

Configurar o Catalyst 9800 WLC com autenticação LDAP para 802.1X e autenticação da Web

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar LDAP com um SSID Webauth](#)

[Diagrama de Rede](#)

[Configurar o controlador](#)

[Configurar LDAP com um SSID dot1x \(usando EAP local\)](#)

[Entender detalhes do servidor LDAP](#)

[Entender campos na interface do usuário da Web do 9800](#)

[Autenticação LDAP 802.1x com atributo sAMAccountName.](#)

[Configuração da WLC:](#)

[Verificar a partir da interface da Web:](#)

[Verificar](#)

[Troubleshoot](#)

[Como verificar o processo de autenticação no controlador](#)

[Como verificar a conectividade de 9800 para LDAP](#)

[Referências](#)

Introduction

Este documento descreve como configurar um Catalyst 9800 para autenticar clientes com um Servidor LDAP como o banco de dados para credenciais de usuário.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Servidores Microsoft Windows
- Active Directory ou qualquer outro banco de dados LDAP

Componentes Utilizados

C9800 EWC no Access Point (AP) C9100 com Cisco IOS®-XE versão 17.3.2a

Servidor Microsoft Active Directory (AD) com Armazenamento de Acesso à Rede (NAS) QNAP que atua como banco de dados LDAP

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar LDAP com um SSID Webauth

Diagrama de Rede

Este artigo foi escrito com base em uma configuração muito simples:

Um EWC AP 9115 com IP 192.168.1.15

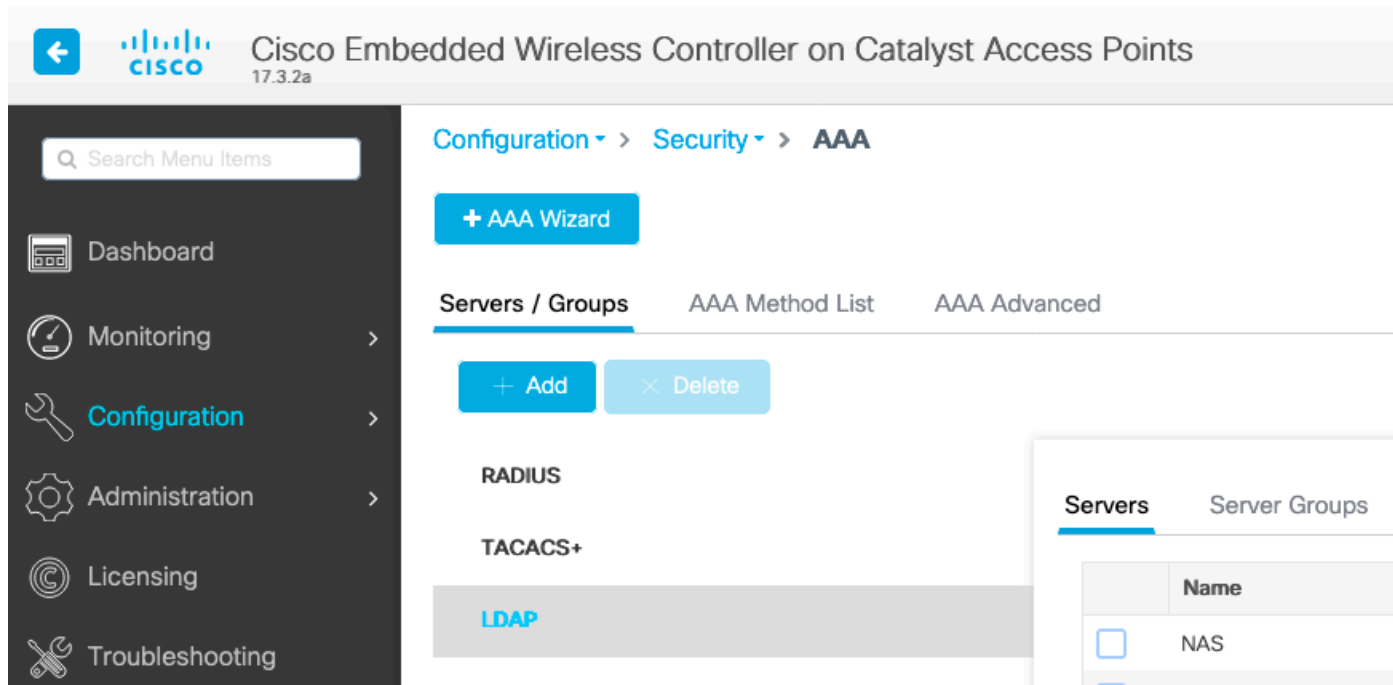
Um servidor Active Directory com IP 192.168.1.192

Um cliente que se conecta ao AP interno do EWC

Configurar o controlador

Etapa 1. Configurar o servidor LDAP

Navegue para **Configuration > Security > AAA > Servers/Groups > LDAP** e clique em **+ Add**



The screenshot shows the Cisco Embedded Wireless Controller configuration interface. The breadcrumb navigation is **Configuration > Security > AAA**. Under the **Servers / Groups** tab, there are buttons for **+ Add** and **× Delete**. The **LDAP** option is selected and highlighted in blue. A table on the right shows the list of servers:

Servers	
	Name
<input type="checkbox"/>	NAS

Escolha um nome para o servidor LDAP e preencha os detalhes. Para obter explicações sobre cada campo, consulte a seção "Compreender os detalhes do servidor LDAP" deste documento.

Server Name*	<input type="text" value="AD"/>					
Server Address*	<input type="text" value="192.168.1.192"/>	⚠ Provide a valid Server address				
Port Number*	<input type="text" value="389"/>					
Simple Bind	<input type="text" value="Authenticated"/>					
Bind User name*	<input type="text" value="Administrator@lab.cor"/>					
Bind Password *	<input type="text" value="."/>					
Confirm Bind Password*	<input type="text" value="."/>					
User Base DN*	<input type="text" value="CN=Users,DC=lab,DC:"/>					
User Attribute	<input type="text"/>					
User Object Type	<input type="text"/>	+				
	<table border="1"> <thead> <tr> <th>User Object Type</th> <th>Remove</th> </tr> </thead> <tbody> <tr> <td>Person</td> <td>✕</td> </tr> </tbody> </table>	User Object Type	Remove	Person	✕	
User Object Type	Remove					
Person	✕					
Server Timeout (seconds)	<input type="text" value="0-65534"/>					
Secure Mode	<input type="checkbox"/>					
Trustpoint Name	<input type="text"/>					

Salvar clicando em **Atualizar e aplicar ao dispositivo**

Comandos CLI:

```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

Etapa 2. Configurar um grupo de servidores LDAP.

Navegue para **Configuration > Security > AAA > Servers/ Groups > LDAP > Server Groups** e clique em **+ADD**

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers **Server Groups**

Name	Server 1	Ser
<input type="checkbox"/> Idapgr	AD	N/A

1 10 items per page

Digite um nome e adicione o servidor LDAP que você configurou na etapa anterior.

Name*

Idapgr

Group Type

LDAP

Available Servers

Assigned Servers

NAS

AD

>

<

>>

<<

⌵

⌶

⌵

⌵

Clique em **Update and apply** para salvar.

Comandos CLI :

```
aaa group server ldap ldapgr server AD
```

Etapa 3. Configurar o método de autenticação AAA

Navegue para **Configuration > Security > AAA > AAA method List > Authentication** e clique em **+Add**

+ AAA Wizard

Authentication

Authorization

Accounting

+ Add × Delete

	Name	Type	Group Type	Group1
<input type="checkbox"/>	default	login	local	N/A
<input type="checkbox"/>	ldapauth	login	group	ldapgr

Insira um nome, escolha o tipo **Login** e aponte para o grupo de servidores LDAP configurado anteriormente.

Quick Setup: AAA Authentication

Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Available Server Groups Assigned Server Groups

radius

ldap

tacacs+

>

<

>>

<<

ldapgr

⏪

⏩

⏴

⏵

Comandos CLI :

```
aaa authentication login ldapauth group ldapgr
```

Etapa 4. Configurar um método de autorização AAA

Navegue para **Configuration > Security > AAA > AAA method list > Authorization** e clique em **+Add**

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add
× Delete

	Name	Type	Group Type	Group1
<input type="checkbox"/>	default	credential-download	group	ldapgr
<input type="checkbox"/>	ldapauth	credential-download	group	ldapgr

1 items per page

Crie uma regra do tipo de download de credenciais com o nome de sua escolha e aponte-a para o grupo de servidores LDAP criado anteriormente

Quick Setup: AAA Authorization

Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Authenticated

Available Server Groups

radius

ldap

tacacs+

>

<

>>

<<

Assigned Server Groups

ldapgr

⏪

⏩

⏴

⏵

Comandos CLI :

```
aaa authorization credential-download ldapauth group ldapgr
```

Etapa 5. Configurar a autenticação local

Navegue até **Configuration > Security > AAA > AAA Advanced > Global Config**

Defina a autenticação local e a autorização local como **Lista de métodos** e selecione o método de autenticação e autorização configurado anteriormente.

[+ AAA Wizard](#)

Servers / Groups AAA Method List **AAA Advanced**

Global Config

- RADIUS Fallback
- Attribute List Name
- Device Authentication
- AP Policy
- Password Policy
- AAA Interface

Local Authentication	Method List
Authentication Method List	ldapauth
Local Authorization	Method List
Authorization Method List	ldapauth
Radius Server Load Balance	<input checked="" type="checkbox"/> DISABLED
Interim Update	<input type="checkbox"/>

[Show Advanced Settings >>>](#)

Comandos CLI :

```
aaa local authentication ldapauth authorization ldapauth
```

Etapa 6. Configurar o mapa de parâmetros webauth

Navegue até **Configuration > Security > Web Auth** e edite o mapa global

Configuration > Security > Web Auth

[+ Add](#) [× Delete](#)

	Parameter Map Name
<input type="checkbox"/>	global

« ‹ 1 › » 10 items per page

Certifique-se de configurar um endereço IPv4 virtual, como 192.0.2.1 (esse IP/sub-rede específico é reservado para IP virtual não roteável).

Edit Web Auth Parameter

General

Advanced

Parameter-map name	<input type="text" value="global"/>
Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Banner Title <input type="radio"/> File Name
Maximum HTTP connections	<input type="text" value="100"/>
Init-State Timeout(secs)	<input type="text" value="120"/>
Type	<input type="text" value="webauth"/>
Virtual IPv4 Address	<input type="text" value="192.0.2.1"/>
Trustpoint	<input type="text" value="--- Select ---"/>
Virtual IPv4 Hostname	<input type="text"/>
Virtual IPv6 Address	<input type="text" value=":::"/>
Web Auth intercept HTTPs	<input type="checkbox"/>
Watch List Enable	<input type="checkbox"/>
Watch List Expiry Timeout(secs)	<input type="text" value="600"/>
Captive Bypass Portal	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>
Sleeping Client Status	<input type="checkbox"/>
Sleeping Client Timeout (minutes)	<input type="text" value="720"/>

Clique em **Aplicar** para salvar.

Comandos CLI :

