ScanSafe/クラウドWebセキュリティ設定例にWebリダイレクトのISR IP管理およびLDAP

内容

概要
前提条件
要件
使用するコンポーネント
背景説明
設定
ネットワーク図
LDAP の設定
AAA の設定
IP アドミッションの設定
IP アドミッションの有効化
内部ホストの認証免除
ISR での HTTP サーバの有効化
CWS リダイレクションの設定
完全な設定例
[LDAP]
[AAA]
IP アドミッション
HTTP Server
コンテンツ スキャンおよび CWS
AD 内の DN オブジェクトの判別（ADSI Edit）
認証方式
アクティブ NTLM
トランスペアレント NTLM
基本認証（クリア テキストで HTTP を使用）
パッシブ NTLM
アクティブ NTLM 認証のメッセージ シーケンス
確認
トラブルシュート
show コマンド
デバッグ コマンド
一般的な問題
IP アドミッションが HTTP 要求を代行受信しない
考えられる解決策
ユーザが 404 Not Found エラーを受け取る
考えられる解決策

[プロンプトが出された時点でユーザ認証が失敗する](#)
[よくある原因](#)
[LDAP のトラブルシューティング](#)
[LDAP 認証の基本手順](#)
[LDAP デバッグ出力の分析](#)
[RFC 4511](#)

概要

このドキュメントでは、Cisco G2 シリーズ サービス統合型ルータ（ISR）の設定方法について説明します。 ISR の認証プロキシには IP アドミッションと Lightweight Directory Access Protocol（LDAP）の設定だけを使用することもできますが、通常は、Cisco クラウド Web セキュリティ（CWS）のリダイレクト機能と併せて使用します。したがって、このドキュメントは、ISR での CWS リダイレクションの設定およびトラブルシューティングのドキュメントを補足することを目的としています。

前提条件

要件

このドキュメントで説明している設定を開始する前に、次の推奨要件を満たしていることを確認してください。

- ISR はバージョン 15.2(1) T1 以降のコードを実行している必要があります。
- ご使用のシステムには、セキュリティ機能セット（SEC）ライセンスが適用されたイメージが必要です。これらのイメージは、Cisco IOS®（ユニバーサル）から入手できます。
- Active Directory（AD）ドメインのクライアント ワークステーションには、Web ブラウザでアクティブ認証を実行する機能が必要です。
- CWS サブスクリプションを持っている必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Internet Explorer、Google Chrome、Mozilla Firefox（トランスペアレント NT LAN Manager（NTLM）認証用の追加設定が必要です）
- Cisco G2 800、1900、2900、3900 シリーズ ISR
- Microsoft Windows AD ドメイン コントローラ（ADDC）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています

。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

> **注：**Cisco G1 1800、2800、3800 シリーズ ルータはサポートされていません。

背景説明

ネットワークに Cisco Adaptive Security Appliance（ASA）がない状態で Cisco G2 シリーズ ISR をインストールする管理者の多くは、Web フィルタリングに CWS ソリューションを利用するために、ISR CWS（旧称 ScanSafe）リダイレクション機能を使用することを選択します。また、ほとんどの管理者は、CWS ポータルの Web フィルタリング ポリシーにユーザベースまたはグループベースのポリシーを適用する目的でユーザ ID 情報を CWS タワーに送信するために、現在の AD インフラストラクチャをこのソリューションの一部として利用することも選択します。

全体的な概念は、ASA と Context Directory Agent（CDA）の統合と同様ですが、いくつかの違いがあります。最も顕著な違いは、ISR ではユーザと IP をマッピングするパッシブ データベースを実際に保守するわけではないという点です。したがって、ISR 経由でユーザまたはグループ情報を CWS ポータルに送信するためには、ユーザが何らかのタイプの認証に合格する必要があります。

