

Configurez et dépannez les serveurs TACACS externes sur ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurez ISE](#)

[Configurez ACS](#)

[Vérifiez](#)

[Dépannez](#)

Introduction

Ce document décrit la caractéristique pour utiliser le serveur externe TACACS+ dans un déploiement utilisant la gestion d'identité Engine(ISE) comme proxy.

Conditions préalables

Conditions requises

- Compréhension de base de gestion de périphérique sur ISE.
- Ce document est basé sur la version 2.0 d'engine de gestion d'identité, applicable sur n'importe quelle version du supérieur à 2.0 de version d'engine de gestion d'identité.

Composants utilisés

Note: N'importe quelle référence à ACS dans ce document peut être interprétée pour être une référence à n'importe quel serveur externe TACACS+. Cependant, la configuration sur l'ACS et la configuration sur n'importe quel autre serveur TACACS peuvent varier.

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

- Engine 2.0 de gestion d'identité
- Système de contrôle d'accès (ACS) 5.7

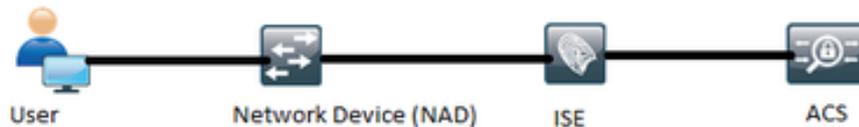
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que

vous comprenez l'impact potentiel de n'importe quelle modification de configuration.

Configurez

Cette section aide à configurer ISE aux demandes du proxy TACACS+ à ACS.

Diagramme du réseau



Configurez ISE

1. Des serveurs TACACS externes de multiple peuvent être configurés sur ISE et peuvent être utilisés pour authentifier les utilisateurs. Afin de configurer le serveur externe TACACS+ sur ISE, naviguez vers les **centres de travail > la gestion de périphérique > les ressources de réseau > les serveurs externes TACACS**. Cliquez sur Add et complétez les coordonnées des petits groupes de serveur externe.

La capture d'écran montre l'interface de configuration d'un serveur externe TACACS dans l'Identity Services Engine. Le menu de gauche indique la navigation : TrustSec > Device Administration > Network Resources > TACACS External Servers > External_Server. Le formulaire principal contient les champs suivants :

- Name : External_Server
- Description : External TACACS Server
- Host IP : 10.127.196.237
- Connection Port : 49 (1-65,535)
- Timeout : 20 Seconds (1-999)
- Shared Secret : ***** (avec un bouton Show Secret)
- Use Single Connect :

Des boutons Cancel et Save sont situés en bas à droite.

Le secret partagé fourni dans cette section doit être le même secret utilisé dans l'ACS.

2. Afin d'utiliser le serveur TACACS externe configuré, il doit ajouter dans un ordre de serveur TACACS à utiliser dans les positionnements de stratégie. Je passe commande pour configurer l'ordre de serveur TACACS, navigue vers les **centres de travail > la gestion de**

périphérique > les ressources de réseau > l'ordre de serveur TACACS. Cliquez sur Add, complétez les détails et choisissez les serveurs qui sont nécessaires pour être utilisés dans cet ordre.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a TACACS Server Sequence. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > TrustSec > Device Administration > Network Resources. The main configuration area is titled 'Server Sequence' and includes the following fields and options:

- Name:** External_Server_Sequence
- Description:** Sequence for External Servers
- Server List:** The TACACS Proxy Servers selected will be tried in order. It consists of two columns: 'Available' (empty) and 'Chosen' (containing 'External_Server').
- Logging Control:** Accounting requests should be handled. Options include 'Local Accounting' and 'Remote Accounting'.
- Username Stripping:** Options include 'Prefix Strip' (with a dropdown set to '1') and 'Suffix Strip' (with a dropdown set to '@').

