

# ダイナミックな属性マップを使用した IOS デバイス上の LDAP の設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[主な問題](#)

[解決方法](#)

[設定](#)

[サンプル コンフィギュレーション](#)

[AD ツール](#)

[潜在的な問題](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco IOS® ヘッドエンドで Lightweight Directory Access Protocol ( LDAP ) の認証を使用して、デフォルトの [相対識別名 \( RDN \) を Common Name \( CN \) から sAMAccountName に変更する方法について説明します。](#)

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco IOS ソフトウェア リリース 15.0 以降を実行する Cisco IOS デバイスに基づいています。

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。

## 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## 主な問題

LDAP ユーザがいるほとんどの Microsoft Active Directory (AD) では一般的に RDN を sAMAccountName として定義します。VPN クライアントのヘッドエンドとして認証プロキシ (auth-proxy) および適応型セキュリティ アプライアンス (ASA) サーバを使用する場合は、AAA サーバを定義するときに AD サーバタイプを定義するか、[ldap-naming-attribute](#) コマンドを入力するのであれば、簡単に修正されます。ただし、Cisco IOS ソフトウェアでは、このいずれのオプションも使用できません。デフォルトで、Cisco IOS ソフトウェアでは、ユーザ名の認証に AD の CN 属性値を使用します。たとえば、AD でユーザ *John Fernandes* が作成されますが、ユーザ ID は *jfern* として保存されます。デフォルトでは、Cisco IOS ソフトウェアは、CN 値をチェックします。つまり、Cisco IOS ソフトウェアでは、ユーザ名の認証で *John Fernandes* をチェックし、sAMAccountName 値に *jfern* を認証でチェックしません。Cisco IOS ソフトウェアで sAMAccountName の属性値からのユーザ名をチェックするように強制するには、このドキュメントで詳述されているダイナミック属性マップを使用します。

## 解決方法

Cisco IOS デバイスでは RDN 変更の次の方法をサポートしていませんが、ダイナミックな属性マップを使用して Cisco IOS ソフトウェアで同様な結果を実現できます。Cisco IOS ヘッドエンドで `show ldap attribute` コマンドを入力すると、次の出力が表示されます。

LDAP 属性	書式	AAA 属性
airespaceBwDataBurstContract	Ulong	bsn- data-bandwidth-burst-contr
userPassword	String	password
airespaceBwRealBurstContract	Ulong	bsn-realtime-bandwidth-burst-c
employeeType	String	employee-type
airespaceServiceType	Ulong	service-type
airespaceACLName	String	bsn-acl-name
priv-lvl	Ulong	priv-lvl
memberOf	String DN	supplicant-group
cn	String	username
airespaceDSCP	Ulong	bsn-dscp

policyTag	String	tag-name
airespaceQOSLevel	Ulong	bsn-qos-level
airespace8021PType	Ulong	bsn-8021p-type
airespaceBwRealAveContract	Ulong	bsn-realtime-bandwidth-average
airespaceVlanInterfaceName	String	bsn-vlan-interface-name
airespaceVapId	Ulong	bsn-wlan-id
airespaceBwDataAveContract	Ulong	bsn-data-bandwidth-average-con
sAMAccountName	String	sam-account-name
meetingContactInfo	String	contact-info
telephoneNumber	String	telephone-number

強調表示された属性からわかるように、Cisco IOS ネットワーク アクセス デバイス (NAD) では、認証の要求と応答に、この属性マップを使用します。基本的に、Cisco IOS デバイスのダイナミック LDAP 属性マップは双方向で機能します。つまり、属性は、応答を受信するときだけでなく、LDAP 要求が送信されるときにもマップされます。ユーザ定義の属性マップである NAD 上の基本 LDAP 設定がない場合は、要求が送信されるときに次のログメッセージが表示されます。

```
*Jul 24 11:04:50.568: LDAP: Check the default map for aaa type=username
*Jul 24 11:04:50.568: LDAP: Ldap Search Req sent
ld 1054176200
base dn DC=cisco,DC=com
scope 2
filter (&(objectclass=*)(cn=xyz))ldap_req_encode
put_filter "(&(objectclass=person)(cn=xyz))"
put_filter: AND
put_filter_list "(objectclass=person)(cn=xyz)"
put_filter "(objectclass=person)"
put_filter: simple
put_filter "(cn=xyz)"
put_filter: simple
Doing socket write
*Jul 24 11:04:50.568: LDAP: LDAP search request sent successfully (reqid:13)
```

