Admissions et LDAP IP ISR pour la redirection de Web à ScanSafe/à exemple de configuration sécurité Web de nuage

Contenu

Introduction

Ce document décrit comment configurer les Integrated Services Router de gamme Cisco G2 (ISR). Tandis que la configuration d'ip admission et de Protocole LDAP (Lightweight Directory Access Protocol) peut être utilisée simplement pour le Seveur mandataire d'authentification sur l'ISR, elle est typiquement utilisée en même temps que la caractéristique de redirection de la sécurité Web de nuage de Cisco (CWS). En soi, ce document est destiné pour être une référence afin de compléter la documentation de configuration et de dépannage de redirection CWS sur des ISR.

Conditions préalables

Conditions requises

Cisco recommande que votre rassemblement de système ces conditions requises avant que vous tentiez les configurations qui sont décrites dans ce document :

- L'ISR doit exécuter la version 15.2(1)T1 ou ultérieures de code.
- Votre système doit avoir les images avec le permis (sec) réglé par fonctionnalité de sécurité qui sont disponibles dans le Cisco IOS® (universel).
- Le poste de travail de client sur le domaine de Répertoire actif (AD) doit avoir la capacité pour exécuter l'authentification active par l'intermédiaire d'un navigateur Web.
- Vous devez avoir un abonnement CWS.

Composants utilisés

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

- Internet Explorer, Google Chrome, Mozilla Firefox (exige la configuration supplémentaire pour l'authentification transparente du LAN Manager de NT (NTLM))
- Cisco G2 800, 1900, 2900, et gamme 3900 ISR.

- Contrôleur de domaine d'AD de Microsoft Windows (ADDC)

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.

> Remarque: Cisco G1 1800, 2800, et des Routeurs de gamme 3800 ne sont pas pris en charge.

Informations générales

Beaucoup d'administrateurs qui installent la gamme Cisco G2 ISR qui n'ont pas les appliances de sécurité adaptable Cisco (ASA) dans leurs réseaux choisissent d'utiliser la fonctionnalité de redirection ISR CWS (autrefois ScanSafe) afin de tirer profit de la solution CWS pour le filtrage de Web. En tant qu'élément de cette solution, la plupart des administrateurs veulent également utiliser l'infrastructure en cours d'AD afin d'envoyer les informations d'identité de l'utilisateur aux towers CWS aux fins de l'application basée sur groupe d'utilisateur ou de stratégie pour les stratégies de filtrage de Web dans le portail CWS.

Le concept global est semblable à l'intégration entre l'ASA et l'agent de répertoire de contexte (CDA), avec quelques différences. La différence la plus notable est que l'ISR ne met pas à jour réellement une base de données passive du mappage utilisateur-à-IP, ainsi les utilisateurs doivent traverser un certain type d'authentification afin de transiter l'ISR et envoyer l'utilisateur ou l'information du groupe au portail CWS.

> **Conseil** : Référez-vous à la section de **méthodes d'authentification de** ce document pour plus d'informations sur les différences entre les diverses méthodes d'authentification qui sont disponibles.

Tandis que la partie de redirection CWS de la configuration qui est décrite dans ce document est relativement simple, quelques administrateurs pourraient rencontrer la difficulté avec des tentatives de configurer la partie d'authentification. Cette partie fonctionne avec la commande d'**ip admission** qui met en référence les instuctions d'authentification de serveurs LDAP et d'Authentification, autorisation et comptabilité (AAA) qui doivent également être configurées. Le but de ce document est de fournir à des opérateurs réseau une source de référence complète afin de configurer ou dépanner les admissions IP et les parties de LDAP de cette configuration sur la gamme Cisco G2 ISR.

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer Cisco ISR.