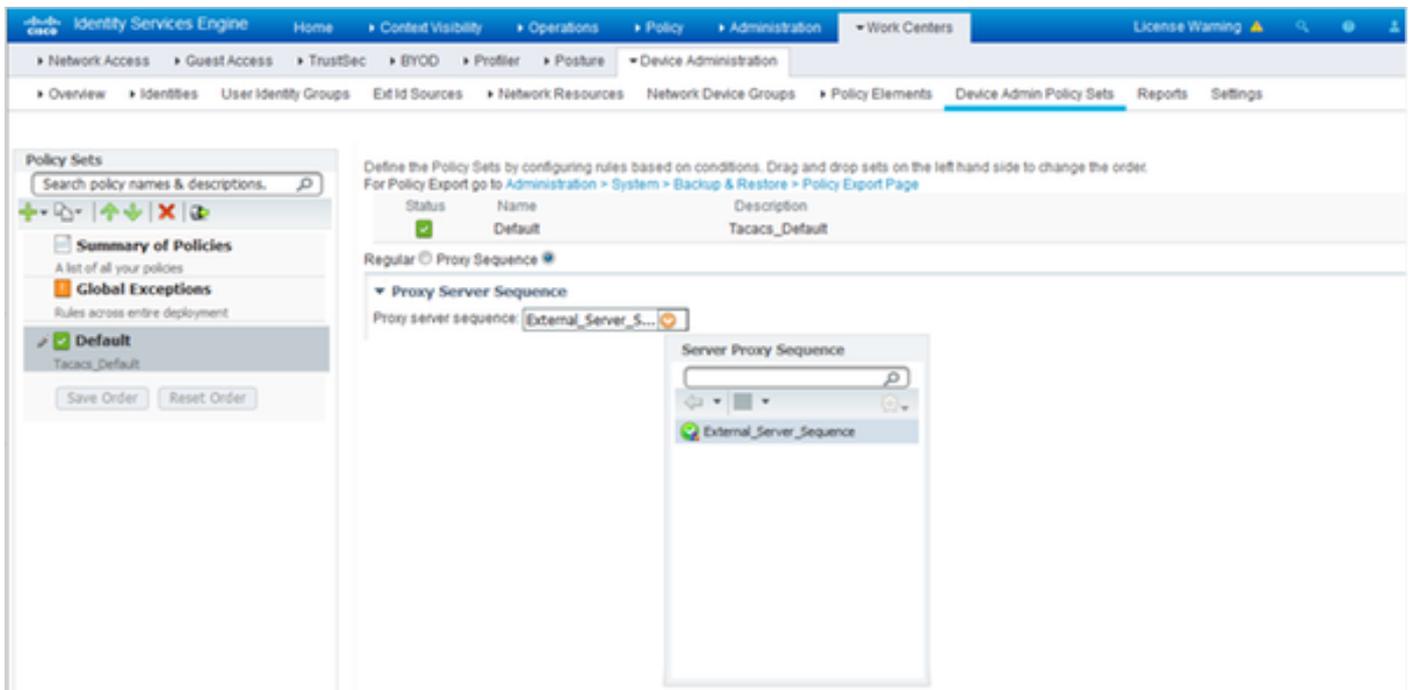
Buttons for 'Choose all' and 'Clear all' are located below the server list. At the bottom right, there are 'Cancel' and 'Submit' buttons.

En plus de l'ordre de serveur, deux autres options ont été fournies. Se connecter le contrôle et éliminer de nom d'utilisateur.

Se connecter le contrôle donne à une option au log les demandes de comptabilité localement sur ISE ou se connecte les demandes de comptabilité au serveur externe qui manipule l'authentification aussi bien.

