

Intégration de système de FireSIGHT avec ACS 5.x pour l'authentification d'utilisateur RADIUS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configuration](#)

[Configuration ACS 5.x](#)

[Configurer des périphériques et des groupes de périphériques réseau de réseau](#)

[Ajouter un groupe d'Idenity dans ACS](#)

[Ajouter un utilisateur local à ACS](#)

[Configurer la stratégie ACS](#)

[Configuration de centre de Gestion de FireSIGHT](#)

[Configuration de politique de système de gestionnaire de FireSIGHT](#)

[Authentification externe d'enable](#)

[Vérification](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit l'étape nécessaire de configuration pour intégrer un centre de Gestion de Cisco FireSIGHT (FMC) ou le périphérique géré de FirePOWER avec le Système de contrôle d'accès sécurisé Cisco 5.x (ACS) pour l'authentification à distance se connectent l'authentification de l'utilisateur de service d'utilisateur (RADIUS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration initiale de système et de périphérique géré de FireSIGHT par l'intermédiaire de GUI et/ou de shell
- Configurer des stratégies d'authentification et d'autorisation sur ACS 5.x
- La connaissance de base de RADIUS

[Composants utilisés](#)

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

- Système de contrôle d'accès sécurisé Cisco 5.7 (ACS 5.7)
- Centre 5.4.1 de gestionnaire de Cisco FireSIGHT

Au-dessus des versions sont les dernières versions disponibles actuellement. La caractéristique est prise en charge sur toutes les versions ACS 5.x et versions FMC 5.x.

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.

Configuration

Configuration ACS 5.x

Configurer des périphériques et des groupes de périphériques réseau de réseau

- Du GUI ACS, naviguez vers le **groupe de périphériques réseau**, cliquez sur en fonction le **type de périphérique** et créez un groupe de périphériques. Dans le tir d'écran d'exemple qui suit, le type de périphérique FireSIGHT a été configuré. Ce type de périphérique sera mis en référence dans la définition de règle de stratégie d'autorisation dans une étape postérieure. Cliquez sur **Save**.

The screenshot shows the ACS GUI interface. On the left is a navigation pane with 'Network Resources' expanded to 'Device Type'. The main area shows the configuration for 'Device Group - General'. The 'Name' field is set to 'FireSight', the 'Parent' is 'All Device Types', and there is a 'Select' button. A legend indicates that orange asterisks denote required fields.

Network Resources > Network Device Groups > Device Type > Edit: "Device Type:All Device Types:FireSight"

Device Group - General

* Name:

Description:

* Parent:

* = Required fields

- Du GUI ACS, naviguez vers le **groupe de périphériques réseau**, cliquez sur en fonction les **clients de NetworkDevices et d'AAA** et ajoutez un périphérique. Fournissez un nom et une adresse IP descriptifs de périphérique. Le centre de Gestion de FireSIGHT est défini dans l'exemple ci-dessous.

Network Resources > Network Devices and AAA Clients > Edit: "FireSight Management Center"

Name: FireSight Management Center
Description:

Network Device Groups
Location: All Locations [Select]
Device Type: All Device Types:FireSight [Select]

IP Address
 Single IP Address IP Subnets IP Range(s)
 IP: 10.150.176.224

Authentication Options
 TACACS+ RADIUS
 Shared Secret: ***** [Show]
 CoA port: 1700
 Enable KeyWrap
 Key Encryption Key:
 Message Authenticator Code Key:
 Key Input Format: ASCII HEXADECIMAL

* = Required fields

Submit Cancel

- Aux groupes de périphériques réseau, configurez le **type de périphérique** mêmes que le groupe de périphériques créé dans l'étape ci-dessus.
- Cochez la case à côté des **options d'authentification**, sélectionnez la case de RADIUS et introduisez la clé **secrète partagée** qui sera utilisée pour ce NAD. Notez la même chose la clé que secrète partagée sera utilisée de nouveau plus tard quand configurant le serveur de RADIUS au centre de Gestion de FireSIGHT. Pour passer en revue la valeur principale de texte brut, cliquez sur le bouton d'**exposition**. Cliquez sur **Submit**.
- Répétez les étapes ci-dessus pour tous les centres et périphériques gérés de Gestion de FireSIGHT qui exigeront l'authentification d'utilisateur RADIUS/autorisation pour l'accès GUI et/ou de shell.