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

[Diagramme du réseau]

Configurez le LDAP

Terminez-vous ces étapes afin de configurer les propriétés de LDAP des serveurs d'AAA :

1. Configurez une carte d'attribut de LDAP afin de forcer le nom d'utilisateur qui est écrit par l'utilisateur pour apparier la propriété de **sAMAccountName** dans l'AD :
   ```
   C-881(config)#ldap attribute-map ldap-username-map map type sAMAccountName
    username
   C-881(config-attr-map)#map type sAMAccountName username
   ```
   Remarque: Cette configuration est exigée parce que l'attribut de **sAMAccountName** est une seule valeur dans l'AD, à la différence de l'attribut commun du nom (NC), qui est autrement utilisé afin de s'assortir par défaut. Par exemple, il peut y avoir des multiples instances de *John Smith* dans l'AD, mais il peut seulement y avoir un utilisateur avec le **sAMAccountName du** *jsmith*, qui est également la connexion de compte utilisateur. D'autres comptes de *John Smith* ont des **sAMAccountNames** tels que *jsmith1* ou *jsmith2*.
   La commande d'**attributs de show ldap** peut également être utilisée afin de visualiser une liste des attributs de LDAP et des attributs associés d'AAA.

2. Configurez le groupe de serveur LDAP :
   ```
   C-881(config)#aaa group server ldap LDAP_GROUP
   C-881(config-ldap-sg)#server DC01
   ```
3. Configurez les serveurs LDAP :
   ```
   C-881(config)#ldap server DC01
   C-881(config-ldap-server)# ipv4 10.10.10.150
   C-881(config-ldap-server)#attribute map ldap-username-map
   C-881(config-ldap-server)# bind authenticate root-dn CN=Csco_Service,CN=Users,
   DC=lab,DC=cisco,DC=com password Cisco12345!

   C-881(config-ldap-server)#base-dn DC=lab,DC=cisco,DC=com
   C-881(config-ldap-server)#search-filter user-object-type top
   C-881(config-ldap-server)#authentication bind-first
   ```

Cette configuration généralement n'exige pas la modification, à moins qu'il y ait un besoin d'implémenter un recherche-filtre fait sur commande. Seulement les administrateurs qui sont bien-versés dans le LDAP et savent entrer correctement ces informations devraient utiliser les filtres faits sur commande de recherche. Si vous êtes incertain au sujet du filtre de recherche qui devrait être utilisé, utilisez simplement le filtre décrit ; il localise les utilisateurs dans un environnement normal d'AD.

Une autre partie de la configuration de LDAP qui exige également l'attention aux détails particulière est les noms uniques (dn) qui sont exigés dans les commandes de grippage-authentifier-racine-**dn** et de base-**dn**. Ceux-ci doivent être entrés exactement pendant qu'ils apparaissent dans le serveur LDAP, ou les requêtes de LDAP échouent. En outre, la commande de base-**dn** doit être la partie la plus inférieure de l'arborescence de LDAP, où tous les utilisateurs qui sont authentifiés résident.

Considérez le scénario dans lequel la commande de base-**dn** dans la configuration précédente est modifiée comme ceci :

```
base-dn OU=TestCompany,DC=lab,DC=cisco,DC=com
```

Dans ce cas, la requête pour les utilisateurs qui sont inclus dans le **CN=Users, DC=lab, DC=cisco,**

DC=com ne renvoie aucun résultat, puisque le serveur LDAP recherche seulement l'unité organisationnelle de TestCompany (OU) et les objets d'enfant dans elle. En conséquence, l'authentification échoue toujours pour utilisateurs jusqu'à ce qu'ils soient entrés dans l'OU de TestCompany ou son sous-arbre, ou si la commande de base-**dn** est modifiée afin de l'inclure dans la requête.

> **Conseil** : Référez-vous à la **détermination que le DN objecte dans l'AD - ADSI éditent la** section de ce document pour des informations sur la façon déterminer les dn appropriés pour les commandes de base et de racine.

Configurez l'AAA

Maintenant que les serveurs LDAP sont configurés, vous devez les mettre en référence dans les instructions AAA correspondantes qui sont utilisées par le processus d'ip admission :

```
C-881(config)#aaa authentication login SCANSAFE_AUTH group LDAP_GROUP
C-881(config)#aaa authorization network SCANSAFE_AUTH group LDAP_GROUP
```

> Remarque: Si ces commandes ne sont pas disponibles, alors la commande d'**aaa new-model** pourrait devoir être sélectionnée afin d'activer cette fonctionnalité d'AAA parce qu'elle n'est pas activée par défaut.