> **ヒント**：使用できる各種の認証方式の違いについて詳しくは、このドキュメントの「**認証方式」のセクションを参照してください。**

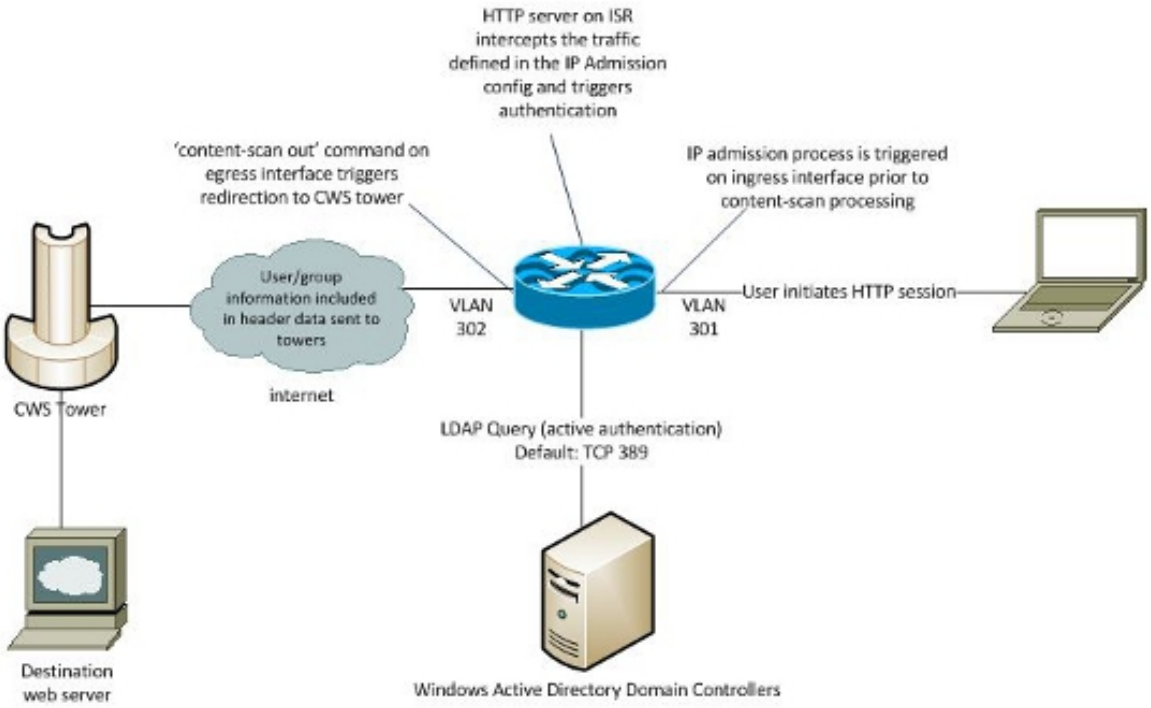
このドキュメントで説明する設定の CWS リダイレクションの部分は比較的単純なものですが、管理者によっては認証の部分を設定する際に問題に突き当たることも考えられます。認証の部分で処理する **ip admission コマンドは LDAP サーバおよび認証、許可、およびアカウンティング（AAA）認証ステートメントを参照しますが、このステートメントも設定する必要があります。**このドキュメントの目的は、ネットワーク オペレータが Cisco G2 シリーズ ISR でこの設定の IP アドミッションおよび LDAP の部分を設定したり、トラブルシューティングしたりできるよう、包括的な参照情報を提供することにあります。

設定

このセクションで説明する情報を使用して、Cisco ISR を設定します。

> **注：**このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



LDAP の設定

AAA サーバの LDAP プロパティを設定するには、次の手順を実行します。

1. ユーザが入力したユーザ名を AD 内の **sAMAccountName プロパティと照合するために、LDAP 属性マップを設定します。**

```
C-881(config)#ldap attribute-map ldap-username-map map type sAMAccountName
 username
C-881(config-attr-map)#map type sAMAccountName username
```

