Exemple de configuration de l'affectation de groupe de stratégies pour les clients AnyConnect qui utilisent LDAP sur les têtes de réseau Cisco IOS

Contenu

Introduction

Ce document décrit comment configurer des mappages d'attributs LDAP (Lightweight Directory Access Protocol) pour attribuer automatiquement la stratégie VPN correcte à un utilisateur en fonction de ses informations d'identification.

> **Note**: La prise en charge de l'authentification LDAP pour les utilisateurs VPN SSL (Secure Sockets Layer VPN) qui se connectent à une tête de réseau Cisco IOS® est suivie par l'ID de bogue Cisco CSCuj20940. Tant que le support n'est pas officiellement ajouté, le support LDAP est le meilleur effort.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN SSL sur Cisco IOS
- Authentification LDAP sur Cisco IOS

- Services d'annuaire

Components Used

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

- CISCO881-SEC-K9
- Logiciel Cisco IOS, Logiciel C880 (C880DATA-UNIVERSALK9-M), Version 15.1(4)M, VERSION LOGICIELLE (fc1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le protocole LDAP est un protocole d'application standard ouvert, neutre pour les fournisseurs, qui permet d'accéder aux services d'informations d'annuaire distribués et de les gérer sur un réseau IP (Internet Protocol). Les services d'annuaire jouent un rôle important dans le développement d'applications intranet et Internet car ils permettent le partage d'informations sur les utilisateurs, les systèmes, les réseaux, les services et les applications sur l'ensemble du réseau.

Fréquemment, les administrateurs veulent fournir à des utilisateurs VPN différentes autorisations d'accès ou de contenu WebVPN. Ceci peut être complété par la configuration de différentes stratégies VPN sur le serveur VPN et l'attribution de ces jeux de stratégies à chaque utilisateur en fonction de leurs informations d'identification. Bien que cela puisse être effectué manuellement, il est plus efficace d'automatiser le processus avec les services d'annuaire. Afin d'utiliser LDAP pour affecter une stratégie de groupe à un utilisateur, vous devez configurer une carte qui mappe un attribut LDAP tel que l'attribut Active Directory (AD) « memberOf » à un attribut compris par la tête de réseau VPN.

Sur le dispositif de sécurité adaptatif (ASA), ceci est régulièrement réalisé par l'affectation de différentes stratégies de groupe à différents utilisateurs avec une carte d'attribut LDAP comme illustré dans l'Exemple de configuration de l'utilisation ASA des mappages d'attributs LDAP.

Sur Cisco IOS, la même chose peut être obtenue avec la configuration de différents groupes de politiques sous le contexte WebVPN et l'utilisation de mappages d'attributs LDAP afin de déterminer quel groupe de politiques l'utilisateur sera affecté. Sur les têtes de réseau Cisco IOS, l'attribut AD « memberOf » est mappé au groupe de supplicants d'attribut AAA (Authentication, Authorization, and Accounting). Pour plus d'informations sur les mappages d'attributs par défaut, consultez Exemple de configuration LDAP sur les périphériques IOS utilisant des mappages d'attributs dynamiques. Cependant, pour le VPN SSL, il existe deux mappages d'attributs AAA pertinents :

Nom d'attribut AAA	Pertinence VPN SSL
user-vpn-group	mappe au groupe de stratégies défini dans le contexte WebVPN
webvpn-context	mappe au contexte WebVPN lui-même