Configurez l'ip admission

La partie d'ip admission déclenche un processus qui incite l'utilisateur pour l'authentification (ou exécute l'authentification transparente) et puis exécute des requêtes de LDAP basées sur les identifiants utilisateurs et les serveurs d'AAA qui sont définis dans la configuration. Si les utilisateurs sont authentifiés avec succès, les informations d'identité de l'utilisateur sont alors tirées par le processus de contenu-balayage et envoyées aux towers CWS, avec l'écoulement réorienté. Le processus d'ip admission n'est pas lancé jusqu'à ce que la commande d'**ip admission name** soit sélectionnée sur l'interface d'entrée du routeur. Par conséquent, cette partie de la configuration peut être mise en application sans n'importe quelle incidence du trafic.

```
C-881(config)#ip admission virtual-ip 1.1.1.1 virtual-host ISR_PROXY
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm
C-881(config)#ip admission name SCANSAFE_ADMISSION method-list authentication
 SCANSAFE_AUTH authorization SCANSAFE_AUTH
```

Ip admission d'enable

Voici la configuration qui est utilisée afin d'activer l'ip admission :

> Remarque: Ceci force les utilisateurs à authentifier, qui entraîne l'interruption de la circulation si l'authentification échoue.

```
C-881(config)#int vlan301 (internal LAN-facing interface)
C-881(config-if)#ip admission SCANSAFE_ADMISSION
```

Hôtes internes exempts de l'authentification

Quelques administrateurs pourraient désirer exempter quelques hôtes internes de la procédure d'authentification pour différentes raisons. Par exemple, il pourrait être indésirable pour les serveurs internes ou les périphériques qui ne sont pas capables de NTLM ou d'authentification de base à affecter par le processus d'admissions IP. Dans ces exemples, une liste de contrôle d'accès (ACL) peut être appliquée à la configuration d'ip admission afin d'empêcher l'hôte spécifique IPS ou les sous-réseaux de déclencher l'ip admission.

Dans cet exemple, l'hôte interne **10.10.10.150** est exempt de la condition requise de l'authentification, alors que l'authentification est encore exigée pour tous autres hôtes :

```
C-881(config)#ip access-list extended NO_ADMISSION
C-881(config-ext-nacl)#deny ip host 10.10.10.150 any
C-881(config-ext-nacl)#permit ip any any
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm list NO_ADMISSION
```

Activez le serveur HTTP sur l'ISR

On l'exige que vous permettez au serveur HTTP afin d'intercepter les sessions de HTTP et initier la procédure d'authentification :

```
Ip http server
Ip http secure-server
```

> Remarque: **L'ip http secure-server** est seulement nécessaire si la redirection à HTTPS pour l'authentification est exigée.

Configurez la redirection CWS

Voici une configuration récapitulative de base pour la redirection CWS :

```
Ip http server
Ip http secure-server
```

Configuration d'échantillon complète

Cette section fournit des exemples de configuration complets pour les sections précédentes.

LDAP

```
Ip http server
Ip http secure-server
```

AAA

```
Ip http server
Ip http secure-server
```

Ip admission

```
Ip http server
```

```
Ip http secure-server
```

Serveur HTTP

```
Ip http server
Ip http secure-server
```

Contenu-balayage et CWS

```
Ip http server
Ip http secure-server
```

Déterminez les objets de DN dans l'AD - ADSI éditent

Si nécessaire, il est possible de parcourir des dn d'une consultation de structure d'AD pour l'usage avec la base d'utilisateur ou de recherche de groupe. Les administrateurs peuvent utiliser un outil appelé l'*ADSI éditent* qui est construit dans des contrôleurs de domaine d'AD. Afin d'ouvrir ADSI éditez, choisissez le **Start > Run** sur le contrôleur de domaine d'AD et écrivez **adsiedit.msc.**