```
parameter-map type webauth global type webauth virtual-ip ipv4 192.0.2.1
```

Etapa 7. Configurar uma WLAN de webauth

Navegue até **Configuration > WLANs** e clique em **+Add**

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security Add To Policy Tags

⚠ Please add the WLANs to Policy Tags for them to broadcast.

Profile Name*	<input type="text" value="webauth"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="webauth"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="2"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Configure o nome, verifique se ele está no estado habilitado e vá para a guia **Segurança**.

Na subguia **Layer 2**, certifique-se de que não haja segurança e que a transição rápida esteja desativada.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input type="checkbox"/>	Fast Transition	<input type="text" value="Disabled"/>
OWE Transition Mode	<input type="checkbox"/>	Over the DS	<input type="checkbox"/>
		Reassociation Timeout	<input type="text" value="20"/>

Na guia **Layer3**, ative a **política da Web**, defina o mapa de parâmetros como **global** e defina a lista de autenticação para o método de login aaa configurado anteriormente.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy



[Show Advanced Settings >>>](#)

Web Auth Parameter Map

global



Authentication List

ldapauth



For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Salvar clicando em **Aplicar**

Comandos CLI :

```
wlan webauth 2 webauth no security ft adaptive no security wpa no security wpa wpa2 no security wpa wpa2 ciphers aes no security wpa akm dot1x security web-auth security web-auth authentication-list ldapauth security web-auth parameter-map global no shutdown
```

Etapa 8. Verifique se o SSID foi transmitido

Navegue até **Configuration > Tags** e verifique se o SSID está incluído no perfil de política atualmente em serviço pelo SSID (a tag de política padrão para uma nova configuração nova se você ainda não tiver configurado as tags). Por padrão, a tag-política padrão não transmite novos SSIDs criados até que você os inclua manualmente.

Este artigo não aborda a configuração de perfis de política e presume que você esteja familiarizado com essa parte da configuração.

Configurar LDAP com um SSID dot1x (usando EAP local)

A configuração do LDAP para um SSID 802.1X no 9800 normalmente exige também a configuração do EAP local. Se você fosse usar o RADIUS, seria seu servidor RADIUS estabelecer uma conexão com o banco de dados LDAP e isso está fora do escopo deste artigo. Antes de tentar essa configuração, é recomendável configurar o EAP Local primeiro com um usuário local configurado no WLC. Um exemplo de configuração é fornecido na seção de referências no final deste artigo. Depois de concluído, você pode tentar mover o banco de dados do usuário para LDAP.

Etapa 1. Configurar um perfil EAP Local

Navegue até **Configuration > Local EAP** e clique em **+Add**



Search Menu Items



Dashboard



Monitoring



Configuration



Administration



Licensing



Troubleshooting

Configuration > Security > Local EAP

Local EAP Profiles

EAP-FAST Parameters

+ Add

× Delete

	Profile Name
<input type="checkbox"/>	PEAP

1 10 items per page

Escolha qualquer nome para o seu perfil. Habilite pelo menos o PEAP e escolha um Nome de Ponto de Confiança. Por padrão, sua WLC tem apenas certificados autoassinados, portanto, não importa qual você escolha (normalmente TP-self-signed-xxxx é o melhor para essa finalidade), mas como as novas versões do sistema operacional dos smartphones confiam menos e menos certificados autoassinados, considere a instalação de um certificado confiável assinado publicamente.

Edit Local EAP Profiles

Profile Name*

PEAP

LEAP

EAP-FAST

EAP-TLS

PEAP

Trustpoint Name

TP-self-signed-3059

Comandos CLI :

```
eap profile PEAP method peap pki-trustpoint TP-self-signed-3059261382
```

Etapa 2. Configurar o servidor LDAP

Navegue para **Configuration > Security > AAA > Servers/Groups > LDAP** e clique em **+ Add**

The screenshot shows the Cisco Embedded Wireless Controller configuration interface. The breadcrumb navigation is **Configuration > Security > AAA**. The main content area is titled **Servers / Groups** and includes a **+ AAA Wizard** button. Below this, there are three tabs: **Servers / Groups** (selected), **AAA Method List**, and **AAA Advanced**. There are **+ Add** and **× Delete** buttons. The **Servers** tab is active, showing a table with a **Name** column. One entry is visible: **NAS**. The **LDAP** option is highlighted in the left sidebar.

Escolha um nome para o servidor LDAP e preencha os detalhes. Para obter explicações sobre cada campo, consulte a seção "Compreender os detalhes do servidor LDAP" deste documento.

Server Name*	<input type="text" value="AD"/>					
Server Address*	<input type="text" value="192.168.1.192"/>	<div style="border: 1px solid gray; padding: 2px; display: inline-block;">ⓘ Provide a valid Server address</div>				
Port Number*	<input type="text" value="389"/>					
Simple Bind	<input type="text" value="Authenticated"/>					
Bind User name*	<input type="text" value="Administrator@lab.cor"/>					
Bind Password *	<input type="text" value="."/>					
Confirm Bind Password*	<input type="text" value="."/>					
User Base DN*	<input type="text" value="CN=Users,DC=lab,DC:"/>					
User Attribute	<input type="text"/>					
User Object Type	<input type="text"/>	+				
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="text-align: left;">User Object Type</th> <th style="text-align: right;">Remove</th> </tr> </thead> <tbody> <tr> <td>Person</td> <td style="text-align: right;">×</td> </tr> </tbody> </table>		User Object Type	Remove	Person	×
User Object Type	Remove					
Person	×					
Server Timeout (seconds)	<input type="text" value="0-65534"/>					
Secure Mode	<input type="checkbox"/>					
Trustpoint Name	<input type="text"/>					

Salvar clicando em **Atualizar e aplicar ao dispositivo**

```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

Etapa 3. Configurar um grupo de servidores LDAP.

Navegue para **Configuration > Security > AAA > Servers/ Groups > LDAP > Server Groups** e clique em **+ADD**

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Server 1	Ser
<input type="checkbox"/> Idapgr	AD	N/A

1 10 items per page

Digite um nome e adicione o servidor LDAP que você configurou na etapa anterior.

Name*

Idapgr

Group Type

LDAP

Available Servers

Assigned Servers

NAS

AD

>

<

>>

<<

⌵

⌶

⌵

⌵

Clique em **Update and apply** para salvar.

Comandos CLI :

```
aaa group server ldap ldapgr server AD
```

Etapa 4. Configurar um método de autenticação AAA

Navegue para **Configuration > Security > AAA > AAA Method List > Authentication** e clique em **+Add**

Configure um método de autenticação do tipo **dot1x** e aponte-o somente para local. Seria tentador apontar para o grupo de servidores LDAP, mas é o próprio WLC que atua como o autenticador

802.1X aqui (embora o banco de dados do usuário esteja no LDAP, mas esse é o trabalho do método de autorização).

Quick Setup: AAA Authentication

Method List Name*

ldapauth

Type*

dot1x



Group Type

local



Available Server Groups

Assigned Server Groups

radius
ldap
tacacs+
ldapgr



Comando CLI:

```
aaa authentication dot1x ldapauth local
```

Etapa 5. Configurar um método de autorização AAA

Navegue para **Configuration > Security > AAA > AAA Method List > Authorization** e clique em **+Add**

Crie um tipo de método de autorização **credential-download** e aponte para o grupo LDAP.

Quick Setup: AAA Authorization

Method List Name*

ldapauth

Type*

credential-download ▾



Group Type

group ▾



Fallback to local

Authenticated

Available Server Groups

radius
ldap
tacacs+



Assigned Server Groups

ldapgr



Comando CLI :

```
aaa authorization credential-download ldapauth group ldapgr
```

Etapa 6. Configurar detalhes da autenticação local

Navegue até **Configuration > Security > AAA > AAA Method List > AAA advanced**

Escolha **Method List** para autenticação e autorização e selecione o método de autenticação dot1x que aponta localmente e o método de autorização de download de credenciais que aponta para LDAP

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config	Local Authentication	Method List
RADIUS Fallback	Authentication Method List	ldapauth
Attribute List Name	Local Authorization	Method List
Device Authentication	Authorization Method List	ldapauth
AP Policy	Radius Server Load Balance	<input type="checkbox"/> DISABLED
Password Policy	Interim Update	<input type="checkbox"/>
AAA Interface	Show Advanced Settings >>>	

Comando CLI :

```
aaa local authentication ldapauth authorization ldapauth
```

Etapa 7. Configurar uma WLAN dot1x

Navegue até **Configuration > WLAN** e clique em **+Add**

Escolha um perfil e um nome SSID e verifique se ele está ativado.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security Add To Policy Tags

⚠ Please add the WLANs to Policy Tags for them to broadcast.

Profile Name*	LDAP	Radio Policy	All
SSID*	LDAP	Broadcast SSID	ENABLED <input checked="" type="checkbox"/>
WLAN ID*	1		
Status	ENABLED <input checked="" type="checkbox"/>		

Vá para a guia Layer 2 **security**.

Escolha WPA+WPA2 como modo de segurança da camada 2

Verifique se WPA2 e AES estão habilitados nos parâmetros WPA e habilite 802.1X

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

PSK

CCKM

FT + 802.1x

FT + PSK

802.1x-SHA256

PSK-SHA256

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Vá até a subguia AAA.

Escolha o método de autenticação dot1x criado anteriormente, ative a autenticação EAP local e escolha o perfil EAP configurado na primeira etapa.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Add To Policy Tags

Layer2 Layer3 **AAA**

Authentication List

ldapauth ⓘ

Local EAP Authentication



EAP Profile Name

PEAP

Salvar clicando em Aplicar

Comandos CLI:

```
wlan LDAP 1 LDAP local-auth PEAP security dot1x authentication-list ldapauth no shutdown
```

Etapa 8. Verificar se a WLAN está em broadcast.

Navegue até **Configuration > Tags** e verifique se o SSID está incluído no perfil de política atualmente em serviço pelo SSID (a tag de política padrão para uma nova configuração nova se você ainda não tiver configurado as tags). Por padrão, a tag-política padrão não transmite novos SSIDs criados até que você os inclua manualmente.

Este artigo não aborda a configuração de perfis de política e presume que você esteja familiarizado com essa parte da configuração.

Se estiver usando o Ative Directory, você deverá configurar o servidor do AD para enviar o atributo "userPassword". Esse atributo precisa ser enviado para a WLC. Isso ocorre porque a WLC faz a verificação, não o servidor do AD. Você também pode ter problemas de autenticação com o método PEAP-mschapv2, pois a senha nunca é enviada em texto não criptografado e, portanto, não pode ser verificada com o banco de dados LDAP. Somente o método PEAP-GTC funcionaria com determinados bancos de dados LDAP.

Entender detalhes do servidor LDAP

Entender campos na interface do usuário da Web do 9800

Este é um exemplo de um Ative Directory muito básico que atua como servidor LDAP configurado

Edit AAA LDAP Server



Server Name*	<input type="text" value="AD"/>					
Server Address*	<input type="text" value="192.168.1.192"/>	Provide a valid Server address				
Port Number*	<input type="text" value="389"/>					
Simple Bind	<input type="text" value="Authenticated"/>					
Bind User name*	<input type="text" value="Administrator@lab.cor"/>					
Bind Password *	<input type="password" value="."/>					
Confirm Bind Password*	<input type="password" value="."/>					
User Base DN*	<input type="text" value="CN=Users,DC=lab,DC:"/>					
User Attribute	<input type="text"/>					
User Object Type	<input type="text"/>					
	<table border="1"> <thead> <tr> <th>User Object Type</th> <th>Remove</th> </tr> </thead> <tbody> <tr> <td>Person</td> <td></td> </tr> </tbody> </table>	User Object Type	Remove	Person		
User Object Type	Remove					
Person						
Server Timeout (seconds)	<input type="text" value="0-65534"/>					
Secure Mode	<input type="checkbox"/>					
Trustpoint Name	<input type="text"/>					

Nome e IP são, esperamos, autoexplicativos.