注：この設定が必要なのは、**sAMAccountName属性はAD内で一意の値であるた**め、デフォルトで一致するために使用される共通名(CN)属性とは異なります。たとえば、AD内に*John Smithの複数インスタンスが*、**AMAには1人の**ユーザのみAMAが*JSMITH*のCCOUNTName。これはユーザアカウントのログオンでもあります。他の *John Smith アカウントの* **sAMAccountNames には、***jsmith1 または jsmith2* などの値が設定されます。
show ldap attributes コマンドを使用して、LDAP 属性および関連する AAA 属性のリストを表示することもできます。

2. LDAP サーバ グループを設定します。

```
C-881(config)#aaa group server ldap LDAP_GROUP
C-881(config-ldap-sg)#server DC01
```

3. LDAP サーバを設定します。

```
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
```

カスタム検索フィルタを実装する必要がない限り、通常はこの設定を変更する必要はありません。カスタム検索フィルタは、LDAP およびこの情報を適切に入力する方法に精通している管理者だけが利用できます。使用すべき検索フィルタがわからない場合は、ここに記載されているフィルタをそのまま使用してください。このフィルタは、通常の AD 環境でユーザを検索します。

bind-authenticate-root-dn および base-dn コマンドに必要な識別名（DN）も、LDAP 設定で細心の注意が必要な部分です。LDAP サーバで表示されるとおりに DN を入力しなければ、LDAP クエリは失敗します。さらに、**base-dn コマンドは、認証対象の全ユーザが所属する LDAP ツリーの最下位の部分とならなければなりません。**

上記の設定に含まれる **base-dn コマンドを以下のように変更したとします。**

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

この場合、**CN=Users,DC=lab,DC=cisco,DC=com に含まれるユーザに対するクエリは、結果を一切返しません。LDAP サーバは、TestCompany 組織単位（OU）とそこに含まれる子オブジェクトだけを検索するためです。**したがって、ユーザの認証を成功させるには、これらのユーザを TestCompany OU またはそのサブツリーに移動するか、あるいは該当する検索場所がクエリに含まれるように **base-dn コマンドを変更しなければなりません。**

> **ヒント**：base および root コマンドに適切な DN を判別する方法について詳しくは、このドキュメントの「**とAD 内の DN オブジェクトの判別（ADSI Edit）」セクションを参照してください。**

AAA の設定

LDAP サーバを設定したら、IP アドミッション プロセスで使用される、対応する AAA ステートメントでこれらのサーバを参照する必要があります。

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

> **注：**上記のコマンドが使用可能でない場合は、**aaa new-model コマンドを入力して、この AAA 機能を有効にする必要があります（デフォルトでは有効にされていません）。**

IP アドミッションの設定

IP アドミッションの部分は、ユーザに認証を求めるプロンプトを出し（またはトランスペアレント認証を実行）、次にユーザ クレデンシャルと設定に定義されている AAA サーバに基づく LDAP クエリを実行するプロセスをトリガーします。ユーザが正常に認証されると、コンテンツスキャン プロセスによってユーザ ID 情報がプルされて、リダイレクトされたフローと併せて CWS タワーに送信されます。IP アドミッション プロセスは、ルータの入力インターフェイスで ip admission ***name コマンドが入力されるまではアクティブになりません。***したがって、設定のこの部分は、トラフィックに影響を与えることなく実装できます。

```
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 アドミッションの有効化

以下に、IP アドミッションを有効にするために使用する設定を示します。

> **注：**この設定により、ユーザの認証が強制され、認証に失敗した場合はトラフィック フローが中断されます。

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

内部ホストの認証免除

管理者によっては、さまざまな理由から、一部の内部ホストを認証プロセスから免除したいと考える場合があります。たとえば、NTLM や基本認証に対応できない内部サーバまたはデバイスに IP アドミッション プロセスが適用されるのは望ましくない場合があります。このような場合には、特定のホスト IP またはサブネットで IP アドミッションがトリガーされないように、アクセス コントロール リスト（ACL）を IP アドミッション設定に適用することができます。

以下の例では、内部ホスト **10.10.10.150 が認証を免除されますが、その他すべてのホストには引き続き認証が必要です。**