この動作を変更し、ユーザ名の確認に sAMAccountName の属性を使用するように強制する場合は、`ldap attribute map username` コマンドを入力して、このダイナミック属性マップをまず作成します。

```
ldap attribute map username
  map type sAMAccountName username
```

この属性マップを定義したら、[attribute map <dynamic-attribute-map-name>](#) コマンドを入力して

[、選択した AAA サーバグループ \( aaa-server \) にこの属性をマップします。](#)

注：このプロセス全体を簡単にするために、Cisco Bug ID [CSCtr45874 \( 登録ユーザ専用 \)](#) が提出されています。この機能要求が実装されていると、使用されている LDAP サーバをユーザが識別でき、その特定のサーバによって使用された値を反映するようにこれらのデフォルト マップの一部を自動的に変更できます。

## 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool ( 登録ユーザ専用 ) を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

## サンプル コンフィギュレーション

このドキュメントでは、次の構成を使用します。

- ダイナミック属性マップを定義するには、次のコマンドを入力します。

```
ldap attribute map  
  
map type sAMAccountName username
```

- AAA サーバグループを定義するには、次のコマンドを入力します。

```
aaa group server ldap  
  
server
```

- サーバを定義するには、次のコマンドを入力します。

```
ldap server  
  
ipv4  
attribute map  
  
bind authentication root-dn password  
  
base-dn
```

- 使用する認証方式のリストを定義するには、次のコマンドを入力します。

```
aaa authentication login group
```

## AD ツール

ユーザの絶対識別名 ( DN ) をチェックするには、AD のコマンド プロンプトから次のいずれかのコマンドを入力します。

```
dsquery user -name user1
```

または

```
dsquery user -samid user1
```

注：上に挙げた「user1」はregex文字列です。regex 文字列に「user\*」を使用して、user から開始されるユーザ名を持つすべての DN を登録することもできます。

シングル ユーザのすべての属性を登録するには、AD のコマンド プロンプトで次のコマンドを入力します。

```
dsquery * -filter "(&(objectCategory=Person)(sAMAccountName=username))" -attr *
```

## 潜在的な問題

LDAP 導入では、検索操作が最初に実行され、バインド操作が後で実行されます。この操作が行われるのは、検索操作の一部としてパスワード属性が返される場合に、LDAP クライアントでローカル的にパスワード検証を実施でき、追加のバインド操作が不要であるためです。パスワード属性が返されない場合は、バインド操作を後で実行できます。検索操作を先に実行し、バインド操作を後で実行するもう一つの利点は、ユーザ名 ( CN 値 ) の前にベース DN が付加されているときに DN を形成するのではなく、検索結果で受け取った DN をユーザ DN として使用できる点です。

ユーザ名属性のマッピングのポイントを変更するユーザ定義属性とともに **authentication bind-first** コマンドを使用すると問題がある可能性があります。たとえば、この設定を使用すると、認証を試行したときに通常は失敗します。

```
ldap server ss-ldap
ipv4 192.168.1.3
attribute map ad-map
transport port 3268
bind authenticate root-dn CN=abcd,OU=Employees,OU=qwrt Users,DC=qwrt,DC=com
password blabla
base-dn DC=qwrt,DC=com
authentication bind-first
ldap attribute-map ad-map
map type sAMAccountName username
```