Une fois qu'ADSI Edit est ouvert, cliquez avec le bouton droit n'importe quel objet, tel qu'une OU, groupe, ou utilisateur, et choisissez Properties afin de visualiser le DN de cet objet. La chaîne de DN peut alors être facilement copiée et collée à la configuration de routeur afin d'éviter toutes les erreurs typographiques. Cette image illustre le processus :

Méthodes d'authentification

Il y a quatre types différents de méthodes d'authentification disponibles qui utilisent l'ip admission, et ils sont souvent mal compris, particulièrement la différence entre NTLM transparent et passif. Les sections suivantes décrivent les différences entre ces types d'authentification.

NTLM actif

La méthode d'authentification active NTLM incite des utilisateurs pour l'authentification quand l'authentification transparente NTLM échoue. C'est habituellement dû au fait que le navigateur de client ne prend en charge pas l'authentification intégrée de Microsoft Windows ou parce que l'utilisateur s'est connecté dans le poste de travail avec les qualifications locales (de non-domaine). L'authentification active NTLM exécute des requêtes de LDAP au contrôleur de domaine afin de s'assurer que les qualifications fournies sont correctes.

> Remarque: Avec tous les types d'authentification NTLM, des qualifications ne sont pas passées par l'intermédiaire du texte clair. Cependant, la version 1 (NTLMv1) NTLM a des vulnérabilités bien documentées. L'ISR est NTLMv2-capable, bien que par défaut, des versions plus anciennes de Microsoft Windows pourrait négocier par l'intermédiaire de NTLMv1. Ce comportement dépend des stratégies d'authentification d'AD.

NTLM transparent

L'authentification transparente NTLM se produit quand un utilisateur est enregistré dans le poste de travail avec des qualifications de domaine, et ces qualifications sont passées d'une manière transparente par le navigateur au routeur IOS. Le routeur IOS exécute alors une requête de LDAP afin de valider les identifiants utilisateurs. C'est généralement la forme d'authentification la plus désirée pour cette caractéristique.

Authentification de base (par l'intermédiaire du HTTP en texte clair)

Cette forme d'authentification est typiquement utilisée comme mécanisme de repli quand l'authentification NTLM échoue ou n'est pas possible aux clients tels que des périphériques de Macintosh, de Linux, ou des périphériques mobiles. Avec cette méthode, si le serveur sécurisé de HTTP n'est pas activé, puis ces qualifications sont passées par l'intermédiaire du HTTP en texte clair (très non sécurisé).

NTLM passif

Les qualifications passives de demandes d'authentification NTLM des utilisateurs mais n'authentifie pas réellement l'utilisateur contre le contrôleur de domaine. Tandis que ceci peut éviter des problèmes liés à la LDAP où les requêtes échouent contre le contrôleur de domaine, il expose également des utilisateurs dans l'environnement à un risque de sécurité. Si l'authentification transparente échoue ou n'est pas possible, alors les utilisateurs sont incités pour des qualifications. Cependant, l'utilisateur peut entrer dans toutes les qualifications qu'ils choisissent, qui sont passés au tower CWS. En conséquence, des stratégies ne pourraient pas être appliquées convenablement.

Par exemple, l'utilisateur A peut utiliser Firefox (qui par défaut ne permet pas NTLM transparent sans configuration supplémentaire) et écrire le nom d'utilisateur de l'utilisateur B avec n'importe quel mot de passe, et les stratégies pour l'utilisateur B sont appliquées à l'utilisateur R. L'exposition de risque peut être atténuée si des utilisateurs tous sont forcés pour utiliser les navigateurs qui prennent en charge l'authentification transparente NTLM, mais dans la plupart des cas, l'utilisation de l'authentification passive n'est pas recommandée.