Porta: 389 é a porta padrão para LDAP, mas o servidor pode usar outra.

Ligação simples : atualmente, é muito raro ter um banco de dados LDAP que suporte associação não autenticada (o que significa que qualquer pessoa pode fazer uma pesquisa LDAP nele sem qualquer forma de autenticação). A ligação simples autenticada é o tipo mais comum de autenticação e o que o Active Directory permite por padrão. Você pode inserir um nome de conta de administrador e uma senha para poder pesquisar no banco de dados de usuários a partir daí.

Associar nome de usuário: Você precisa apontar para um nome de usuário com privilégios de administrador no Ative Diretory. O AD tolera o formato "user@domain" para ele, enquanto muitos outros bancos de dados LDAP esperam um formato "CN=xxx,DC=xxx" para o nome de usuário. Um exemplo com outro banco de dados LDAP diferente do AD é fornecido mais adiante neste artigo.

Ligar senha: Insira a senha que o nome de usuário admin inseriu anteriormente.

DN base do usuário: Digite aqui a "raiz de pesquisa", que é o local na árvore LDAP onde as pesquisas começam. Neste exemplo, todos os nossos usos estão sob o grupo "Usuários", cujo DN é "CN=Users,DC=lab,DC=com" (já que o domínio LDAP do exemplo é lab.com). Um exemplo de como descobrir esse DN base do usuário é fornecido posteriormente nesta seção.

Atributo de usuário: Isso pode ser deixado em branco ou apontar para um mapa de atributos LDAP que indica qual campo LDAP conta como nome de usuário para seu banco de dados LDAP. No entanto, devido à ID de bug da Cisco [CSCv11813](#), a WLC tenta uma autenticação com o campo CN, não importa o que aconteça.

Tipo de objeto do usuário: Isso determina o tipo de objetos que são considerados usuários. Normalmente, é "Pessoa". Pode ser "Computadores" se você tiver um banco de dados do AD e autenticar contas de computador, mas o LDAP fornece mais uma vez muita personalização.

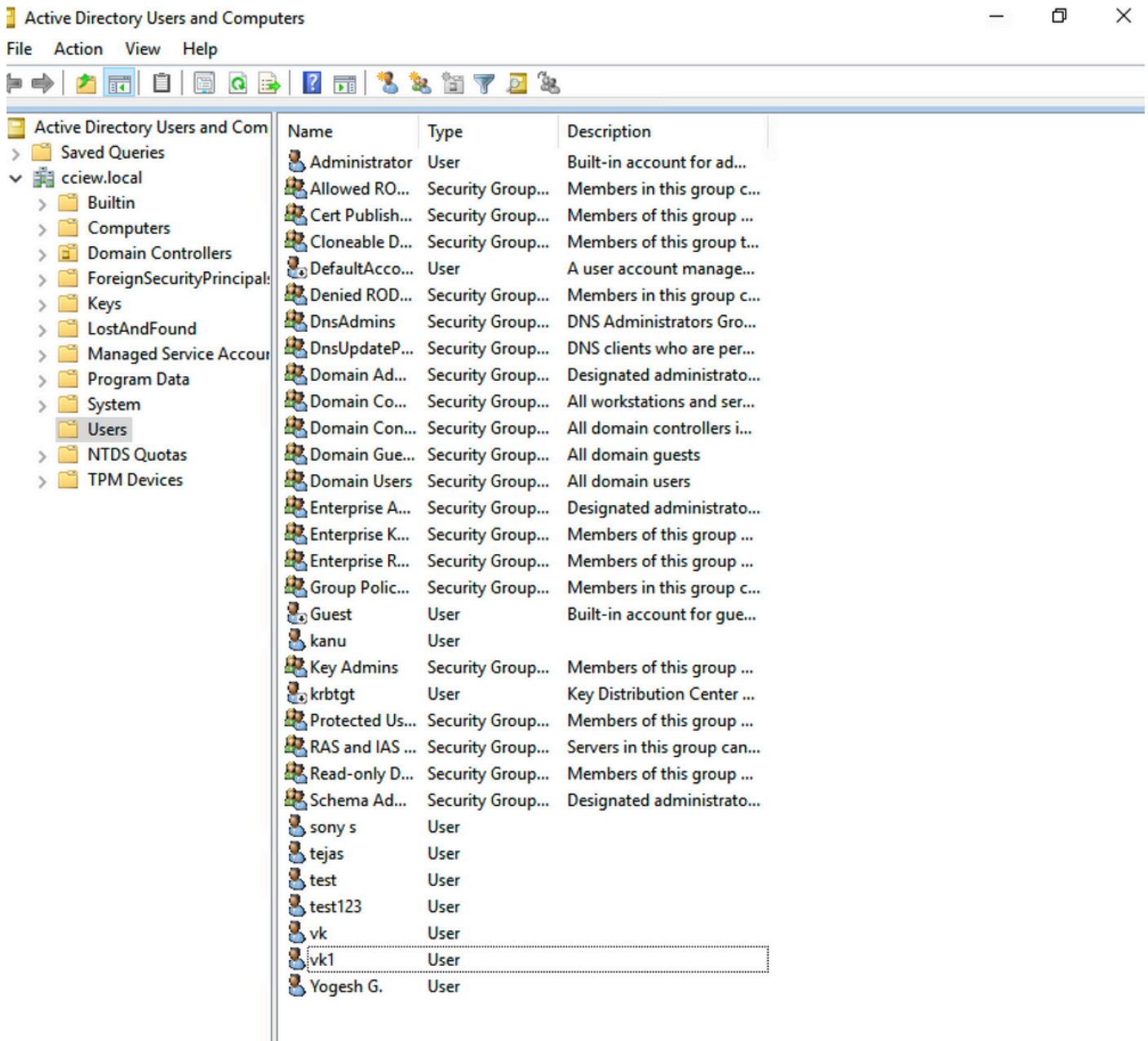
O modo seguro habilita o LDAP seguro sobre TLS e exige que você selecione um ponto confiável no 9800 para usar um certificado para a criptografia TLS.

Autenticação LDAP 802.1x com atributo sAMAaccountName.

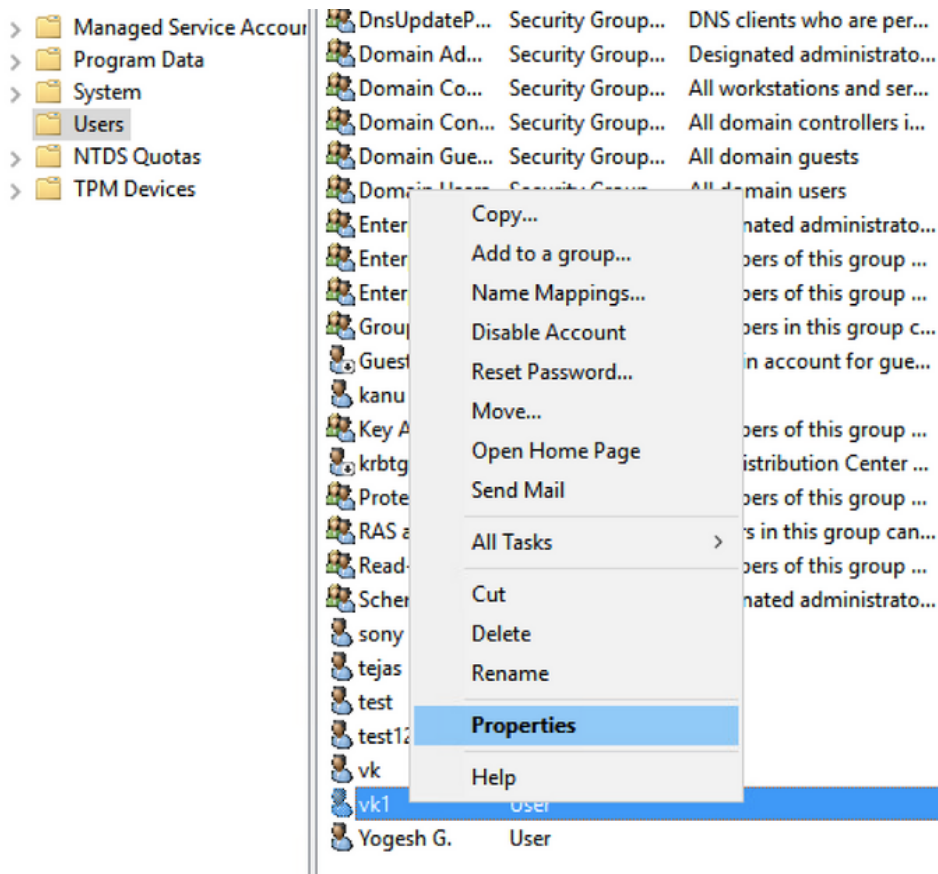
Esse aprimoramento foi introduzido na versão 17.6.1.

Configure o atributo "userPassword" para o usuário.

Etapa 1. No servidor Windows, navegue até Usuários e Computadores do Ative Diretory



Etapa 2. Clique com o botão direito do mouse no respectivo nome de usuário e selecione as propriedades



Etapa 3. Selecionar o editor de atributos na janela de propriedades

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
General	Address	Account	Profile	Telephones	Organization
Remote Desktop Services Profile			COM+	Attribute Editor	

Attributes:

Attribute	Value
uid	<not set>
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x10200 = (NORMAL_ACCOUNT DONT_I
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	vk1@cciew.local
userSharedFolder	<not set>

Edit

Filter

OK

Cancel

Apply

Help

Etapa 4. Configurar o atributo "userPassword". Esta é a senha do usuário, que precisa ser

configurada em valor Hex.

vk1 Properties



Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
General	Address	Account	Profile	Telephones
				Organization

Multi-valued Octet String Editor

Attribute: userPassword

Values:

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
General Address Account Profile Telephone Organization

Multi-valued Octet String Editor ✖

Octet String Attribute Editor ✖

Attribute: userPassword

Value format: Hexadecimal ▾

Value:
43 69 73 63 6F 31 32 33

Clear OK Cancel

OK Cancel Apply Help

Clique em ok, verifique se ele mostra a senha correta

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
General Address Account Profile Telephones Organization

Multi-valued Octet String Editor ✕

Attribute: userPassword

Values:

Cisco123

Add

Remove

Edit

OK

Cancel

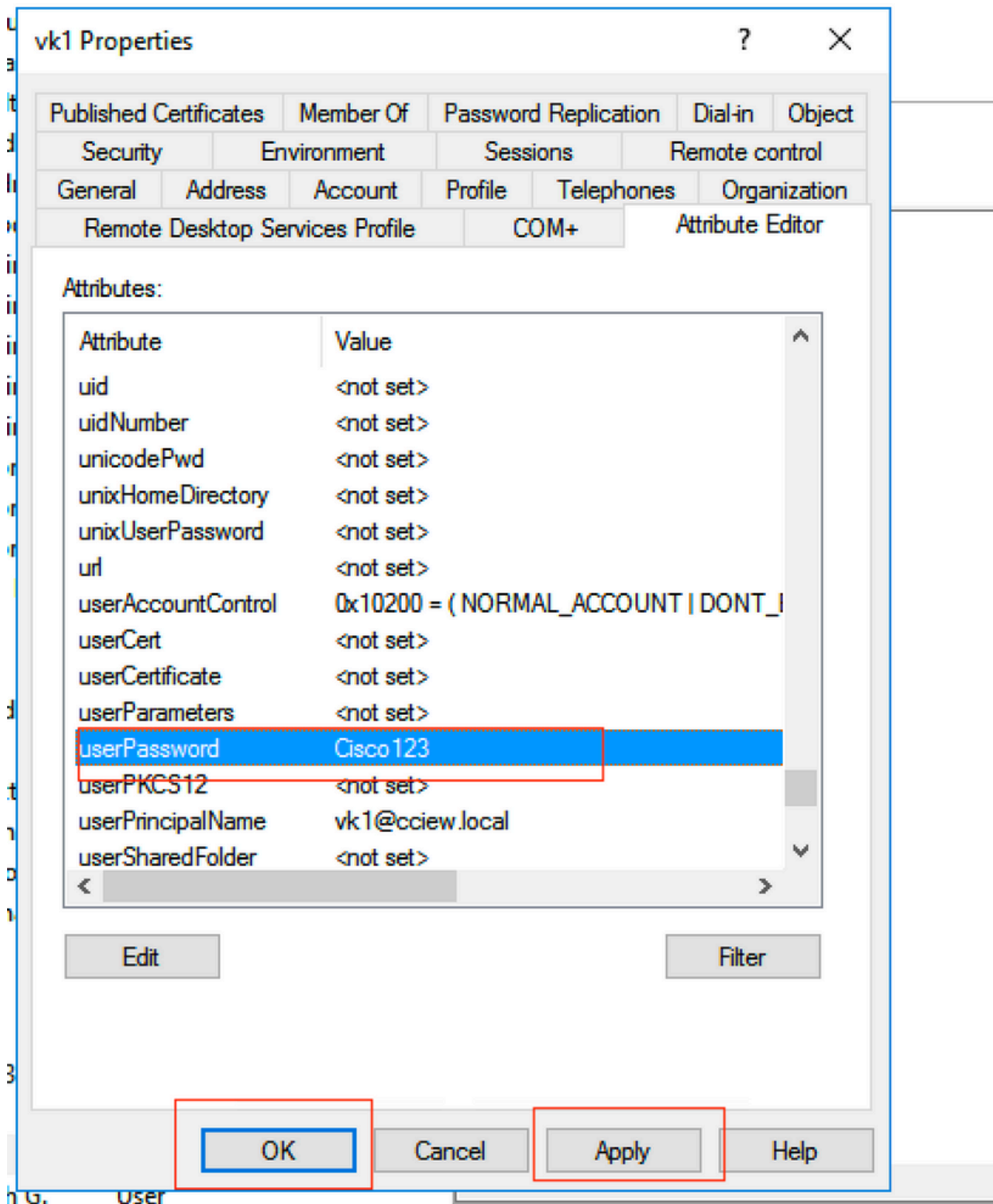
OK

Cancel

Apply

Help

Etapa 5. Clique em Aplicar e em OK



Etapa 6. Verifique o valor do atributo "sAMAccountName" para o usuário e ele usaria o nome de usuário para autenticação.

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
General	Address	Account	Profile	Telephones	Organization
Remote Desktop Services Profile		COM+	Attribute Editor		

Attributes:

Attribute	Value
sAMAccountName	vkokila
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT)
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	<not set>
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>
shadowMin	<not set>

Edit Filter

OK Cancel Apply Help

G. User

Configuração da WLC:

Etapa 1. Criar MAP de atributo LDAP

Etapa 2. Configure o atributo "sAMAccountName" e digite como "username"

Etapa 3. Escolha o atributo MAP criado na configuração do servidor LDAP.

```
ldap attribute-map VK
```

```
map type sAMAccountName username
```

```
ldap server ldap
```

```
ipv4 10.106.38.195
```

```
attribute map VK
```

```
bind authenticate root-dn vk1 password 7 00271A1507545A545C
```

```
base-dn CN=users,DC=cciew,DC=local
```

```
search-filter user-object-type Person
```

Verificar a partir da interface da Web:

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller web interface. The breadcrumb navigation is Configuration > Security > AAA. The main content area is titled "Servers / Groups" and includes a table of configured servers. A red box highlights the "ldap" server entry in the table.

Name	Server Address	Port Number	Simple Bind
ldap	10.106.38.195	389	Authenticated

Last login NA ...

Edit AAA LDAP Server

AAA Advanced

Server Groups

Name	Server Address
ldap	10.106.38.195

1 10 items per page

Server Name* ldap

Server Address* 10.106.38.195

Port Number* 389

Simple Bind Authenticated

Bind User name* vk1

Bind Password* .

Confirm Bind Password* .

User Base DN* CN=users,DC=cciew,DC

User Attribute VK

User Object Type

User Object Type	Remove
Person	X

Server Timeout (seconds) 30

Verificar

Para verificar sua configuração, verifique novamente os comandos CLI com os deste artigo.

Os bancos de dados LDAP normalmente não fornecem logs de autenticação, portanto pode ser difícil saber o que está acontecendo. Visite a seção Solução de problemas deste artigo para ver como capturar rastreamentos e farejadores para ver se uma conexão foi estabelecida com o banco de dados LDAP ou não.

Troubleshoot

Para solucionar esse problema, é melhor dividi-lo em duas partes. A primeira parte é validar a parte EAP local. A segunda é validar se o 9800 está se comunicando corretamente com o servidor LDAP.

Como verificar o processo de autenticação no controlador

Você pode coletar um rastreamento radioativo para obter as "depurações" da conexão do cliente.

Basta ir para **Troubleshooting > Radioative Trace**. Adicione o endereço MAC do cliente (preste atenção para o fato de que o seu cliente pode estar usando um MAC aleatório e não o seu próprio MAC; você pode verificar isso no perfil SSID no dispositivo do cliente em si) e pressione Start.

Depois de reproduzir a tentativa de conexão, você pode clicar em "Gerar" e obter os logs dos últimos X minutos. Certifique-se de clicar em **internal**, pois algumas linhas de log LDAP não serão exibidas se você não ativá-las.

Este é um exemplo de rastreamento radioativo de um cliente que se autentica com êxito em um SSID de autenticação da Web. Algumas peças redundantes foram removidas para maior clareza:

```
2021/01/19 21:57:55.890953 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC:
2elf.3a65.9c09 Association received. BSSID f80f.6f15.66ae, WLAN webauth, Slot 1 AP
f80f.6f15.66a0, AP7069-5A74-933C 2021/01/19 21:57:55.891049 {wncd_x_R0-0}{1}: [client-orch-sm]
[9347]: (debug): MAC: 2elf.3a65.9c09 Received Dot11 association request. Processing
started,SSID: webauth, Policy profile: LDAP, AP Name: AP7069-5A74-933C, Ap Mac Address:
f80f.6f15.66a0 BSSID MAC0000.0000.0000 wlan ID: 2RSSI: -45, SNR: 0 2021/01/19 21:57:55.891282
{wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2elf.3a65.9c09 Client state
transition: S_CO_INIT -> S_CO_ASSOCIATING 2021/01/19 21:57:55.891674 {wncd_x_R0-0}{1}: [dot11-
validate] [9347]: (info): MAC: 2elf.3a65.9c09 WiFi direct: Dot11 validate P2P IE. P2P IE not
present. 2021/01/19 21:57:55.892114 {wncd_x_R0-0}{1}: [dot11] [9347]: (debug): MAC:
2elf.3a65.9c09 dot11 send association response. Sending association response with
resp_status_code: 0 2021/01/19 21:57:55.892182 {wncd_x_R0-0}{1}: [dot11-frame] [9347]: (info):
MAC: 2elf.3a65.9c09 WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
2021/01/19 21:57:55.892248 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC: 2elf.3a65.9c09 dot11
send association response. Sending assoc response of length: 179 with resp_status_code: 0,
DOT11_STATUS: DOT11_STATUS_SUCCESS 2021/01/19 21:57:55.892467 {wncd_x_R0-0}{1}: [dot11] [9347]:
(note): MAC: 2elf.3a65.9c09 Association success. AID 2, Roaming = False, WGB = False, 11r =
False, 11w = False 2021/01/19 21:57:55.892497 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC:
2elf.3a65.9c09 DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED 2021/01/19
21:57:55.892616 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2elf.3a65.9c09 Station
Dot11 association is successful. 2021/01/19 21:57:55.892730 {wncd_x_R0-0}{1}: [client-orch-sm]
[9347]: (debug): MAC: 2elf.3a65.9c09 Starting L2 authentication. Bssid in state
machine:f80f.6f15.66ae Bssid in request is:f80f.6f15.66ae 2021/01/19 21:57:55.892783 {wncd_x_R0-
0}{1}: [client-orch-state] [9347]: (note): MAC: 2elf.3a65.9c09 Client state transition:
S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS 2021/01/19 21:57:55.892896 {wncd_x_R0-0}{1}:
[client-auth] [9347]: (note): MAC: 2elf.3a65.9c09 L2 Authentication initiated. method WEBAUTH,
Policy VLAN 1,AAA override = 0 2021/01/19 21:57:55.893115 {wncd_x_R0-0}{1}: [auth-mgr] [9347]:
(info): [2elf.3a65.9c09:capwap_90000004] Session Start event called from SANET-SHIM with
conn_hdl 14, vlan: 0 2021/01/19 21:57:55.893154 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] Wireless session sequence, create context with method WebAuth
2021/01/19 21:57:55.893205 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] - authc_list: ldapauth 2021/01/19 21:57:55.893211 {wncd_x_R0-
0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] - authz_list:
Not present under wlan configuration 2021/01/19 21:57:55.893254 {wncd_x_R0-0}{1}: [client-auth]
[9347]: (info): MAC: 2elf.3a65.9c09 Client auth-interface state transition: S_AUTHIF_INIT ->
S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP 2021/01/19 21:57:55.893461 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:unknown] auth mgr attr change notification is received for attr
(952) 2021/01/19 21:57:55.893532 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1263)
2021/01/19 21:57:55.893603 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (220)
2021/01/19 21:57:55.893649 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (952)
2021/01/19 21:57:55.893679 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] Retrieved Client IIF ID 0xd3001364 2021/01/19 21:57:55.893731
{wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] Allocated audit
session id 000000000000009C1CA610D7 2021/01/19 21:57:55.894285 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:capwap_90000004] Device type found in cache Samsung Galaxy S10e
2021/01/19 21:57:55.894299 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e
and old device-type not classified earlier &Device name for the session is detected as Unknown
Device and old device-name not classified earlier & Old protocol map 0 and new is 1057
2021/01/19 21:57:55.894551 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1337)
2021/01/19 21:57:55.894587 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:57:55.894593
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:57:55.894827 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received
```