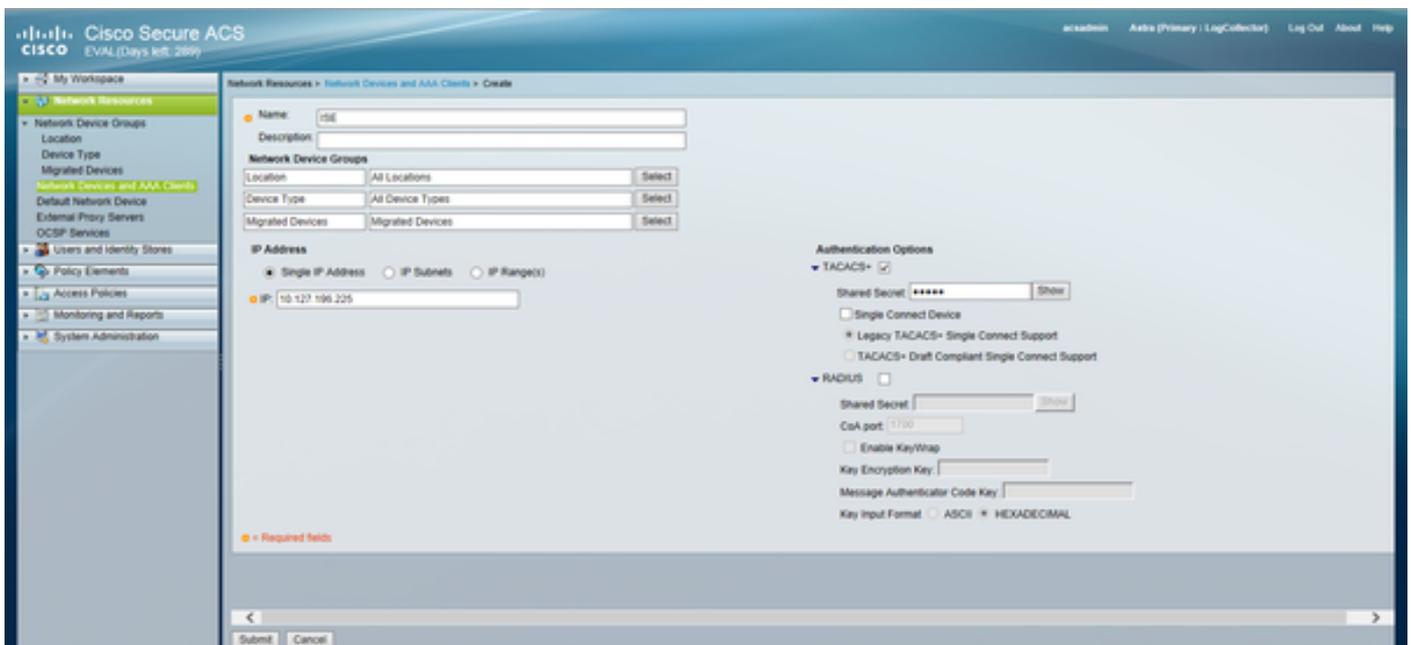
Éliminer de nom d'utilisateur est utilisé pour éliminer le préfixe ou le suffixe par sepcifying un délimiteur avant d'expédier la demande à un serveur TACACS externe.

3. Pour utiliser l'ordre externe de serveur TACACS configuré, les positionnements de stratégie doivent être configurés pour utiliser l'ordre créé. Afin de configurer les positionnements de stratégie pour utiliser l'ordre de serveur externe, naviguez vers des **centres de travail > des positionnements de stratégie d'admin de gestion de périphérique > de périphérique > [sélectionnez la stratégie réglée]**. Case d'option à bascule qui indique l'ordre de proxy. Choisissez l'ordre de serveur externe créé.