```
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
```

ISR での HTTP サーバの有効化

HTTP セッションを代行受信して認証プロセスを開始するには、以下のコマンドを使用して HTTP サーバを有効にする必要があります。

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

> **注：Ip http secure-server が必要となるのは、認証で HTTPS へのリダイレクションが必要な場合のみです。**

CWS リダイレクションの設定

以下に、CWS リダイレクションの基本的なサマリ設定を示します。

```
parameter-map type content-scan global
 server scansafe primary name proxy139.scansafe.net port http 8080 https 8080
```

```
 server scansafe secondary name proxy187.scansafe.net port http 8080 https 8080
 license 0 DE749585HASDH83HGA94EA8C369
 source interface Vlan302
user-group DEFAULT_GROUP username DEFAULT_USER
 server scansafe on-failure allow-all

interface Vlan302 (egress interface towards Internet)
 content-scan out
```

完全な設定例

以下に、これまでのセクションで行った完全な設定例を記載します。

[LDAP]

```
aaa group server ldap LDAP_GROUP
 server DC01
ldap attribute-map ldap-username-map
 map type sAMAccountName username
ldap server DC01
 ipv4 10.10.10.150
 attribute map ldap-username-map
 bind authenticate root-dn CN=Csco_Service,CN=Users,DC=lab,DC=cisco,DC=com
  password Cisco12345!
 base-dn dc=lab,dc=cisco,dc=com
 search-filter user-object-type top
 authentication bind-first
```

[AAA]

```
aaa new-model
aaa authentication login SCANSAFE_AUTH group LDAP_GROUP
aaa authorization network SCANSAFE_AUTH group LDAP_GROUP
```

IP アドミッション

```
ip admission virtual-ip 1.1.1.1 virtual-host ISR_PROXY
ip admission name SCANSAFE_ADMISSION ntlm
ip admission name SCANSAFE_ADMISSION method-list authentication
 SCANSAFE_AUTH authorization SCANSAFE_AUTH