for attr (1337) 2021/01/19 21:57:55.894858 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:57:55.894862 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004] access_session_acct_filter_spec is NULL 2021/01/19 21:57:55.895918 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [0000.0000.0000:unknown] retrieving vlanid from name failed 2021/01/19 21:57:55.896094 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] SM Reauth Plugin: Received valid timeout = 86400 2021/01/19 21:57:55.896807 {wncd_x_R0-0}{1}: [webauth-sm] [9347]: (info): [0.0.0.0]Starting Webauth, mac [2e:1f:3a:65:9c:09], IIF 0 , audit-ID 000000000000009C1CA610D7 2021/01/19 21:57:55.897106 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2elf.3a65.9c09][0.0.0.0]Applying IPv4 intercept ACL via SVM, name: IP-Adm-V4-Int-ACL-global, priority: 50, IIF-ID: 0 2021/01/19 21:57:55.897790 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] URL-Redirect-ACL = IP-Adm-V4-Int-ACL-global 2021/01/19 21:57:55.898813 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2elf.3a65.9c09][0.0.0.0]Applying IPv6 intercept ACL via SVM, name: IP-Adm-V6-Int-ACL-global, priority: 52, IIF-ID: 0 2021/01/19 21:57:55.899406 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] URL-Redirect-ACL = IP-Adm-V6-Int-ACL-global 2021/01/19 21:57:55.903552 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.3a65.9c09 Client auth-interface state transition: S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTHIF_L2_WEBAUTH_PENDING 2021/01/19 21:57:55.903575 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success. Resolved Policy bitmap:11 for client 2elf.3a65.9c09 2021/01/19 21:57:55.903592 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.3a65.9c09 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_PENDING 2021/01/19 21:57:55.903709 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.3a65.9c09 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_DONE 2021/01/19 21:57:55.903774 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is detected as Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1025 2021/01/19 21:57:55.903858 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is detected as Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1025 2021/01/19 21:57:55.903924 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is detected as Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1025 2021/01/19 21:57:55.904005 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2elf.3a65.9c09 L2 Authentication of station is successful., L3 Authentication : 1 2021/01/19 21:57:55.904173 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC: 2elf.3a65.9c09 Mobility discovery triggered. Client mode: Flex - Local Switching 2021/01/19 21:57:55.904181 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2elf.3a65.9c09 Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS 2021/01/19 21:57:55.904245 {wncd_x_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2elf.3a65.9c09 MMIF FSM transition: S_MA_INIT -> S_MA_MOBILITY_DISCOVERY_PROCESSED_TR on E_MA_MOBILITY_DISCOVERY 2021/01/19 21:57:55.904410 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2elf.3a65.9c09 Invalid transmitter ip in build client context 2021/01/19 21:57:55.904777 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2elf.3a65.9c09 Received mobile_announce, sub type: 0 of XID (0) from (WNCID[0]) 2021/01/19 21:57:55.904955 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2elf.3a65.9c09 Add MCC by tdl mac: client_ifid 0x90000006 is assigned to client 2021/01/19 21:57:55.905072 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 0000.0000.0000 Sending mobile_announce_nak of XID (0) to (WNCID[0]) 2021/01/19 21:57:55.905157 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2elf.3a65.9c09 Received mobile_announce_nak, sub type: 1 of XID (0) from (WNCID[0]) 2021/01/19 21:57:55.905267 {wncd_x_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2elf.3a65.9c09 MMIF FSM transition: S_MA_INIT_WAIT_ANNOUNCE_RSP -> S_MA_NAK_PROCESSED_TR on E_MA_NAK_RCVD 2021/01/19 21:57:55.905283 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2elf.3a65.9c09 Roam type changed - None -> None 2021/01/19 21:57:55.905317 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2elf.3a65.9c09 Mobility role changed - Unassoc -> Local 2021/01/19 21:57:55.905515 {wncd_x_R0-0}{1}: [mm-client] [9347]: (note): MAC: 2elf.3a65.9c09 Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IFID: 0x90000006, Client Role: Local PoA: 0x90000004 PoP: 0x0 2021/01/19 21:57:55.905570 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2elf.3a65.9c09 Processing mobility response from MMIF. Client ifid: 0x90000006, roam type: None, client role: Local 2021/01/19 21:57:55.906210 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2elf.3a65.9c09 Client QoS add mobile cb 2021/01/19 21:57:55.906369 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2elf.3a65.9c09 No QoS PM Name or QoS Level received from SANet for pm_dir:0. Check client is

fastlane, otherwise set pm name to none 2021/01/19 21:57:55.906399 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2elf.3a65.9c09 No QoS PM Name or QoS Level received from SANet for pm_dir:1. Check client is fastlane, otherwise set pm name to none 2021/01/19 21:57:55.906486 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2elf.3a65.9c09 ADD MOBILE sent. Client state flags: 0x12 BSSID: MAC: f80f.6f15.66ae capwap IFID: 0x90000004 2021/01/19 21:57:55.906613 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2elf.3a65.9c09 Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS 2021/01/19 21:57:55.907326 {wncd_x_R0-0}{1}: [dot11] [9347]: (note): MAC: 2elf.3a65.9c09 Client datapath entry params - ssid:webauth,slot_id:1 bssid ifid: 0x0, radio_ifid: 0x90000002, wlan_ifid: 0xf0400002 2021/01/19 21:57:55.907544 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2elf.3a65.9c09 Client QoS dpath create params 2021/01/19 21:57:55.907594 {wncd_x_R0-0}{1}: [avc-afc] [9347]: (debug): AVC enabled for client 2elf.3a65.9c09 2021/01/19 21:57:55.907701 {wncd_x_R0-0}{1}: [dpath_svc] [9347]: (note): MAC: 2elf.3a65.9c09 Client datapath entry created for ifid 0x90000006 2021/01/19 21:57:55.908229 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2elf.3a65.9c09 Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS 2021/01/19 21:57:55.908704 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS 2021/01/19 21:57:55.918694 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.3a65.9c09 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE 2021/01/19 21:57:55.922254 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2elf.3a65.9c09 Neighbor AP fc5b.3984.8220 lookup has failed, ap contextnot available on this instance 2021/01/19 21:57:55.922260 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2elf.3a65.9c09 Neighbor AP 88f0.3169.d390 lookup has failed, ap contextnot available on this instance 2021/01/19 21:57:55.962883 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (note): MAC: 2elf.3a65.9c09 Client IP learn successful. Method: IP Snooping IP: 192.168.1.17 2021/01/19 21:57:55.963827 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 Client IP learn successful. Method: IPv6 Snooping IP: fe80::2c1f:3aff:fe65:9c09 2021/01/19 21:57:55.964481 {wncd_x_R0-0}{1}: [auth_mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (8) 2021/01/19 21:57:55.965176 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE 2021/01/19 21:57:55.965550 {wncd_x_R0-0}{1}: [auth_mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (10) 2021/01/19 21:57:55.966127 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE 2021/01/19 21:57:55.966328 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2elf.3a65.9c09 Received ip learn response. method: IPLEARN_METHOD_IP_SNOOPING 2021/01/19 21:57:55.966413 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2elf.3a65.9c09 Triggered L3 authentication. status = 0x0, Success 2021/01/19 21:57:55.966424 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2elf.3a65.9c09 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS 2021/01/19 21:57:55.967404 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2elf.3a65.9c09 L3 Authentication initiated. LWA 2021/01/19 21:57:55.967433 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.3a65.9c09 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING 2021/01/19 21:57:55.968312 {wncd_x_R0-0}{1}: [sisf-packet] [9347]: (debug): RX: ARP from interface capwap_90000004 on vlan 1 Source MAC: 2elf.3a65.9c09 Dest MAC: ffff.ffff.ffff ARP REQUEST, ARP sender MAC: 2elf.3a65.9c09 ARP target MAC: ffff.ffff.ffff ARP sender IP: 192.168.1.17, ARP target IP: 192.168.1.17, 2021/01/19 21:57:55.968519 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 iplearn receive client learn method update. Prev method (IP Snooping) Cur method (ARP) 2021/01/19 21:57:55.968522 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 Client IP learn method update successful. Method: ARP IP: 192.168.1.17 2021/01/19 21:57:55.968966 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE 2021/01/19 21:57:57.762648 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 iplearn receive client learn method update. Prev method (ARP) Cur method (IP Snooping) 2021/01/19 21:57:57.762650 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 Client IP learn method update successful. Method: IP Snooping IP: 192.168.1.17 2021/01/19 21:57:57.763032 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2elf.3a65.9c09 IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE 2021/01/19 21:58:00.992597 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]GET rcvd when in INIT state 2021/01/19 21:58:00.992617 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:00.992669 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15] url

[http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:00.992694 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Retrieved user-agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:00.993558 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1248) 2021/01/19 21:58:00.993637 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:00.993645 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004] access_session_acct_filter_spec is NULL 2021/01/19 21:58:00.996320 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as Linux-Workstation and old Samsung Galaxy S10e &Device name for the session is detected as Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19 21:58:00.996508 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] DC Profile-name has been changed to Linux-Workstation 2021/01/19 21:58:00.996524 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] update event: Policy is not applied for this Handle 0xB7000080 2021/01/19 21:58:05.808144 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:05.808226 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15] url [http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:05.808251 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Retrieved user-agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:05.860465 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]GET rcvd when in GET_REDIRECT state 2021/01/19 21:58:05.860483 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:05.860534 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15] url [http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:05.860559 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Retrieved user-agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:06.628209 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]GET rcvd when in GET_REDIRECT state 2021/01/19 21:58:06.628228 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:06.628287 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Parse GET, src [192.168.1.17] dst [192.0.2.1] url [https://192.0.2.1:443/login.html?redirect=http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:06.628316 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Retrieved user-agent = Mozilla/5.0 (Linux; Android 11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile Safari/537.36 2021/01/19 21:58:06.628832 {wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Sending Webauth login form, len 8077 2021/01/19 21:58:06.629613 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1248) 2021/01/19 21:58:06.629699 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:06.629709 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004] access_session_acct_filter_spec is NULL 2021/01/19 21:58:06.633058 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e and old Linux-Workstation &Device name for the session is detected as Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19 21:58:06.633219 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] DC Profile-name has been changed to Samsung Galaxy S10e 2021/01/19 21:58:06.633231 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] update event: Policy is not applied for this Handle 0xB7000080 2021/01/19 21:58:06.719502 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]GET rcvd when in LOGIN state 2021/01/19 21:58:06.719521 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:06.719591 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Parse GET, src [192.168.1.17] dst [192.0.2.1] url [https://192.0.2.1:443/favicon.ico] 2021/01/19 21:58:06.719646 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Retrieved user-agent = Mozilla/5.0 (Linux; Android 11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile

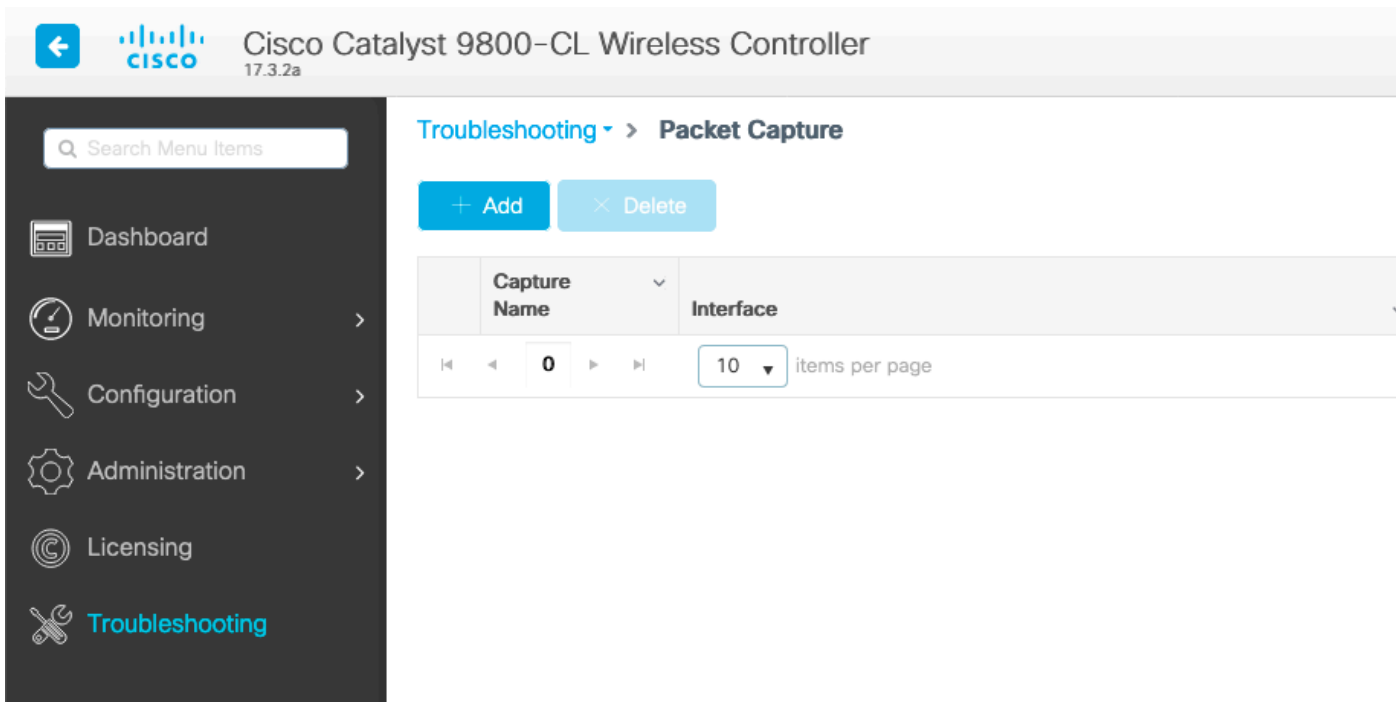
Safari/537.36 2021/01/19 21:58:06.720038 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]Parse logo GET, File "/favicon.ico" not found
2021/01/19 21:58:06.720623 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1248)
2021/01/19 21:58:06.720707 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:06.720716
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:06.724036 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:capwap_90000004] Device type for the session is detected as
Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is detected as
Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19
21:58:06.746127 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2elf.3a65.9c09][192.168.1.17]GET rcvd when in LOGIN state 2021/01/19
21:58:06.746145 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2elf.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:06.746197
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.0.2.1] url
[https://192.0.2.1:443/favicon.ico] 2021/01/19 21:58:06.746225 {wncd_x_R0-0}{1}: [webauth-httpd]
[9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]Retrieved user-agent = Mozilla/5.0
(Linux; Android 11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile
Safari/537.36 2021/01/19 21:58:06.746612 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info):
capwap_90000004[2elf.3a65.9c09][192.168.1.17]Parse logo GET, File "/favicon.ico" not found
2021/01/19 21:58:06.747105 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1248)
2021/01/19 21:58:06.747187 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:06.747197
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:06.750598 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:capwap_90000004] Device type for the session is detected as
Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is detected as
Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19
21:58:15.902342 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2elf.3a65.9c09][192.168.1.17]GET rcvd when in LOGIN state 2021/01/19
21:58:15.902360 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2elf.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:15.902410
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15] url
[http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:15.902435 {wncd_x_R0-0}{1}:
[webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]Retrieved user-
agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:15.903173 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:capwap_90000004] auth mgr attr change notification is received
for attr (1248) 2021/01/19 21:58:15.903252 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]:
(info): [2elf.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:15.903261
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:15.905950 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:capwap_90000004] Device type for the session is detected as
Linux-Workstation and old Samsung Galaxy S10e &Device name for the session is detected as
Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19
21:58:15.906112 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] DC
Profile-name has been changed to Linux-Workstation 2021/01/19 21:58:15.906125 {wncd_x_R0-0}{1}:
[auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_90000004] update event: Policy is not applied
for this Handle 0xB7000080 2021/01/19 21:58:16.357093 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]:
(info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]POST rcvd when in LOGIN state 2021/01/19
21:58:16.357443 {wncd_x_R0-0}{1}: [sadb-attr] [9347]: (info): Removing ipv6 addresses from the
attr list -1560276753,sm_ctx = 0x50840930, num_ipv6 = 1 2021/01/19 21:58:16.357674 {wncd_x_R0-
0}{1}: [caaa-authen] [9347]: (info): [CAAA:AUTHEN:b7000080] DEBUG: mlist=ldapauth for type=0
2021/01/19 21:58:16.374292 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_90000004] Authc success from WebAuth, Auth event success 2021/01/19
21:58:16.374412 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success.
Resolved Policy bitmap:0 for client 2elf.3a65.9c09 2021/01/19 21:58:16.374442 {wncd_x_R0-0}{1}:
[client-auth] [9347]: (info): MAC: 2elf.3a65.9c09 Client auth-interface state transition:
S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_PENDING 2021/01/19 21:58:16.374568 {wncd_x_R0-
0}{1}: [aaa-attr-inf] [9347]: (info): << username 0 "Nico">> 2021/01/19 21:58:16.374574

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): << sam-account-name 0 "Nico">> 2021/01/19
21:58:16.374584 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): << method 0 1 [webauth]>>
2021/01/19 21:58:16.374592 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): << clid-mac-addr 0
2e 1f 3a 65 9c 09 >> 2021/01/19 21:58:16.374597 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info):
<< intf-id 0 2415919108 (0x90000004)>> 2021/01/19 21:58:16.374690 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received
for attr (450) 2021/01/19 21:58:16.374797 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Received User-Name Nico for client 2e1f.3a65.9c09 2021/01/19
21:58:16.375294 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Applying IPv4 logout ACL via SVM, name: IP-Adm-V4-LOGOUT-ACL, priority: 51, IIF-ID:
0 2021/01/19 21:58:16.376120 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info):
[0000.0000.0000:unknown] URL-Redirect-ACL = IP-Adm-V4-LOGOUT-ACL 2021/01/19 21:58:16.377322
{wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]HTTP/1.0 200 OK 2021/01/19 21:58:16.378405 {wncd_x_R0-0}{1}: [client-auth] [9347]:
(note): MAC: 2e1f.3a65.9c09 L3 Authentication Successful. ACL:[ ] 2021/01/19 21:58:16.378426
{wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client auth-interface state
transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE 2021/01/19 21:58:16.379181
{wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Client QoS add mobile cb
2021/01/19 21:58:16.379323 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC:
2e1f.3a65.9c09 No QoS PM Name or QoS Level received from SANet for pm_dir:0. Check client is
fastlane, otherwise set pm name to none 2021/01/19 21:58:16.379358 {wncd_x_R0-0}{1}: [ewlc-qos-
client] [9347]: (info): MAC: 2e1f.3a65.9c09 No QoS PM Name or QoS Level received from SANet for
pm_dir:1. Check client is fastlane, otherwise set pm name to none 2021/01/19 21:58:16.379442
{wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 ADD MOBILE sent. Client
state flags: 0x8 BSSID: MAC: f80f.6f15.66ae capwap IFID: 0x90000004 2021/01/19 21:58:16.380547
{wncd_x_R0-0}{1}: [errmsg] [9347]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE:
Username entry (Nico) joined with ssid (webauth) for device with MAC: 2e1f.3a65.9c09 2021/01/19
21:58:16.380729 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute :bsn-vlan-
interface-name 0 "1" ] 2021/01/19 21:58:16.380736 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]:
(info): [ Applied attribute : timeout 0 86400 (0x15180) ] 2021/01/19 21:58:16.380812 {wncd_x_R0-
0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute : url-redirect-acl 0 "IP-Adm-V4-
LOGOUT-ACL" ] 2021/01/19 21:58:16.380969 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info):
MAC: 2e1f.3a65.9c09 Client QoS run state handler 2021/01/19 21:58:16.381033 {wncd_x_R0-0}{1}:
[rog-proxy-capwap] [9347]: (debug): Managed client RUN state notification: 2e1f.3a65.9c09
2021/01/19 21:58:16.381152 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC:
2e1f.3a65.9c09 Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN 2021/01/19
21:58:16.385252 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
QoS dpath run params 2021/01/19 21:58:16.385321 {wncd_x_R0-0}{1}: [avc-afc] [9347]: (debug): AVC
enabled for client 2e1f.3a65.9c09
```

Como verificar a conectividade de 9800 para LDAP

Você pode fazer uma captura incorporada no 9800 para ver qual tráfego está indo para LDAP.

Para fazer uma captura da WLC, navegue para **Troubleshooting > Packet Capture** e clique em **+Add**. Escolha a porta de uplink e inicie a captura.



Aqui está um exemplo de autenticação de sucesso para o usuário Nico

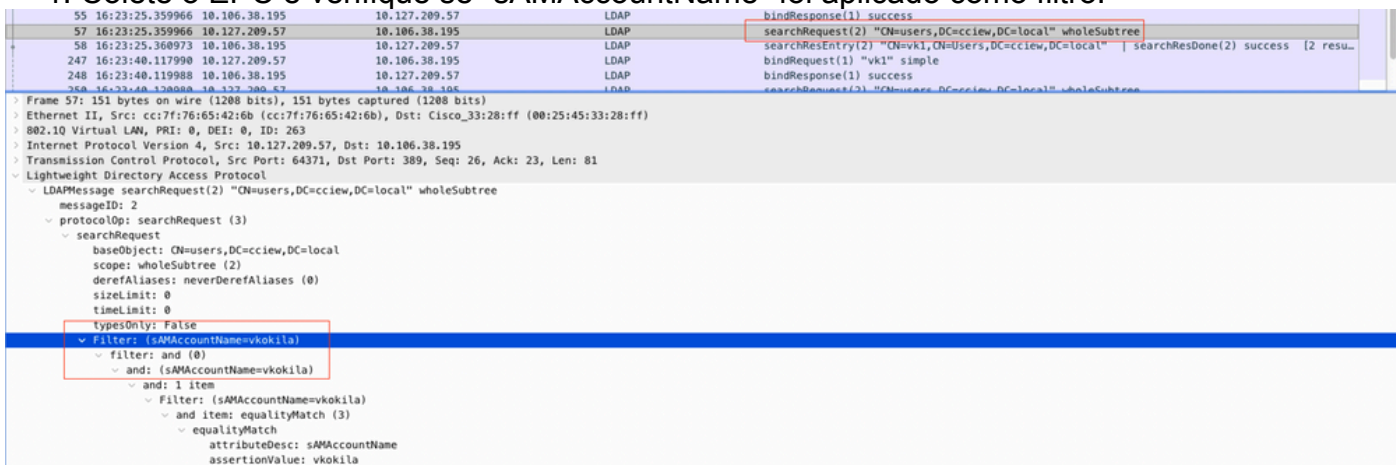
Time	Source	Destination	Protocol	Length	Info
8696	22:58:16.412748	192.168.1.15	192.168.1.192	108	LDAP bindRequest(1) "Administrator@lab.com" simple
8697	22:58:16.414425	192.168.1.192	192.168.1.15	88	LDAP bindResponse(1) success
8699	22:58:16.419645	192.168.1.15	192.168.1.192	128	LDAP searchRequest(2) "CN=Users,DC=lab,DC=com" wholeSubtree
8700	22:58:16.420536	192.168.1.192	192.168.1.15	1260	LDAP searchResEntry(2) "CN=Nico,CN=Users,DC=lab,DC=com" searchResDone(2) success [1 result]
8701	22:58:16.422383	192.168.1.15	192.168.1.192	117	LDAP bindRequest(3) "CN=Nico,CN=Users,DC=lab,DC=com" simple
8702	22:58:16.423513	192.168.1.192	192.168.1.15	88	LDAP bindResponse(3) success

Os 2 primeiros pacotes representam a ligação da WLC ao banco de dados LDAP, ou seja, a WLC que está se autenticando no banco de dados com o usuário admin (para poder executar uma pesquisa).

Esses 2 pacotes LDAP representam a WLC que faz uma pesquisa no DN base (aqui CN=Users,DC=lab,DC=com). O interior do pacote contém um filtro para o nome de usuário (aqui "Nico"). O banco de dados LDAP retorna os atributos do usuário como um sucesso

Os últimos 2 pacotes representam a WLC que está tentando se autenticar com essa senha de usuário para testar se a senha é a correta.

1. Colete o EPC e verifique se "sAMAccountName" foi aplicado como filtro:



Se o filtro mostrar "cn" e se "sAMAccountName" estiver sendo usado como o nome de usuário, a

autenticação falhará.

Reconfigure o atributo de mapa ldap da cli da WLC.

2. Certifique-se de que o servidor retorne "userPassword" em texto não criptografado, caso contrário a autenticação falhará.