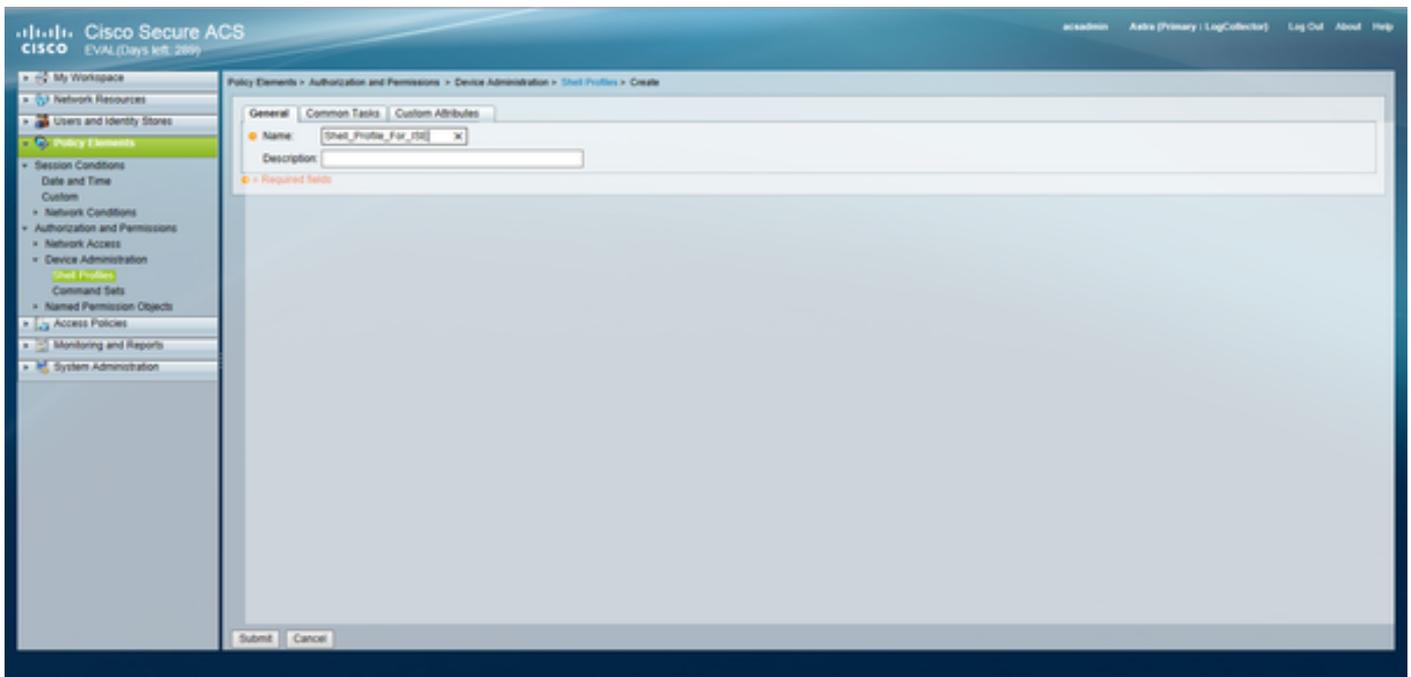


Configurez ACS

Pour l'ACS, ISE est juste un autre périphérique de réseau qui enverra une demande TACACS. Afin de configurer ISE comme périphérique de réseau dans ACS, naviguez vers des **ressources de réseau > des périphériques de réseau et des clients d'AAA**. Le clic **créent** et complètent les coordonnées du serveur ISE utilisant la même chose secret partagé que configuré sur l'ISE.



Configurez les paramètres de gestion de périphérique sur ACS qui sont, les profils de shell et les positionnements de commande. Afin de configurer des profils de shell, naviguez des **profils vers des éléments de stratégie > l'autorisation et des autorisations > de périphérique gestion > shell**. Cliquez sur **créent** et configurent le nom, les fonctionnalités usuelles et les attributs personnalisés selon la condition requise.



Les positionnements de commande de configuration, naviguent vers des **éléments de stratégie > l'autorisation et les autorisations > la gestion > la commande de périphérique place**. Le clic **créent** et complètent les détails selon la condition requise.

General
Name: Status: 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 Protocol:

Results
Service:

Configurez le service d'accès sélectionné dans la règle de sélection de service selon la condition requise. Afin de configurer des règles de service d'accès, naviguez **admin > identité de périphérique pour accéder à de stratégies > de services d'accès >Default** où la mémoire d'identité qui doit être utilisée peut être sélectionnée pour l'authentification. Les règles d'autorisation peuvent être configurées en naviguant **admin > autorisation de périphérique pour accéder à de stratégies > de services d'accès >Default**.