interface Vlan301
 ip admission SCANSAFE_ADMISSION
```

HTTP Server

```
ip http server
```

コンテンツ スキャンおよび CWS

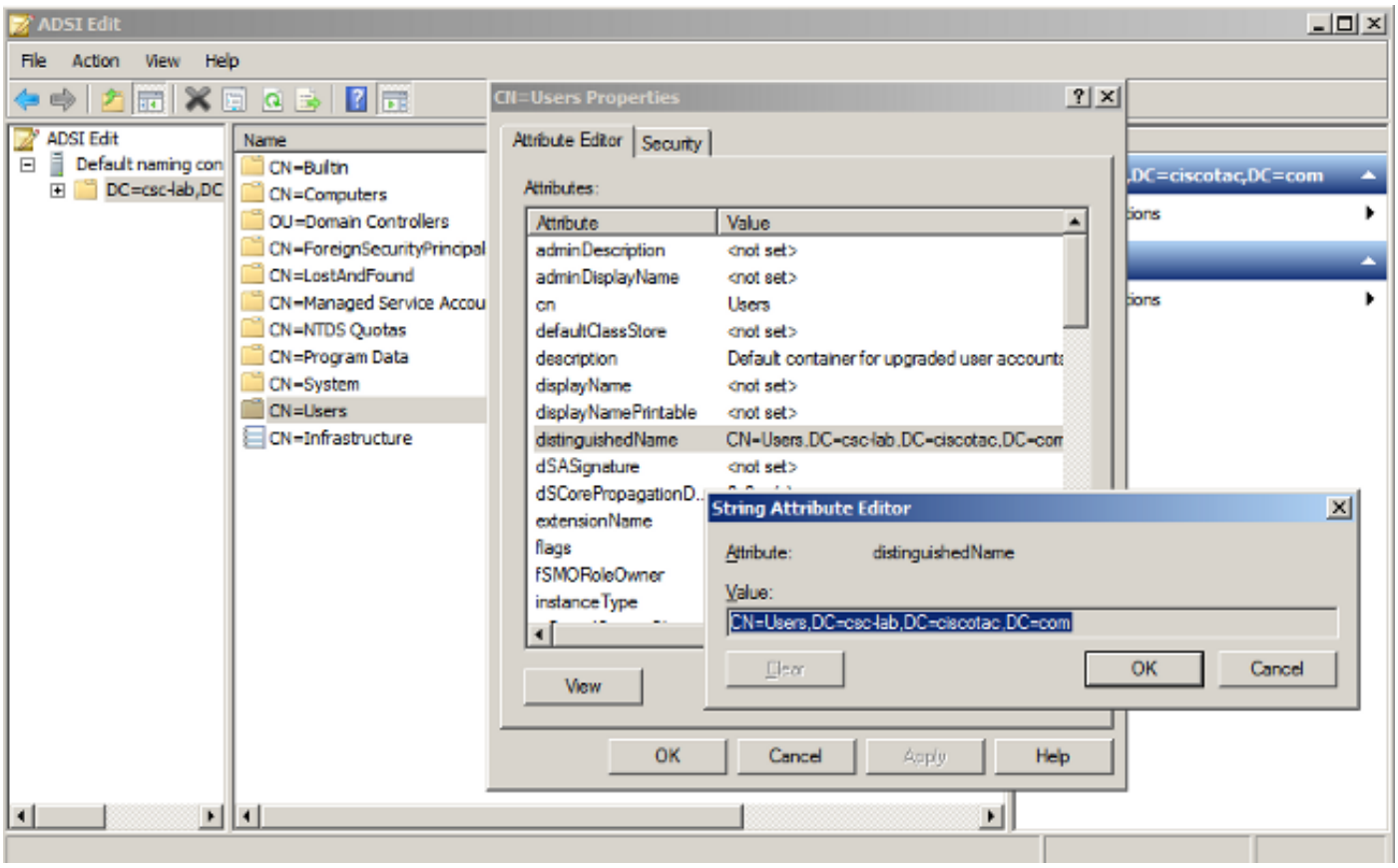
```
parameter-map type content-scan global
 server scansafe primary name proxy139.scansafe.net port http 8080 https 8080
 server scansafe secondary name proxy187.scansafe.net port http 8080 https 8080
 license 0 DE13621993BD87B306B5A5607EA8C369
 source interface Vlan302
 user-group DEFAULT_GROUP username DEFAULT_USER
 server scansafe on-failure allow-all