```
1197 16:25:05.708962 10.127.209.57 10.106.38.195 LDAP searchRequest(3) "CN=users,DC=cciew,DC=local" wholeSubtree
1198 16:25:05.709954 10.106.38.195 10.127.209.57 LDAP searchResEntry(3) "CN=vk1,CN=Users,DC=cciew,DC=local" | searchResDone(3) success [2 res...

- PartialAttributeList item userPassword
  type: userPassword
  vals: 1 item
  AttributeValue: Cisco123
- PartialAttributeList item givenName
  type: givenName
  vals: 1 item
  AttributeValue: vk1
- PartialAttributeList item distinguishedName
  type: distinguishedName
  vals: 1 item
  AttributeValue: CN=vk1,CN=Users,DC=cciew,DC=local
- PartialAttributeList item instanceType
  type: instanceType
  vals: 1 item
  AttributeValue: 4
- PartialAttributeList item whenCreated
  type: whenCreated
```

3. Use a ferramenta ldp.exe no servidor para validar as informações do DN base.



FileZilla Client



Best match



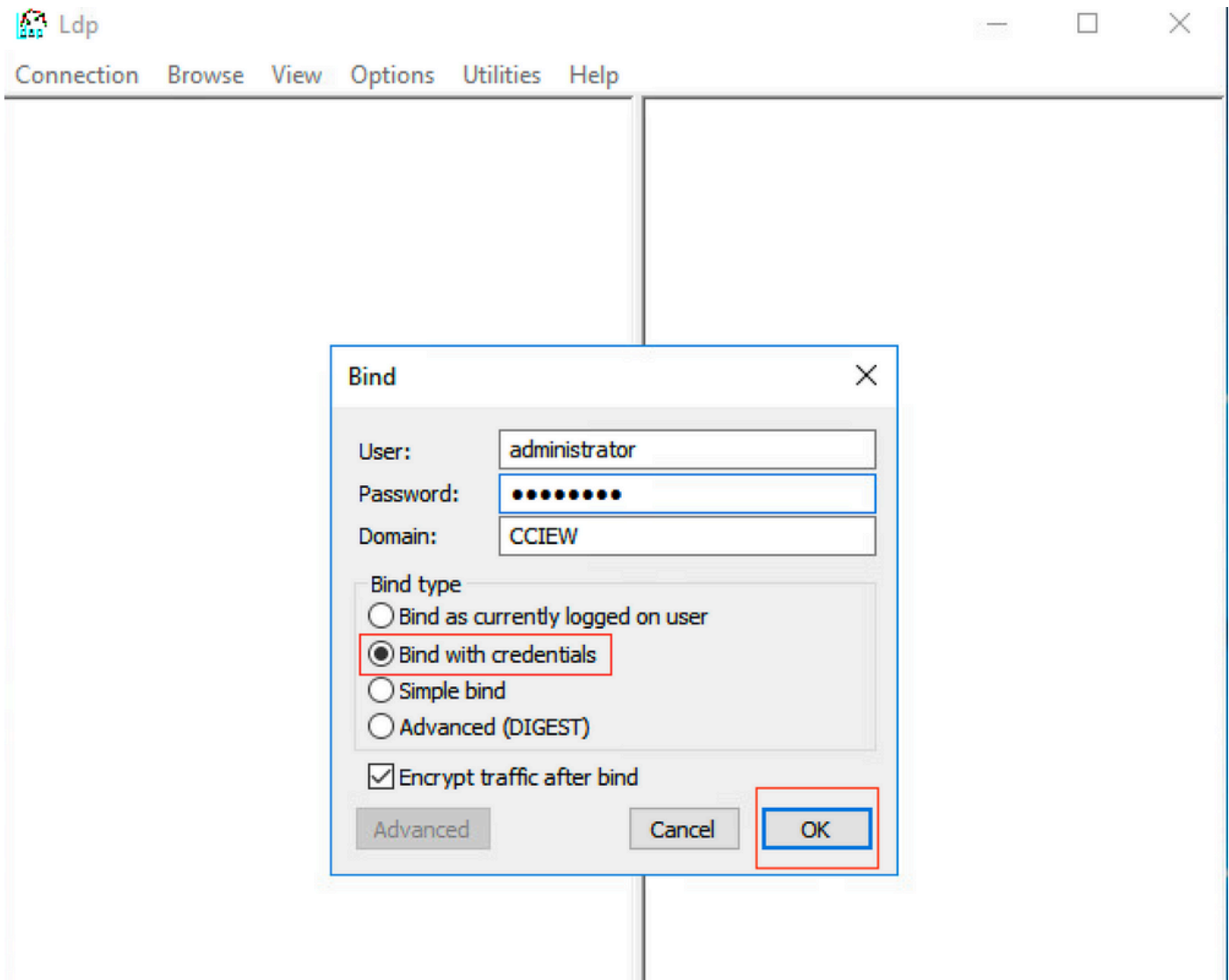
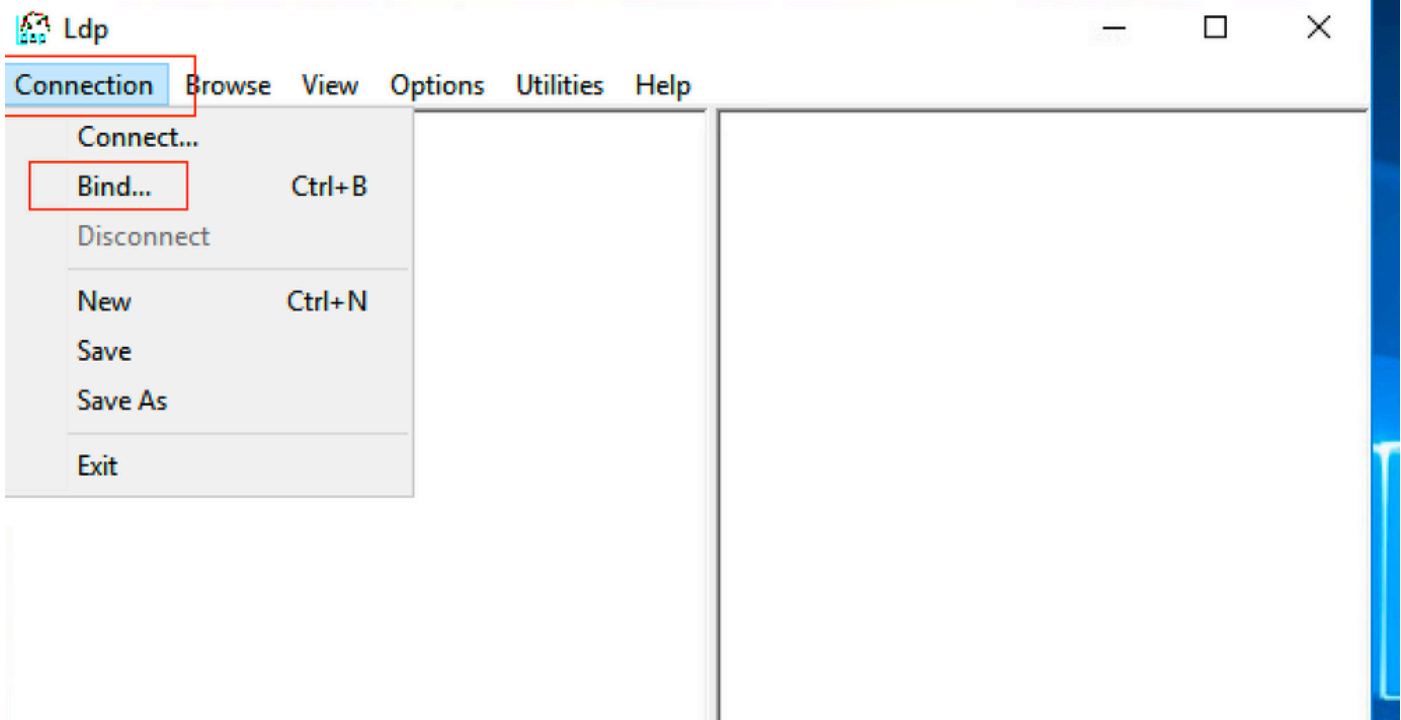
Idp

Run command



Idp





Idap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local

Connection Browse **View** Options Utilities Help

- Tree Ctrl+T
- Enterprise Configuration
- Status Bar
- Set Font...