Note: La configuration des stratégies d'autorisation et des profles de shell pour des appareils spécifiques peut varier et c'est hors de portée de ce document.

Vérifiez

Employez cette section pour confirmer que la configuration fonctionne correctement.

La vérification peut être faite sur l'ISE et l'ACS. N'importe quelle erreur dans la configuration de l'ISE ou de l'ACS aura comme conséquence un échec d'authentification. ACS est le serveur primaire qui traitera l'authentification et les demandes d'autorisation, ISE porte la responsabilité à

et du serveur ACS et agit en tant que proxy pour les demandes. Puisque le paquet traverse par les les deux les serveurs, la vérification de l'authentification ou de la demande d'autorisation peut être faite sur les les deux les serveurs.

Des périphériques de réseau ne sont configurés avec ISE comme serveur TACACS et pas ACS. Par conséquent la demande atteint ISE d'abord et basé sur les règles configurées, ISE décide si la demande doit être expédiée à un serveur externe. Ceci peut être vérifié dans le TACACS vivant ouvre une session l'ISE.

Afin de visualiser le vivant ouvre une session l'ISE, naviguent vers des **exécutions > TACACS > vivent des logs**. Des états vivants peuvent être vus à cette page et les détails d'une demande particulière peuvent être vérifiés en cliquant sur l'icône de loupe concernant cette demande spécifique qui est d'intérêt.

Steps

- 13020 Get TACACS+ default network device setting
- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.Protocol
- 15006 Matched Default Rule
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.
- 13020 Get TACACS+ default network device setting
- 13014 Received TACACS+ Authentication CONTINUE Request
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13071 Continue flow (seq_no > 1).
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.

Afin de visualiser les états d'authentification sur l'ACS, naviguez vers la **surveillance et les états > la surveillance de lancement et la visionneuse de rapports > la surveillance et les états > les états**

> le protocole AAA > l'authentification TACACS. Comme ISE, les détails d'une demande particulière peuvent être vérifiés en cliquant sur l'icône de loupe concernant cette demande spécifique qui est d'intérêt

Steps
Message
Received TACACS+ Authentication START Request
Evaluating Service Selection Policy
Matched rule
Selected Access Service - Default Device Admin
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
TACACS+ will use the password prompt from global TACACS+ configuration.
Returned TACACS+ Authentication Reply
Received TACACS+ Authentication CONTINUE Request
Using previously selected Access Service
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
Authentication Passed
Evaluating Group Mapping Policy
Evaluating Exception Authorization Policy
No rule was matched
Evaluating Authorization Policy
Matched Default Rule
Returned TACACS+ Authentication Reply

Dépannez

Cette section fournit des informations que vous pouvez employer pour dépanner votre configuration

1. Si les détails de l'état sur ISE affichent le message d'erreur représenté sur la figure, alors elle indique un secret partagé non valide configuré sur l'ISE ou le périphérique de Netowrk (NAD).

Message Text

TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. S'il n'y a aucun état d'authentification pour une demande sur l'ISE mais l'accès est refusé à l'utilisateur final à un périphérique de réseau, ceci indique habituellement plusieurs choses.

- La demande elle-même n'a fait aucune portée le serveur ISE.
- Si la Person de gestion de périphérique est désactivée sur ISE, alors n'importe quelle demande TACACS+ à ISE sera abandonnée silencieusement. Aucun log indiquant la même chose ne sera affiché dans les états ou les logs vivants. Pour vérifier ceci, naviguez vers la **gestion > le système > le déploiement > [sélectionnez le noeud]**. Cliquez sur Edit et notez la case « de **service d'admin de périphérique d'enable** » sous l'onglet de **paramètres généraux** suivant les indications de la figure. Que la case à cocher doit être vérifiée la gestion de périphérique à travailler à ISE.