Ordre de message pour l'authentification active NTLM

Voici l'ordre de message complet pour la méthode d'authentification active NTLM :

```
Browser -->  ISR : GET / google.com
Browser <--  ISR : 302 Page moved http://1.1.1.1/login.html
Browser -->  ISR : GET /login.html 1.1.1.1
Browser <--  ISR : 401 Unauthorized..Authenticate using NTLM
Browser -->  ISR : GET /login.html + NTLM Type-1 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-1 msg
```

L'ISR copie le message de type 1 du HTTP sur le LDAP, octet-par-octet sans n'importe quelle modification de données.

```
ISR     <--  AD  : LDAP Bind Response + NTLM Type-2 msg
Browser <--  ISR : 401 Unauthorized + NTLM Type-2 msg
```

Le message de type-2 est également copié octet-par-octet de LDAP sur le HTTP. Ainsi, dans le

PCAP, il semble provenir de **1.1.1.1**, mais le contenu réel est de l'AD.

```
Browser -->  ISR : GET /login.html + NTLM Type-3 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-3 msg
ISR     <--  AD  : LDAP Bind response - Success
Browser <--  ISR : 200OK + redirect to google.com
```

Quand NTLM actif est configuré, l'ISR ne gêne pas pendant l'échange NTLM. Cependant, si NTLM passif est configuré, puis l'ISR génère son propre message de type-2.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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

Commandes show

> Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show**.**

Vous pouvez employer ces **commandes show** afin de dépanner votre configuration :

- **cache de show ip admission**
- **état de show ip admission**
- **statistiques de show ip admission**
- **serveur tout de show ldap**

Commandes de débogage

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

Voici quelques commandes de débogage utiles que vous pouvez employer afin de dépanner votre configuration :

- **mettez au point le LDAP entièrement que** cette commande peut être utilisée afin de découvrir la raison pour laquelle l'authentification échoue.
- **mettez au point le détail d'ip admission** - Cette commande est très bavarde et CPU-intensive. Cisco recommande que vous l'utilisiez seulement avec les clients simples de test qui déclenchent l'ip admission.

- **mettez au point le ntlm d'ip admission** - Cette commande peut être utilisée afin de découvrir la raison pour laquelle le processus d'ip admission est déclenché.
- **mettez au point le httpd d'ip admission**
- **debug ip http transaction**
- **autorisation de debug aaa de debug aaa authentication**

Problèmes courants

Cette section décrit quelques problèmes courants qui sont produits avec la configuration décrite dans ce document.

L'ip admission n'intercepte pas des demandes de HTTP

Cette question devient évidente quand vous visualisez la sortie de commande de **statistiques de show ip admission**. La sortie n'affiche pas l'interception d'aucune demande de HTTP :

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

Solutions possibles

Il y a deux solutions possibles à cette question. Le premier est de vérifier que l'**ip http server** est activé.

Si le serveur HTTP pour l'ISR n'est pas activé, alors les déclencheurs d'ip admission mais intercepte jamais réellement la session de HTTP. Par conséquent, il incite pour l'authentification. Dans cette situation, il n'y a aucune sortie pour la commande de **cache de show ip admission**, mais beaucoup de récurrences de ces lignes sont vues dans la sortie de la commande de **détail d'ip admission de débogage** :

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

La deuxième solution à cette question est de vérifier que l'adresse IP d'utilisateur n'est pas exempte de l'ACL dans la configuration d'ip admission.

Les utilisateurs reçoivent une erreur *404 non trouvée*

Cette question est observée quand des utilisateurs sont réorientés pour l'authentification, et une erreur **404 non trouvée** se produit dans le navigateur.

Solution possible

Assurez-vous que le nom dans le **serveur virtuel ISR_PROXY virtuel-IP 1.1.1.1 d'ip admission** peut avec succès le résoudre avec le serveur de Système de noms de domaine (DNS) de client. Dans ce cas, le client exécute une requête DNS pour **ISR_PROXY.lab.cisco.com** puisque **lab.cisco.com** est le nom de domaine complet (FQDN) du domaine auquel le poste de travail est joint. Si la requête DNS échoue, le client envoie une requête de la résolution de noms de Multidiffusion de Lien-gens du pays (LLMNR), suivie d'une requête de NETBIOS qui est émission au sous-réseau local.

