez le **groupe d'identité**, **NDG : Emplacement**, et **type de NDGevice**. Placez Protocol à **Tacacs**, et sélectionnez le profil de shell nommé **RO MOTO**. Cliquez sur OK :

Cliquez sur **Create**. Dans la zone d'**identification**, entrez dans **MotorolaRW**, et sélectionnez le **groupe d'identité**, **NDG : Emplacement**, et **type de NDGevice**. Placez Protocol à **Tacacs**, et sélectionnez le profil de shell nommé **MOTO RW**. Cliquez sur OK :

Vous avez maintenant créé des **stratégies d'autorisation de périphérique** nommées MotorolaRO et MotorolaRW :

Configuration de l'aile 5.2 de solutions de Motorola

Stratégies de l'AAA TACACS

La stratégie de l'AAA TACACS définit la configuration de client TACACS+ sur un périphérique de l'aile 5. Chaque stratégie de l'AAA TACACS peut contenir jusqu'à deux entrées de serveur d'AAA TACACS+ en plus des noms du service et des protocoles d'authentification TACACS+ définis sur le Cisco Secure ACS. La stratégie d'AAA TACACS+ détermine également les informations qui sont expédiées au serveur de comptabilité.

Cet exemple de stratégie de l'AAA TACACS définit un Cisco Secure ACS pour l'AAA TACACS+, définit les services TACACS+ et les protocoles nommés le RO et le MOTO RW MOTO, et active la commande CLI et la comptabilité de session.

Exemple de stratégie de l'AAA TACACS

```
aaa-tacacs-policy CISCO-ACS-SERVER

authentication server 1 host 192.168.10.21 secret 0 hellomoto

authorization server 1 host 192.168.10.21 secret 0 hellomoto

accounting server 1 host 192.168.10.21 secret 0 hellomoto

authentication service MOTO protocol RO

authentication service MOTO protocol RW

accounting commands

accounting session

!
```

Stratégies de Gestion

Une fois qu'une stratégie de l'AAA TACACS+ est définie, elle doit être assignée à un ou plusieurs stratégies de Gestion avant que TACACS+ soit utilisé. Les stratégies de Gestion déterminent les interfaces de gestion qui sont activées sur chaque périphérique de l'aile 5, utilisateurs administratifs locaux, rôles et autorisation d'accès, et les serveurs externes de RAYON ou TACACS+ utilisés afin d'authentifier les utilisateurs administratifs.

Par défaut, chaque périphérique de l'aile 5 est assigné à une stratégie de Gestion, nommée le par défaut, qui est assigné avec l'utilisation des profils. TACACS+ peut être activé sur la stratégie de gestion par défaut ou n'importe quelle stratégie de Gestion définie par l'utilisateur.

La plupart des déploiements typiques incluent des stratégies de Gestion distinctes pour des contrôleurs sans-fil et des Points d'accès. Des stratégies de Gestion distinctes sont recommandées, parce que les besoins en matière de gestion et les interfaces pour chaque périphérique diffèrent. Dans ce cas, TACACS+ doit être activé sur chaque stratégie de Gestion afin d'activer TACACS+ sur des contrôleurs sans-fil et des Points d'accès.

Les exemples de stratégie de Gestion dans la section suivante activent l'AAA TACACS+ sur les stratégies de Gestion définies par l'utilisateur qui sont assignées aux contrôleurs sans-fil et aux Points d'accès. Le retour TACACS+ à l'authentification locale est également activé au cas où un périphérique de l'aile 5 ne pourrait atteindre aucun serveurs définis TACACS+ pour l'authentification.

Exemples de stratégie de Gestion

```
!

management-policy CONTROLLER-MANAGEMENT

no http server

https server

ssh
```

```
user admin password 0 hellomoto role superuser access all

snmp-server user snmptrap v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpoperator v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpmanager v3 encrypted des auth md5 0 hellomoto

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!

!

management-policy AP-MANAGEMENT

ssh

user admin password 0 hellomoto role superuser access all

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!
```

Vérifiez

Cette section fournit l'étape nécessaire nécessaire afin de valider l'AAA TACACS+. Dans cet exemple, deux comptes utilisateurs sont définis sur chaque Cisco Secure ACS et assignés aux groupes appropriés. L'adhésion à des associations de l'utilisateur détermine le rôle et l'autorisation d'accès assignés à l'utilisateur de Gestion.

```
Username           Role          Access Permissions
-----------------------------------------------------
monitor Monitor Web
super user Superuser all
```

Affectation de rôle

Cette section fournit l'étape nécessaire de vérification afin de vérifier des affectations d'authentification et de rôle.

Sur le Web UI, procédure de connexion au contrôleur sans-fil avec le nom d'utilisateur et mot de passe de **moniteur** :

L'utilisateur est authentifié, autorisé, et assigné au rôle de moniteur, qui fournit seulement l'accès

lu sur le contrôleur sans-fil. **Configuration > périphériques** choisis, et tentative d'éditer un périphérique.

> **Note**: Aucun éditez la fonctionnalité est disponible, parce qu'on permet à l'utilisateur seulement l'accès lu.

Access sur le périphérique : (Seulement le bouton de **vue** est disponible ; le bouton d'**effacement** est greyed-.)

Sur le Web UI, procédure de connexion au contrôleur sans-fil avec le nom d'utilisateur et mot de passe de **super utilisateur** :

L'utilisateur est authentifié, autorisé, et assigné au rôle de super utilisateur, qui fournit l'accès complet sur le contrôleur sans-fil. **Configuration > périphériques** choisis, et tentative d'éditer un périphérique.

> **Note**: Le bouton d'**éditer** est maintenant disponible, parce qu'on permet à l'utilisateur l'accès complet sur le périphérique.

Dépannez

Sur la version 5.X de Cisco Secure ACS, naviguez vers la **surveillance et les états > la surveillance et la visionneuse de rapports de lancement > sélectionnent les états > le catalogue > le protocole AAA > l'authentification TACACS > exécuté**.

Ceci présente les résultats pour tous les passé et authentifications défaillantes pour des utilisateurs et inclut la raison de panne. Cliquez sur le bouton de **loupe** (détails) pour d'autres détails.