Personas

Administration Role **PRIMARY**

Monitoring Role PRIMARY Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group None

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service Use Interface GigabitEthernet 0

Enable Device Admin Service

Enable Passive Identity Service

pxGrid

- Si un permis de gestion de périphérique n'est pas présent d'expirer, alors toutes les demandes TACACS+ sont abandonnées silencieusement. Aucun log n'est affiché dans le GUI pour la même chose. Naviguez vers la **gestion > le système > en autorisant** à vérifier le permis de gestion de périphérique.

Licenses How do I register/modify or lookup my licenses?

License File	Quantity	Term	Expiration Date
EVALUATION Lic			
Base	100	90 days	⚠ 22-Jan-2017 (43 days remaining)
Plus	100	90 days	⚠ 22-Jan-2017 (43 days remaining)
Apex	100	90 days	⚠ 22-Jan-2017 (43 days remaining)
Wired	100	90 days	⚠ 22-Jan-2017 (43 days remaining)
Device Admin	Uncounted	90 days	⚠ 22-Jan-2017 (43 days remaining)

- Si le périphérique de réseau n'est pas configuré ou si un IP faux de périphérique de réseau est configuré sur l'ISE, alors ISE relâchera silencieusement le paquet. Aucune réponse n'est renvoyée au client et aucun log n'est affiché dans le GUI. C'est un changement du comportement d'ISE pour TACACS+ une fois comparé à cela d'ACS qui informe que la demande est entrée d'un périphérique de réseau d'unknown ou d'un client d'AAA.
- La demande a atteint l'ACS mais la réponse n'est pas revenue à l'ISE. Ce scénario peut être vérifié des états sur l'ACS suivant les indications de la figure. Habituellement c'est en raison d'un secret partagé non valide sur l'ACS configuré pour ISE ou sur l'ISE configuré pour l'ACS.

Steps

Message

Received TACACS+ Authentication START Request
Invalid TACACS+ request packet - possibly mismatched Shared Secrets

- La réponse ne sera pas envoyée même si l'ISE n'est pas configuré ou l'adresse IP de l'interface de gestion d'ISE n'est pas configurée sur l'ACS dans la configuration de périphérique de réseau. Dans un tel scénario, on peut observer le message dans la figure sur l'ACS.

Steps

Message

Received TACACS+ packet from unknown Network Device or AAA Client

- Si un état réussi d'authentification est vu sur l'ACS mais aucun état n'est vu sur l'ISE et l'utilisateur est rejeté, alors ce pourrait très bien être une question dans le réseau. Ceci peut être vérifié par une capture de paquet sur ISE avec les filtres nécessaires. Pour collecter une capture de paquet sur ISE, naviguez vers des **exécutions > dépannant > des outils de diagnostic > les outils généraux > le vidage mémoire de TCP**.

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Stopped

Host Name

Network Interface

Promiscuous Mode On Off

Filter

Example: 'ip host helios and not iceberg'

Format

Dump File Last created on Fri Dec 09 20:51:18 IST 2016
File size: 9,606 bytes
Format: Raw Packet Data
Host Name: tornado
Network Interface: GigabitEthernet 0
Promiscuous Mode: On

3. Si les états peuvent être vus sur ISE mais pas sur l'ACS, il pourrait l'un ou l'autre de moyen que la demande n'a pas atteint l'ACS en raison d'une mauvaise configuration des positionnements de stratégie sur ISE qui peut être dépanné a basé sur le rapport détaillé sur ISE ou en raison d'un problème de réseau qui peut être identifié par une capture de paquet sur l'ACS.

4. Si les états sont vus sur ISE et l'ACS mais utilisateur est refusés toujours l'accès, alors c'est plus souvent une question dans la configuration de stratégies d'Access sur ACS qui peut être dépanné a basé sur le rapport détaillé sur l'ACS. En outre, on doit permettre le trafic de retour de l'ISE au périphérique de Network.