Si toutes ces tentatives de résolution échouent, alors des **404 non trouvés** ou l'**Internet Explorer ne peuvent pas afficher l'**erreur de **page Web** est affichés dans le navigateur.

L'authentification de l'utilisateur échoue une fois incitée

Ceci peut sont provoqué par par de diverses raisons mais sont habituellement liés à la configuration de LDAP sur l'ISR, ou à la transmission entre l'ISR et le serveur LDAP. Sur l'ISR, on observe généralement le symptôme quand des utilisateurs sont coincés dans l'**état Init** une fois que l'ip admission est déclenché :

```
C-881(config)#do show ip admi cac
Authentication Proxy Cache
Client Name N/A, Client IP 10.10.10.152, Port 56674, timeout 60,
 Time Remaining 2, state INIT
```

Causes classiques

Ce sont les causes classiques pour cette question :

- Un nom d'utilisateur et/ou un mot de passe non valides est entré par l'utilisateur pour l'authentification active.
- **Un base-dn** non valide est utilisé dans la configuration de LDAP, qui a comme conséquence les recherches qui ne renvoient aucun résultat.
- **Un racine-dn** non valide d'authentification de grippage est configuré pour le nom d'utilisateur ou mot de passe, qui fait échouer le grippage de LDAP.
- La transmission entre l'ISR et le serveur LDAP échoue. Vérifiez que le serveur LDAP écoute sur le port TCP spécifié la transmission de LDAP et que tous les Pare-feu entre les deux permettent le trafic.
- Un filtre non valide de recherche n'entraîne aucun résultat pour la recherche de LDAP.

Dépannez le LDAP

La meilleure manière de déterminer la raison pour laquelle l'authentification échoue est d'utiliser les commandes de débogage de LDAP sur l'ISR. Maintenez dans l'esprit qui met au point peut être cher et dangereux de s'exécuter sur un ISR s'il y a sortie excessive, et ils peuvent faire arrêter

et avoir besoin le routeur d'un arrêt et redémarrage dur. Cela vaut particulièrement pour les Plateformes plus bas de gamme.

Afin de dépanner, Cisco recommande que vous vous appliquiez un ACL à la règle d'ip admission afin de soumettre seulement un poste de travail simple de test sur le réseau à l'authentification. De cette façon, met au point peut être activée avec un risque minimal d'incidence négative à la capacité du routeur de passer le trafic.

> **Conseil** : Référez-vous aux **hôtes internes exempts de la** section d'**authentification de** ce document pour plus d'informations sur l'application d'un ACL à la configuration d'admissions IP.

Quand vous dépannez des problèmes liés à la LDAP, il est utile de comprendre les étapes dans lesquelles le LDAP traite des demandes de l'ISR.

Étapes de haut niveau pour l'authentification LDAP

Voici les étapes de haut niveau pour l'authentification LDAP :

1. Ouvrez la connexion au serveur LDAP sur le port spécifié. Le port par défaut est le **TCP 389**.
2. Le grippage au serveur LDAP avec le grippage authentifient l'utilisateur et le mot de passe de racine-**dn**.
3. Exécutez la recherche de LDAP, avec l'utilisation du base-**dn** et des recherche-filtres qui sont définis dans la configuration de LDAP, pour l'utilisateur qui tente d'authentifier.
4. Obtenez les résultats de LDAP du serveur LDAP et créez une entrée de cache d'ip admission pour l'utilisateur si l'authentification est réussie, ou le reprompt pour des qualifications en cas d'un échec d'authentification.