interface Vlan302
 content-scan out
```

AD 内の DN オブジェクトの判別 (ADSI Edit)

必要に応じて、AD構造を参照して、ユーザーまたはグループ検索ベースで使用するDNを検索できます。管理者は、ADドメインコントローラーに組み込まれた*ADSI Editというツールを使用*できます。ADSI Edit を開くには、AD ドメイン コントローラで [Start] > [Run] を選択し、**adsiedit.msc と入力します。**

ADSI Edit が開いたら、オブジェクト (OU、グループ、ユーザなど) を右クリックし、[Properties] を選択してそのオブジェクトの DN を表示します。DN 文字列は簡単にコピーしてルータ設定に貼り付けることができるので、入力ミスを回避できます。以下のイメージに、このプロセスを示します。



認証方式

IP アドミッションを使用する、選択可能な認証方式のタイプは 4 つあります。これらの認証方式

は、特にトランスペアレント NTML とパッシブ NTLM との違いをはじめ、誤解されがちです。以降のセクションで、認証方式のタイプによる違いについて説明します。

アクティブ NTLM

アクティブ NTLM 認証方式は、トランスペアレント NTLM 認証が失敗した場合に、ユーザに認証を求めるプロンプトを出します。一般に、認証失敗の原因となることは、クライアント ブラウザが統合 Microsoft Windows 認証をサポートしていないこと、あるいはユーザがローカル (非ドメイン) クレデンシャルを使用してワークステーションにログインしたことです。アクティブ NTLM 認証では、提供されたクレデンシャルが正しいことを確認するために、ドメイン コントローラに対して LDAP クエリを行います。

> **注：**いずれのタイプの NTLM 認証でも、クレデンシャルがクリア テキストで渡されることはありません。ただし、NTLM バージョン 1 (NTLMv1) には明確に文書化された脆弱性があります。ISRはNTLMv2対応ですが、デフォルトでは、古いバージョンのMicrosoft WindowsがNTLMv1を介してネゴシエートする場合があります。この動作は、AD認証ポリシーに依存します。

トランスペアレント NTLM

トランスペアレント NTLM 認証は、ユーザがドメイン クレデンシャルでワークステーションにログインすると行われます。これらのクレデンシャルは、ブラウザによってトランスペアレントに IOS ルータに渡されます。すると、IOS ルータはユーザ クレデンシャルを検証するために LDAP クエリを実行します。通常、この機能にはトランスペアレント NTLM が最も望ましい形の認証です。

基本認証 (クリア テキストで HTTP を使用)

この形の認証は一般に、NTLM 認証が失敗した場合、またはクライアント (Macintosh、Linux ベースのデバイス、またはモバイル デバイスなど) で NTLM 認証を行えない場合のフォールバック メカニズムとして使用されます。この認証方式では、HTTP セキュア サーバが有効にされてない場合、HTTP でクリア テキストのクレデンシャルが渡されます (かなり危険です)。

パッシブ NTLM

パッシブ NTLM 認証では、ユーザにクレデンシャルを要求しますが、ドメイン コントローラに対して実際にユーザを認証するわけではありません。これにより、クエリがドメインコントローラに対して失敗するLDAP関連の問題を回避できますが、環境内のユーザーにセキュリティ上のリスクが生じます。透過的な認証が失敗したり実行できない場合は、資格情報の入力を求められます。ただし、ユーザは任意のクレデンシャルを入力することができ、そのクレデンシャルが CWS タワーに渡されます。そのため、ポリシーが適切に適用されない可能性があります。

たとえば、Firefox (追加の設定を行わない限り、デフォルトではトランスペアレント NTLM を許可しません) を使用しているユーザ A がユーザ B のユーザ名と任意のパスワードを入力すると、ユーザ B に対するポリシーがユーザ A に適用されます。このリスクを軽減するには、すべてのユーザにトランスペアレント NTLM 認証をサポートするブラウザを使用させるという方法がありますが、ほとんどの場合、パッシブ認証の使用は推奨されません。

アクティブ NTLM 認証のメッセージ シーケンス

アクティブ NTLM 認証方式の完全なメッセージ シーケンスは、以下のとおりです。

```
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
```

ISR が HTTP からの Type-1 メッセージを、データを変更することなくバイトごとに LDAP にコピーします。

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

Type-2 メッセージもバイトごとに LDAP から HTTP にコピーされます。したがって、PCAP では 1.1.1.1 から発信されたように見えますが、実際のコンテンツは AD からのものです。