Ajouter un groupe d'Idenity dans ACS

- Naviguez vers des **utilisateurs et les mémoires d'identité**, configurent le **groupe d'identité**. Dans cet exemple, le groupe d'identité créé est « administrateur de FireSIGHT ». Ce groupe sera lié au profil d'autorisation défini dans les étapes ci-dessous.

Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:FireSight Administrator"

General

- Name: FireSight Administrator
- Description:
- Parent: All Groups

= Required fields

Ajouter un utilisateur local à ACS

- Naviguez vers des **utilisateurs et les mémoires d'identité**, configurez des **utilisateurs** dans la section **interne de mémoires d'identité**. Entrez les informations requises pour la création d'utilisateur local, sélectionnez le **groupe d'identité** créé dedans au-dessus de l'étape et cliquez sur Submit.

Users and Identity Stores > Internal Identity Stores > Users > Edit: "test"

General

- Name: test Status: Enabled
- Description:
- Identity Group: All Groups:FireSight Administrator
- Email Address:

Account Disable

- Disable Account if Date Exceeds: 2015-Nov-01
- Disable account after 3 successive failed attempts

Password Hash

- Enable Password Hash

Applicable only for Internal Users to store password as hash. Authentication types CHAP/MSCHAP will not work if this option is enabled. While disabling the hash, ensure that password is reconfigured using change password option.

Password Lifetime

- Password Never Expired/Disabled: Overwrites user account blocking in case password expired/disabled

User Information

There are no additional identity attributes defined for user records

Creation/Modification Information

- Date Created: Wed Sep 02 13:15:56 UTC 2015
- Date Modified: Wed Sep 02 23:12:39 UTC 2015
- Date Enabled: Wed Sep 02 13:15:56 UTC 2015

= Required fields

Configurer la stratégie ACS

- Dans le GUI ACS, naviguez vers des **éléments de stratégie > l'autorisation et des autorisations > des profils d'accès au réseau > d'autorisation**. Créez un nouveau profil d'autorisation avec un nom descriptif. Dans l'exemple ci-dessous, la stratégie créée est administrateur de FireSIGHT.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"

General Common Tasks RADIUS Attributes

Name: FireSight Administrator

Description:

= Required fields

- Dans les **attributs RADIUS** tabulez, ajoutez l'attribut manuel pour autoriser le groupe d'identité créé ci-dessus et cliquez sur Submit

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Class	String	Groups:FireSight Administrator

Add ^ Edit V Replace ^ Delete

Dictionary Type: RADIUS-IETF

RADIUS Attribute: Class Select

Attribute Type: String

Attribute Value: Static

Groups:FireSight Administrator

= Required fields

Submit Cancel

- Naviguez pour accéder à **des stratégies > des services d'accès > l'accès au réseau > l'autorisation de par défaut** et pour configurer une nouvelle stratégie d'autorisation pour les sessions de gestion de centre de Gestion de FireSIGHT. L'exemple ci-dessous utilise le **NDG** : État de **groupe de type de périphérique** et d'identité pour appairer le groupe configuré de type de périphérique et d'identité dans les étapes ci-dessus.

- Cette stratégie est alors associée avec le profil d'autorisation d'administrateur de FireSIGHT configuré au-dessus de l'en conséquence. Cliquez sur **Submit**.

Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | [Exception Policy](#)

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	Status	Name	Conditions	Results	Hit Count
1	<input checked="" type="checkbox"/>	Rule-1	NDG:Device Type in All Device Types:FireSight	Identity Group in All Groups:FireSight Administrator Authorization Profiles FireSight Administrator	7

Configuration de centre de Gestion de FireSIGHT

Configuration de politique de système de gestionnaire de FireSIGHT

- Ouvrez une session à FireSIGHT MC et naviguez vers le **système > les gens du pays > la gestion des utilisateurs**. Cliquez sur en fonction le clic de tableau d'**authentification externe + créent le** bouton d'**objet d'authentification** pour ajouter un nouveau serveur de RADIUS pour l'authentification de l'utilisateur/autorisation.
- **RADIUS** choisi pour la **méthode d'authentification**. Écrivez un nom descriptif pour le serveur de RADIUS. **Clé** écrivez le **nom d'hôte/adresse IP** et de **RADIUS secret**. La clé secrète devrait apparier la clé précédemment configurée sur ACS. Écrivez sur option un **nom d'hôte de serveur ACS/adresse IP** de sauvegarde si on existe.

Overview Analysis Policies Devices Objects AMP Health System

Local > User Management Updates Licenses Mor

Users User Roles External Authentication

External Authentication Object

Authentication Method: RADIUS

Name *: ACS

Description:

Primary Server

Host Name/IP Address *: 172.18.75.172 ex. IP or hostname

Port *: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address: ex. IP or hostname

Port: 1812

RADIUS Secret Key:

- Sous la section de **paramètres de RADIUS-particularité**, dans cet exemple, le Class=Groups : La valeur d'administrateur de FireSIGHT est tracée au groupe d'administrateur de FireSIGHT. C'est la valeur qu'ACS renvoie en tant qu'élément de l'ACCESS-ACCEPT. Cliquez sur la **sauvegarde** pour sauvegarder la configuration ou pour procéder à la section de vérifier ci-dessous au test d'authentification à ACS.

RADIUS-Specific Parameters

Timeout (Seconds)

Retries

Access Admin

Administrator

- Sous le **filtre d'Access de shell**, écrivez une virgule liste séparée d'utilisateurs pour limiter des sessions shell/SSH.

Shell Access Filter

Administrator Shell Access
User List

Authentification externe d'enable

En conclusion, terminez-vous ces étapes afin d'activer l'authentification externe sur le FMC :

1. Naviguez vers le **système** > la **stratégie de gens du pays** > de **système**.
2. **Authentification externe** choisie sur le panneau gauche.
3. Changez l'*état* à **activer** (désactivé par défaut).
4. Activez le serveur ajouté ACS RADIUS.
5. Sauvegardez la stratégie et réappliquez la stratégie sur l'appliance.

Vérification

- Pour tester l'authentification de l'utilisateur contre ACS, faites descendre l'écran à la section **supplémentaire de paramètres de test** et écrivez un nom d'utilisateur et mot de passe pour l'utilisateur ACS. **Test de clic**. Un essai réussi aura comme conséquence un succès **vert** : Message complet de test en haut de la fenêtre du navigateur.

Additional Test Parameters

User Name

Password



Success



Test Complete.

- Pour visualiser les résultats du test d'authentification, aller à la **section de sortie de test** et cliquer sur la flèche **noire** à côté des **détails d'exposition**. Dans le tir d'écran d'exemple ci-dessous, notez le « radiusauth - réponse : [Class=Groups : Administrateur de FireSIGHT] » valeur reçue d'ACS. Ceci devrait appairer la valeur de classe associée avec le groupe configuré local de FireSIGHT sur FireSIGHT MC ci-dessus. Cliquez sur **Save**.

Test Output

Show Details



```
check_auth_radius: szUser: test
RADIUS config file: /var/tmp/_bcEn4h_wF/radiusclient_0.conf
radiusauth - response: [User-Name=test]
radiusauth - response: [Class=Groups:FireSight Administrator]
radiusauth - response: [Class=CACS: ████████-acs/229310634/47]
"test" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Groups:FireSight Administrator] - [Class=Groups:FireSight Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

User Test

*Required Field

Save

Test

Cancel