Analyse de sortie de débogage de LDAP

Ces processus peuvent être visualisés dans la sortie du **LDAP de débogage toute la** commande. Cette section fournit un exemple de la sortie de débogage de LDAP pour une authentification qui échoue en raison d'un base-**dn** non valide. Passez en revue la sortie de débogage et les commentaires associés, qui décrivent les parties de la sortie qui affichent où les étapes mentionnées ci-dessus pourraient rencontrer la panne.

```
*Jan 30 20:51:50.818: LDAP: LDAP: Queuing AAA request 23 for processing
*Jan 30 20:51:50.818: LDAP: Received queue event, new AAA request
*Jan 30 20:51:50.818: LDAP: LDAP authentication request
*Jan 30 20:51:50.818: LDAP: Username sanity check failed
*Jan 30 20:51:50.818: LDAP: Invalid hash index 512, nothing to remove
*Jan 30 20:51:50.818: LDAP: New LDAP request
*Jan 30 20:51:50.818: LDAP: Attempting first next available LDAP server
*Jan 30 20:51:50.818: LDAP: Got next LDAP server :DC01
*Jan 30 20:51:50.818: LDAP: Free connection not available. Open a new one.
*Jan 30 20:51:50.818: LDAP: Opening ldap connection
( 10.10.10.150, 389 )ldap_open
```

La partie du résultat présenté en gras indique que ce n'est pas une question de couche réseau, puisque la la connexion est avec succès ouverte.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

L'authentifier-dn de grippage est correct dans cette sortie. Si la configuration est incorrecte pour ceci, alors des pannes de grippage sont vues.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

La partie du résultat présenté en gras indique que toutes les exécutions de grippage sont réussies et il poursuit pour rechercher l'utilisateur réel.

```
*Jan 30 20:51:51.854: LDAP: SASL NTLM authentication done..Execute search
*Jan 30 20:51:51.854: LDAP: Next Task: Send search req
*Jan 30 20:51:51.854: LDAP: Transaction context removed from list[ldap reqid=15]
*Jan 30 20:51:51.854: LDAP: Dynamic map configured
*Jan 30 20:51:51.854: LDAP: Dynamic map found for aaa type=username
*Jan 30 20:51:51.854: LDAP: Ldap Search Req sent
ld 2293572544
base dn     dc=lab1,dc=cisco,dc=comscope       2
filter (&(objectclass=top)(sAMAccountName=testuser5))
ldap_req_encode
put_filter "(&(objectclass=top)(sAMAccountName=testuser5))"
put_filter: AND
put_filter_list "(objectclass=top)(sAMAccountName=testuser5)"
put_filter "(objectclass=top)"
put_filter: simple
put_filter "(sAMAccountName=testuser5)"
put_filter: simple
Doing socket write
*Jan 30 20:51:51.854: LDAP: lctx conn index = 2
```

La première ligne (affichée en gras) indique que la sortie de débogage de recherche de LDAP commence. En outre, notez que le contrôleur de domaine de base-dn devrait être configuré pour le laboratoire, pas lab1.

```
*Jan 30 20:51:52.374: LDAP: LDAP Messages to be processed: 1
*Jan 30 20:51:52.374: LDAP: LDAP Message type: 101
*Jan 30 20:51:52.374: LDAP: Got ldap transaction context from reqid
16ldap_parse_result
*Jan 30 20:51:52.374: LDAP: resultCode: 10 (Referral)
*Jan 30 20:51:52.374: LDAP: Received Search Response resultldap_parse_result
ldap_err2string
*Jan 30 20:51:52.374: LDAP: Ldap Result Msg: FAILED:Referral, Result code =10
*Jan 30 20:51:52.374: LDAP: LDAP Search operation result : failedldap_msgfree
*Jan 30 20:51:52.374: LDAP: Closing transaction and reporting error to AAA
*Jan 30 20:51:52.374: LDAP: Transaction context removed from list
[ldap reqid=16]
*Jan 30 20:51:52.374: LDAP: Notifying AAA: REQUEST FAILED
```

La partie du résultat présenté en gras indique que la recherche n'a renvoyé aucun résultat, qui est dans ce cas due à un base-dn non valide.

RFC 4511

RFC 4511 (**Protocole LDAP (Lightweight Directory Access Protocol) : Protocol**) fournit les informations sur les messages de code de résultat pour le LDAP et d'autres informations liées à la Protocol de LDAP, qui peuvent être mises en référence par l'intermédiaire du site Web IETF.