```
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
```

アクティブ NTLM が設定されている場合、NTML 交換中に ISR が干渉することはありません。ただし、パッシブ NTLM が設定されていると、ISR は独自の Type-2 メッセージを生成します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

show コマンド

> **注：**アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

次の show コマンドを使用して、設定のトラブルシューティングを行うことができます。

- show ip admission cache
- show ip admission status
- show ip admission statistics

- show ldap server all

デバッグ コマンド

> **注**：debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。

設定をトラブルシュートする際には、以下の debug コマンドを使用すると役立ちます。

- **debug ldap all：このコマンドは、認証が失敗した理由を調べるために使用します。**
- **debug ip admission detail：このコマンドは、非常に詳細な出力を生成するため、CPU に負担をかけます。**IP アドミッションをトリガーする単一のテスト クライアントにのみ使用することを推奨します。
- **debug ip admission ntlm：このコマンドは、IP アドミッション プロセスがトリガーされた理由を調べるために使用します。**
- debug ip admission httpd
- debug ip http transaction
- debug aaa authentication debug aaa authorization

一般的な問題

ここでは、このドキュメントで説明している設定で発生することがある、一般的な問題について説明します。

IP アドミッションが HTTP 要求を代行受信しない

この問題は、**show ip admission statistics コマンドの出力を調べると明らかになります。**出力には、HTTP の代行受信が示されないためです。

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

HTTPd process 1
Intercepted HTTP requests: 0
```

考えられる解決策

この問題に対しては、2 つの解決策が考えられます。解決策の 1 つとしては、**ip http server が有効にされていることを確認します。**

ISR の HTTP サーバが有効にされていなければ、IP アドミッションはトリガーされても、実際に HTTP セッションを代行受信することはありません。したがって、認証を求めるプロンプトが出

されます。この場合、show ip admission cache コマンドに対する出力はありませんが、debug ip admission detail コマンドの出力に以下の行が何度も繰り返し出現することになります。

```
*Jan 30 20:49:35.726: ip_admission_det:proceed with process path authentication
*Jan 30 20:49:35.726: AUTH-PROXY auth_proxy_find_conn_info :
find srcaddr - 10.10.10.152, dstaddr - 192.168.1.1
ip-srcaddr 10.20.10.1
pak-srcaddr 10.10.10.152
```

この問題に対するもう 1 つの解決策としては、IP アドミッション設定の ACL でこのユーザ IP アドレスが免除対象になっていないことを確認します。

ユーザが 404 Not Found エラーを受け取る

これは、ユーザが認証のためにリダイレクトされる際に見られる問題で、ブラウザに 404 Not Found エラーが表示されます。

考えられる解決策

ip admission virtual-ip 1.1.1.1 virtual-host ISR_PROXY の名前が、ドメイン ネーム システム（DNS）サーバで正常に解決されることを確認します。この場合、クライアントは ISR_PROXY.lab.cisco.com に対して DNS クエリを実行します。これは、lab.cisco.com はワークステーションが参加しているドメインの完全修飾ドメイン名（FQDN）であるためです。DNS クエリが失敗すると、クライアントは Link-Local Multicast Name Resolution（LLMNR）クエリを送信し、続いて NETBIOS クエリがローカル サブネットにブロードキャストされます。

以上の解決策のすべてを試しても名前が解決されない場合は、「404 Not Found」または「Internet Explorer Cannot Display the webpage」エラーがブラウザに表示されます。

プロンプトが出された時点でユーザ認証が失敗する

この問題にはさまざまな原因がありますが、通常は、ISR 上の LDAP 設定、あるいは ISR と LDAP サーバ間の通信に関連しています。ISR でこの症状が観測されるのは、一般に IP アドミッションがトリガーされた後に INIT状態のままになった場合です。

```
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
```

よくある原因

この問題の一般的な原因は以下のとおりです。

- アクティブ認証に対して、ユーザが無効なユーザ名やパスワードを入力した。
- 無効な base-dn が LDAP 設定で使用されているために、検索結果が返されない。

- ユーザ名またはパスワードに無効なバインド認証 **root-dn が設定されているために、LDAP バインドが失敗する。**

- ISR と LDAP サーバ間の通信が失敗する。LDAP サーバが LDAP 通信に指定されたポートでリッスンしていること、また ISR と LDAP サーバ間にあるすべてのファイアウォールがトラフィックを許可することを確認してください。