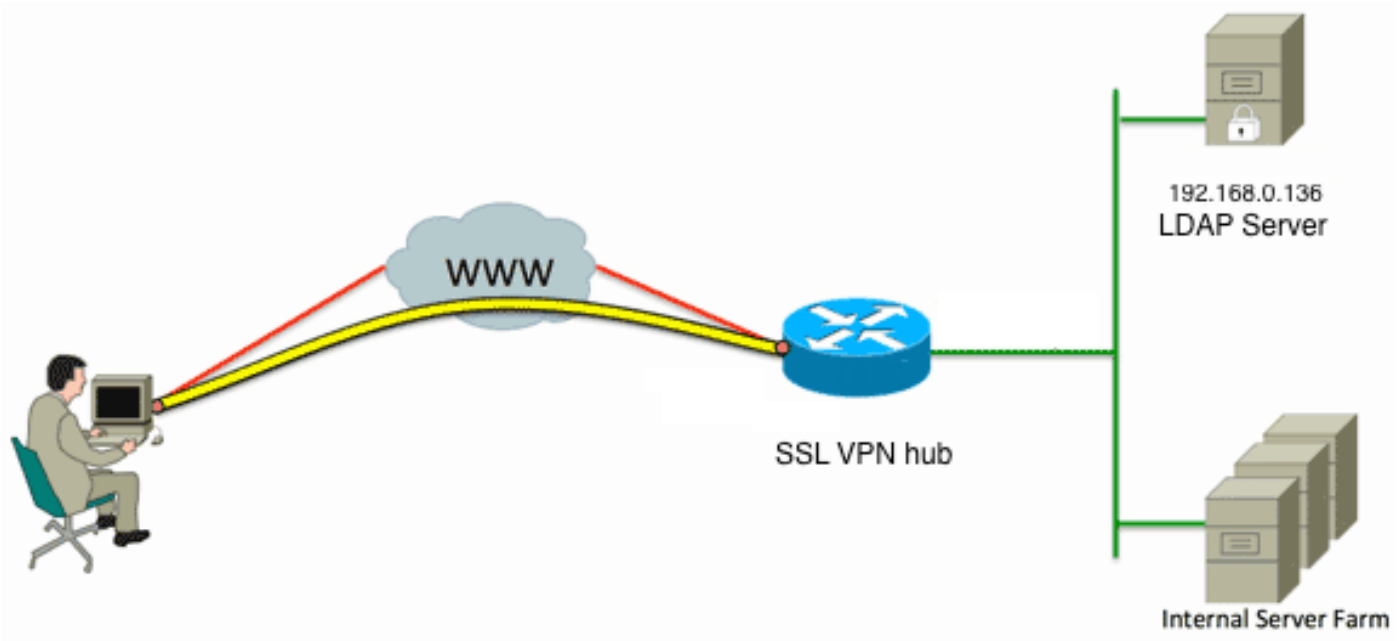
Par conséquent, la carte d'attribut LDAP doit mapper l'attribut LDAP approprié à l'un de ces deux

attributs AAA.

Configuration

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



Cette configuration utilise une carte d'attribut LDAP afin de mapper l'attribut LDAP « memberOf » à l'attribut AAA user-vpn-group.

1. Configurez la méthode d'authentification et le groupe de serveurs AAA.
```
aaa new-model
!
!
aaa group server ldap AD
 server DC1
!
aaa authentication login default local
aaa authentication login vpn local
aaa authentication login AD group ldap local
aaa authorization exec default local
```
2. Configurez une carte d'attribut LDAP.
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Configurez le serveur LDAP qui fait référence au mappage d'attribut LDAP précédent.
```
ldap server DC1
 ipv4 192.168.0.136
 attribute map ADMAP
 bind authenticate root-dn CN=Cisco Systems,OU=Service Accounts,DC=chillsthrills,
DC=local password 7 <removed>
 base-dn DC=chillsthrills,DC=local
```
4. Configurez le routeur pour qu'il agisse en tant que serveur WebVPN. Dans cet exemple,

étant donné que l'attribut « memberOf » sera mappé à l'attribut « user-vpn-group », un contexte WebVPN unique est configuré avec plusieurs groupes de stratégies qui incluent une stratégie « NOACCESS ». Ce groupe de stratégies est destiné aux utilisateurs qui n'ont pas de valeur « memberOf » correspondante.