その結果、Invalid credentials, Result code =49 次のようなログ メッセージが出力されます。

```
Oct 4 13:03:08.503: LDAP: LDAP: Queuing AAA request 0 for processing
Oct 4 13:03:08.503: LDAP: Received queue event, new AAA request
Oct 4 13:03:08.503: LDAP: LDAP authentication request
Oct 4 13:03:08.503: LDAP: Attempting first next available LDAP server
```

```
Oct 4 13:03:08.503: LDAP: Got next LDAP server :ss-ldap
Oct 4 13:03:08.503: LDAP: First Task: Send bind req
Oct 4 13:03:08.503: LDAP: Authentication policy: bind-first
Oct 4 13:03:08.503: LDAP: Dynamic map configured
Oct 4 13:03:08.503: LDAP: Dynamic map found for aaa type=username
Oct 4 13:03:08.503: LDAP: Bind: User-DN=sAMAccountName=abcd,DC=qwrt,DC=com
ldap_req_encode
Doing socket write
Oct 4 13:03:08.503: LDAP: LDAP bind request sent successfully (reqid=36)
Oct 4 13:03:08.503: LDAP: Sent the LDAP request to server
Oct 4 13:03:08.951: LDAP: Received socket event
Oct 4 13:03:08.951: LDAP: Checking the conn status
Oct 4 13:03:08.951: LDAP: Socket read event socket=0
Oct 4 13:03:08.951: LDAP: Found socket ctx
Oct 4 13:03:08.951: LDAP: Receive event: read=1, errno=9 (Bad file number)
Oct 4 13:03:08.951: LDAP: Passing the client ctx=314BA6ECldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_read_activity lc 0x296EA104
Doing socket read
LDAP-TCP:Bytes read = 109
ldap_match_request succeeded for msgid 36 h 0
changing lr 0x300519E0 to COMPLETE as no continuations
removing request 0x300519E0 from list as lm 0x296C5170 all 0
ldap_msgfree
ldap_msgfree
Oct 4 13:03:08.951: LDAP:LDAP Messages to be processed: 1
Oct 4 13:03:08.951: LDAP: LDAP Message type: 97
Oct 4 13:03:08.951: LDAP: Got ldap transaction context from reqid
36ldap_parse_result
Oct 4 13:03:08.951: LDAP: resultCode: 49 (Invalid credentials)
Oct 4 13:03:08.951: LDAP: Received Bind Responseldap_parse_result
ldap_err2string
Oct 4 13:03:08.951: LDAP: Ldap Result Msg: FAILED:Invalid credentials,
Result code =49
Oct 4 13:03:08.951: LDAP: LDAP Bind operation result : failed
Oct 4 13:03:08.951: LDAP: Restoring root bind status of the connection
Oct 4 13:03:08.951: LDAP: Performing Root-Dn bind operationldap_req_encode
Doing socket write
Oct 4 13:03:08.951: LDAP: Root Bind on CN=abcd,DC=qwrt,DC=com
initiated.ldap_msgfree
Oct 4 13:03:08.951: LDAP: Closing transaction and reporting error to AAA
Oct 4 13:03:08.951: LDAP: Transaction context removed from list [ldap reqid=36]
Oct 4 13:03:08.951: LDAP: Notifying AAA: REQUEST FAILED
Oct 4 13:03:08.951: LDAP: Received socket event
Oct 4 13:03:09.491: LDAP: Received socket event
Oct 4 13:03:09.491: LDAP: Checking the conn status
Oct 4 13:03:09.491: LDAP: Socket read event socket=0
Oct 4 13:03:09.491: LDAP: Found socket ctx
Oct 4 13:03:09.495: LDAP: Receive event: read=1, errno=9 (Bad file number)
Oct 4 13:03:09.495: LDAP: Passing the client ctx=314BA6ECldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_read_activity lc 0x296EA104
Doing socket read
LDAP-TCP:Bytes read= 22
ldap_match_request succeeded for msgid 37 h 0
changing lr 0x300519E0 to COMPLETE as no continuations
removing request 0x300519E0 from list as lm 0x296C5170 all 0
ldap_msgfree
ldap_msgfree
Oct 4 13:03:09.495: LDAP: LDAP Messages to be processed: 1
Oct 4 13:03:09.495: LDAP: LDAP Message type: 97
Oct 4 13:03:09.495: LDAP: Got ldap transaction context from reqid
```

```
37ldap_parse_result
Oct  4 13:03:09.495: LDAP: resultCode:      0      (Success)P: Received Bind
Response
Oct  4 13:03:09.495: LDAP: Received Root Bind Response ldap_parse_result
Oct  4 13:03:09.495: LDAP: Ldap Result Msg: SUCCESS, Result code =0
Oct  4 13:03:09.495: LDAP: Root DN bind Successful on:CN=abcd,DC=qwrt,DC=com
Oct  4 13:03:09.495: LDAP: Transaction context removed from list [ldap reqid=37]
ldap_msgfree
ldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_err2string
Oct  4 13:03:09.495: LDAP: Finished processing ldap msg, Result:Success
Oct  4 13:03:09.495: LDAP: Received socket event
```

強調表示された行は、認証の前に最初のバインドで問題のある箇所を示します。上記の設定から authentication bind-first コマンドを除去すると正常に動作します。

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- show ldap attributes
- show ldap server all

## トラブルシューティング

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。

### トラブルシューティングのためのコマンド

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：[debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- debug ldap all
- debug ldap event
- aaa 認証のデバッグ
- debug aaa authorization

## 関連情報

- [AAA LDAP 設定ガイド、Cisco IOS Release 15.1MT](#)
- [ASA 8.0 : WebVPN ユーザのための LDAP 認証の設定](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)