- 無効な検索フィルタにより、LDAP 検索結果が返されない。

LDAP のトラブルシューティング

認証が失敗した理由を判断する最良の方法は、ISR で LDAP デバッグ コマンドを使用することです。過剰な出力が生成されるなら、ISR でデバッグを実行するのはコストが高く危険なことになり、ルータが停止してハードウェアの電源再投入が必要になる可能性があることに注意してください。これは特に、よりローエンドのプラットフォームに当てはまります。

トラブルシューティングの際は、ACL を IP アドミッション ルールに適用し、ネットワークで認証を行う単一のワークステーションだけを対象とすることを推奨します。このようにすると、ルータがトラフィックを渡す機能への悪影響を最小限に抑えてデバッグを有効にすることができます。

> **ヒント**：IP アドミッション設定に ACL を適用する方法について詳しくは、このドキュメントの「**内部ホストの認証免除」セクションを参照してください。**

LDAP 関連の問題をトラブルシューティングする場合、LDAP が ISR からの要求を処理する手順を理解しておくと役立ちます。

LDAP 認証の基本手順

LDAP 認証の基本手順は以下のとおりです。

1. 指定されたポートで LDAP サーバへの接続を開きます。デフォルトのポートは **TCP ポート 389** です。

2. **bind authenticate root-dn によって、LDAP サーバにユーザとパスワードをバインドします。**

3. base-dn と LDAP 設定に定義された検索フィルタ使用した LDAP 検索によって、認証を試行しているユーザを検索します。

4. 認証が成功した場合は、LDAP サーバから LDAP 結果を取得し、ユーザの IP アドミッション キャッシュ エントリを作成します。認証が失敗した場合は、再度クレデンシャルを求めるプロンプトを出します。

LDAP デバッグ出力の分析

上記のプロセスは、**debug ldap** コマンドの出力で確認できます。ここでは、無効な **base-dn** が原因で失敗した認証に対する LDAP デバッグのサンプル出力を記載します。 デバッグ出力および

関連するコマンドを検討し、出力で、上述の手順で問題が発生した部分を調べます。

```
*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
```

上記の出力で太字で示されている部分から、接続は正常に開いたことがわかるので、これはネットワーク層の問題ではありません。

```
*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
```

上記では、**authenticate-dn のバインドは正常に行われています。**バインドの設定が誤っているとしたら、バインドの失敗が示されるはずです。

```
*Jan 30 20:51:51.846: LDAP: Received Bind Responseldap_parse_sasl_bind_result
*Jan 30 20:51:51.846: LDAP: Ldap SASL Result Msg: SUCCESS, Result code =14
sasLres_code =14
*Jan 30 20:51:51.846: LDAP: SASL NTLM authentication do not require
further tasks
*Jan 30 20:51:51.846: LDAP: Next Task: All authentication task completed
*Jan 30 20:51:51.846: LDAP: Transaction context removed from list
[ldap reqid=14]
*Jan 30 20:51:51.846: LDAP: * * AUTHENTICATION COMPLETED SUCCESSFULLY * *
*Jan 30 20:51:51.846: LDAP: Notifying AAA: REQUEST CHALLENGED
```

太字で示されている部分に、バンド操作のすべてが成功し、操作が実際のユーザの検索に移ったことが示されています。

```
*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
```

最初の行（太字で表示）が、LDAP 検索のデバッグ出力が開始したことを示しています。また、base-dn ドメイン コントローラは lab1 ではなく lab に設定しなければなりません。

```
*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
```

以下の出力で、太字で示されている部分から、検索が結果を返さなかったことがわかります。その原因は、base-dn が無効であるためです。

RFC 4511

RFC 4511（Lightweight Directory Access Protocol（LDAP））：このプロトコルは、LDAP の結果コード メッセージに関する情報や、その他の LDAP プロトコル関連の情報を提供します。LDAP については、IETF Web サイトを参照してくだ さい。