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Cavates

1. Si l'utilisateur est un groupe multiple « memberOf », la première valeur « memberOf » est utilisée par le routeur.
2. Ce qui est étrange dans cette configuration, c'est que le nom du groupe de stratégies doit correspondre exactement à la chaîne **complète** poussée par le serveur LDAP pour la valeur « memberOf ». En règle générale, les administrateurs utilisent des noms plus courts et plus pertinents pour le groupe de stratégies, tels que VPNACCESS, mais en dehors du problème

cosmétique, cela peut conduire à un problème plus important. Il n'est pas rare que la chaîne d'attribut « memberOf » soit beaucoup plus grande que celle utilisée dans cet exemple. Par exemple, considérez ce message de débogage :

```
004090: Aug 23 08:26:57.235 PCTime: %SSLVPN-6-INVALID_RADIUS_CONFIGURATION:
Radius configured group policy "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,
DC=chillsthrills,DC=local" does not exist
```

Il montre clairement que la chaîne reçue d'AD est :

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

Cependant, comme aucun groupe de stratégies n'est défini, si l'administrateur tente de configurer une telle stratégie de groupe, il en résulte une erreur car Cisco IOS a une limite sur le nombre de caractères dans le nom du groupe de stratégies :

```
HOURTR1(config-webvpn-context)#webvpn context VPNACCESS
HOURTR1(config-webvpn-context)# policy group "CN=VPNACCESS,OU=Security Groups,
OU=MyBusiness,DC=chillsthrills,DC=local"
Error: group policy name cannot exceed 63 characters
```

Dans de telles situations, il existe deux solutions possibles :

1. Utilisez un attribut LDAP différent, tel que « service ».Considérez cette carte d'attribut LDAP :

   ```
   ldap attribute-map ADMAP
    map type department user-vpn-group
   ```

   Dans ce cas, la valeur de l'attribut de service pour un utilisateur peut être définie sur une valeur telle que VPNACCESS et la configuration WebVPN est un peu plus simple :

   ```
   webvpn context VPNACCESS
    secondary-color white
    title-color #669999
    text-color black
    ssl authenticate verify all
    !
    policy group NOACCESS
     banner "Access denied per user group restrictions in Active Directory.
   Please contact your system administrator or manager to request access."
    !
    policy group VPNACCESS
     functions svc-enabled
     banner "access-granted"
     svc address-pool "vpnpool"
     svc default-domain "cisco.com"
     svc keep-client-installed
     svc rekey method new-tunnel
     svc split dns "cisco.com"
     svc split include 192.168.0.0 255.255.255.0
     svc split include 10.10.10.0 255.255.255.0
     svc split include 172.16.254.0 255.255.255.0
     svc dns-server primary 192.168.0.136
    default-group-policy NOACCESS
    aaa authentication list AD
    gateway gateway_1
    inservice
   !
   end
   ```

2. Utilisez le mot clé DN-to-string dans le mappage d'attribut LDAP.Si la solution de contournement précédente n'est pas appropriée, l'administrateur peut utiliser le mot clé dn-to-string dans le mappage d'attribut LDAP afin d'extraire uniquement la valeur Common Name (CN) de la chaîne « memberOf ». Dans ce scénario, la carte d'attribut LDAP serait :

   ```
   ldap attribute-map ADMAP
    map type memberOf user-vpn-group format dn-to-string
   ```

   Et la configuration WebVPN serait :

   ```
   webvpn context VPNACCESS
   ```

```
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Note: Contrairement aux ASA où vous pouvez utiliser la commande **map value** sous une carte d'attribut afin de faire correspondre la valeur reçue du serveur LDAP à une autre valeur localement significative, les têtes de réseau Cisco IOS n'ont pas cette option et ne sont donc pas aussi flexibles. L'ID de bogue Cisco CSCts31840 a été enregistré afin de résoudre ce problème.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

- **show ldap attributs**
- **show ldap server all**

Dépannage

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

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Afin de dépanner le mappage d'attribut LDAP, activez ces débogages :

- debug ldap all
- debug ldap event
- debug aaa authentication
- debug aaa authorization