```
POLICY_HINTS_DEPRECATED );
2.840.113556.1.4.2090 = ( DIRSYNC_EX );
2.840.113556.1.4.2205 = ( UPDATE_STATS
); 1.2.840.113556.1.4.2204 = (
TREE_DELETE_EX ); 1.2.840.113556.1.4.2206
= ( SEARCH_HINTS );
2.840.113556.1.4.2211 = (
EXPECTED_ENTRY_COUNT );
1.2.840.113556.1.4.2239 = ( POLICY_HINTS
); 1.2.840.113556.1.4.2255;
1.2.840.113556.1.4.2256;
1.2.840.113556.1.4.2309;
supportedLDAPPolicies (20): MaxPoolThreads;
MaxPercentDirSyncRequests;
MaxDatagramRecv; MaxReceiveBuffer;
InitRecvTimeout; MaxConnections;
MaxConnIdleTime; MaxPageSize;
MaxBatchReturnMessage;
```

Idap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local

Connection Browse View Options Utilities Help

```
POLICY_HINTS_DEPRECATED );
1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
1.2.840.113556.1.4.2205 = ( UPDATE_STATS
); 1.2.840.113556.1.4.2204 = (
TREE_DELETE_EX ); 1.2.840.113556.1.4.2206
= ( SEARCH_HINTS );
1.2.840.113556.1.4.2211 = (
EXPECTED_ENTRY_COUNT );
1.2.840.113556.1.4.2239 = ( POLICY_HINTS
); 1.2.840.113556.1.4.2255;
1.2.840.113556.1.4.2256;
1.2.840.113556.1.4.2309;
supportedLDAPPolicies (20): MaxPoolThreads;
MaxPercentDirSyncRequests;
```

Tree View

BaseDN:

```
MaxReceiveBuffer;
ns;
;
Duration;
SetSize;
erConn;
Range;
maxvarrange transitive, threadMemoryLimit;
SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
```

Connection Browse View Options Utilities Help

- DC=cciew,DC=local
- ... CN=Builtin,DC=cciew,DC=local
- ... CN=Computers,DC=cciew,DC=local
- ... OU=Domain Controllers,DC=cciew,DC=local
- ... CN=ForeignSecurityPrincipals,DC=cciew,DC=local
- ... CN=Infrastructure,DC=cciew,DC=local
- ... CN=Keys,DC=cciew,DC=local
- ... CN=LostAndFound,DC=cciew,DC=local
- ... CN=Managed Service Accounts,DC=cciew,DC=local
- ... CN=NTDS Quotas,DC=cciew,DC=local
- ... CN=Program Data,DC=cciew,DC=local
- ... CN=System,DC=cciew,DC=local
- ... CN=TPM Devices,DC=cciew,DC=local
- CN=Users,DC=cciew,DC=local**
- ... CN=Administrator,CN=Users,DC=cciew,DC=local
- ... CN=Allowed RODC Password Replication Group,CN=Users,DC=cciew,DC=local
- ... CN=Cert Publishers,CN=Users,DC=cciew,DC=local
- ... CN=Cloneable Domain Controllers,CN=Users,DC=cciew,DC=local
- ... CN=DefaultAccount,CN=Users,DC=cciew,DC=local
- ... CN=Denied RODC Password Replication Group,CN=Users,DC=cciew,DC=local
- ... CN=DnsAdmins,CN=Users,DC=cciew,DC=local
- ... CN=DnsUpdateProxy,CN=Users,DC=cciew,DC=local
- ... CN=Domain Admins,CN=Users,DC=cciew,DC=local
- ... CN=Domain Computers,CN=Users,DC=cciew,DC=local
- ... CN=Domain Controllers,CN=Users,DC=cciew,DC=local
- ... CN=Domain Guests,CN=Users,DC=cciew,DC=local
- ... CN=Domain Users,CN=Users,DC=cciew,DC=local
- ... CN=Enterprise Admins,CN=Users,DC=cciew,DC=local
- ... CN=Enterprise Key Admins,CN=Users,DC=cciew,DC=local
- ... CN=Enterprise Read-only Domain Controllers,CN=Users,DC=cciew,DC=local
- ... CN=Group Policy Creator Owners,CN=Users,DC=cciew,DC=local
- ... CN=Guest,CN=Users,DC=cciew,DC=local
- ... CN=kanu,CN=Users,DC=cciew,DC=local
- ... CN=Key Admins,CN=Users,DC=cciew,DC=local
- ... CN=krbtgt,CN=Users,DC=cciew,DC=local

```

adminCount: 1;
badPasswordTime: 0 (never);
badPwdCount: 0;
cn: vk1;
codePage: 0;
countryCode: 0;
displayName: vk1;
distinguishedName: CN=vk1,CN=Users,DC=cciew,DC=local;
dSCorePropagationData (2): 29-09-2021 15:16:40 India Standard Time; 0x0 = ( );
givenName: vk1;
instanceType: 0x4 = ( WRITE );
lastLogoff: 0 (never);
lastLogon: 0 (never);
logonCount: 0;
memberOf (4): CN=Domain Admins,CN=Users,DC=cciew,DC=local; CN=Enterprise Admins,CN=Users,DC=cciew,DC=local; CN=Schema Admins,CN=Users,DC=cciew,DC=local; CN=Administrators,CN=Builtin,DC=cciew,DC=local;
name: vk1;
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cciew,DC=local;
objectClass (4): top; person; organizationalPerson; user;
objectGUID: 1814f794-025e-4378-abad-66ff78a4a4d3;
objectSid: S-1-5-21-1375146846-274930181-3003521951-1120;
primaryGroupID: 513 = ( GROUP_RID_USERS );
pwdLastSet: 27-09-2021 22:56:11 India Standard Time;
sAMAccountName: vkokila;
sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
userAccountControl: 0x10200 = ( NORMAL_ACCOUNT | DONT_EXPIRE_PASSWORD );
userPassword: Cisco123;
userPrincipalName: vk1@cciew.local;
uSNChanged: 160181;
uSNCreated: 94284;
whenChanged: 29-09-2021 15:16:40 India Standard Time;
whenCreated: 25-12-2020 16:25:53 India Standard Time;
-----
Expanding base 'CN=Users,DC=cciew,DC=local'...
Getting 1 entries:
Dn: CN=Users,DC=cciew,DC=local
cn: Users;
description: Default container for upgraded user accounts;
distinguishedName: CN=Users,DC=cciew,DC=local;
dSCorePropagationData (2): 29-09-2019 01:09:51 India Standard Time; 0x1 = ( NEW_SD );
instanceType: 0x4 = ( WRITE );
isCriticalSystemObject: TRUE;
name: Users;
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=cciew,DC=local;

```

```

... CN=Users,DC=cciew,DC=local
... CN=Administrator,CN=Users,DC=cciew,DC=local
... CN=Allowed RODC Password Replication Group,CN=Users,DC=cciew,DC=local
... CN=Cert Publishers,CN=Users,DC=cciew,DC=local
... CN=Cloneable Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=DefaultAccount,CN=Users,DC=cciew,DC=local
... CN=Denied RODC Password Replication Group,CN=Users,DC=cciew,DC=local
... CN=DnsAdmins,CN=Users,DC=cciew,DC=local
... CN=DnsUpdateProxy,CN=Users,DC=cciew,DC=local
... CN=Domain Admins,CN=Users,DC=cciew,DC=local
... CN=Domain Computers,CN=Users,DC=cciew,DC=local
... CN=Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=Domain Guests,CN=Users,DC=cciew,DC=local
... CN=Domain Users,CN=Users,DC=cciew,DC=local
... CN=Enterprise Admins,CN=Users,DC=cciew,DC=local
... CN=Enterprise Key Admins,CN=Users,DC=cciew,DC=local
... CN=Enterprise Read-only Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=Group Policy Creator Owners,CN=Users,DC=cciew,DC=local
... CN=Guest,CN=Users,DC=cciew,DC=local
... CN=kanu,CN=Users,DC=cciew,DC=local
... CN=Key Admins,CN=Users,DC=cciew,DC=local
... CN=krbtgt,CN=Users,DC=cciew,DC=local
... CN=Protected Users,CN=Users,DC=cciew,DC=local
... CN=RAS and IAS Servers,CN=Users,DC=cciew,DC=local
... CN=Read-only Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=Schema Admins,CN=Users,DC=cciew,DC=local
... CN=sony s,CN=Users,DC=cciew,DC=local
... CN=tejas,CN=Users,DC=cciew,DC=local
... CN=test,CN=Users,DC=cciew,DC=local
... CN=test123,CN=Users,DC=cciew,DC=local
... CN=vk,CN=Users,DC=cciew,DC=local
... CN=vk1,CN=Users,DC=cciew,DC=local
... No children
... CN=Yogesh G.,CN=Users,DC=cciew,DC=local

```

```

showInAdvancedViewOnly: FALSE,
systemFlags: 0x8C000000 = ( DISALLOW_DELETE | DOMAIN_DISALLOW_REI
uSNChanged: 5888;
uSNCreated: 5888;
whenChanged: 29-09-2019 01:08:06 India Standard Time;
whenCreated: 29-09-2019 01:08:06 India Standard Time;

```

Expanding base 'CN=vk1,CN=Users,DC=cciew,DC=local'...
Getting 1 entries:

```

Dn: CN=vk1,CN=Users,DC=cciew,DC=local
  accountExpires: 9223372036854775807 (never);
  adminCount: 1;
  badPasswordTime: 0 (never);
  badPwdCount: 0;
  cn: vk1;
  codePage: 0;
  countryCode: 0;
  displayName: vk1;
  distinguishedName: CN=vk1,CN=Users,DC=cciew,DC=local;
  dScorePropagationData (2): 29-09-2021 15:16:40 India Standard Time; 0x0 =
  givenName: vk1;
  instanceType: 0x4 = ( WRITE );
  lastLogoff: 0 (never);
  lastLogon: 0 (never);
  logonCount: 0;
  memberOf (4): CN=Domain Admins,CN=Users,DC=cciew,DC=local; CN=Enterp
    Admins,CN=Users,DC=cciew,DC=local; CN=Administrators,CN=Builtin,DC=
    name: vk1;
  objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cciew,DC=loc
  objectClass (4): top; person; organizationalPerson; user;
  objectGUID: 1814f794-025e-4378-abad-66ff78a4a4d3;
  objectSid: S-1-5-21-1375146846-274930181-3003521951-1120;
  primaryGroupID: 513 = ( GROUP_RID_USERS );
  pwdLastSet: 27-09-2021 22:56:11 India Standard Time;
  sAMAccountName: vkokila;
  sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
  userAccountControl: 0x10200 = ( NORMAL_ACCOUNT | DONT_EXPIRE_PASS
  userPassword: Cisco123;
  userPrincipalName: vk1@cciew.local;
  uSNChanged: 160181;
  uSNCreated: 94284;
  whenChanged: 29-09-2021 15:16:40 India Standard Time;
  whenCreated: 25-12-2020 16:25:53 India Standard Time;

```

4. Verificar estatísticas do servidor e MAP de atributos

```
C9800-40-K9#show ldap server all
```

```
Server Information for ldap
```

```
=====
```

```

Server name           :ldap
Server Address        :10.106.38.195
Server listening Port :389
Bind Root-dn          :vk1
Server mode           :Non-Secure
Cipher Suite          :0x00
Authentication Seq    :Search first. Then Bind/Compare password next
Authentication Procedure:Bind with user password

```

Base-Dn :CN=users,DC=cciew,DC=local
Object Class :Person
Attribute map :VK
Request timeout :30
Deadtime in Mins :0
State :ALIVE

* LDAP STATISTICS *

Total messages [Sent:2, Received:3]
Response delay(ms) [Average:2, Maximum:2]
Total search [Request:1, ResultEntry:1, ResultDone:1]
Total bind [Request:1, Response:1]
Total extended [Request:0, Response:0]
Total compare [Request:0, Response:0]
Search [Success:1, Failures:0]
Bind [Success:1, Failures:0]
Missing attrs in Entry [0]
Connection [Closes:0, Aborts:0, Fails:0, Timeouts:0]

No. of active connections :0

Referências

[Exemplo de configuração de EAP local no 9800](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.