802.1X 및 웹 인증을 위한 LDAP 인증을 사용하여 Catalyst 9800 WLC 구성

목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 Webauth SSID로 LDAP 구성 네트워크 다이어그램 컨트롤러 구성 dot1x SSID로 LDAP 구성(로컬 EAP 사용) LDAP 서버 세부사항 이해 9800 웹 UI의 필드 이해 sAMAaccountName 특성을 사용하는 LDAP 802.1x 인증 WLC 구성: 웹 인터페이스에서 확인: 다음을 확인합니다. 문제 해결 컨트롤러에서 인증 프로세스를 확인하는 방법 9800에서 LDAP 연결을 확인하는 방법 참조

소개

이 문서에서는 LDAP 서버를 사용자 자격 증명용 데이터베이스로 사용하여 클라이언트를 인증하도 록 Catalyst 9800을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Microsoft Windows 서버
- Active Directory 또는 기타 LDAP 데이터베이스

사용되는 구성 요소

Cisco IOS®-XE 버전 17.3.2a를 실행하는 C9100 AP(액세스 포인트)의 C9800 EWC

LDAP 데이터베이스 역할을 하는 QNAP NAS(Network Access Storage)가 포함된 Microsoft AD(Active Directory) 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Webauth SSID로 LDAP 구성

네트워크 다이어그램

이 기사는 매우 간단한 설정을 기반으로 작성되었습니다.

IP 192.168.1.15가 포함된 EWC AP 9115

IP 192.168.1.192를 사용하는 Active Directory 서버

EWC의 내부 AP에 연결하는 클라이언트

컨트롤러 구성

1단계. LDAP 서버 구성

Configuration(컨피그레이션) > Security(보안) > AAA> Servers/Groups(서버/그룹) > LDAP로 이동 하고 + Add(추가)를 클릭합니다

¢	cisco	Cisco Embe	edded Wireless	Controller	on Cata	alyst Acc	ess Poin	ts
Q	Search Menu Iter	ms	Configuration - >	Security - >	AAA			
	Dashboard		+ AAA Wizard					
	Monitoring	>	Servers / Groups	AAA Meth	od List	AAA Adva	anced	
Z)	Configuration	>	+ Add	× Delete				
ক্ট্য	Administratior	א ו	RADIUS				Servers	Server Groups
Ô	Licensing		TACACS+					Namo
×	Troubleshooti	ng	LDAP					NAS

LDAP 서버의 이름을 선택하고 세부 정보를 입력합니다. 각 필드에 대한 설명은 이 문서의 "LDAP 서버 세부사항 이해" 섹션을 참조하십시오.

Edit AAA LDAP Server

Server Name*	AD]	
Server Address*	192.168.1.192	< ! Provid	le a valid Server
Port Number*	389	audiess	
Simple Bind	Authenticated 🗸)	
Bind User name*	Administrator@lab.cor]	
Bind Password *	•]	
Confirm Bind Password*	•]	
User Base DN*	CN=Users,DC=lab,DC]	
User Attribute	▼)	
User Object Type		+	
	User Object Type	∨]	Remove
	Person		×
Server Timeout (seconds)	0-65534]	
Secure Mode			
Trustpoint Name)	

Update and apply to device(업데이트 및 디바이스에 적용)를 클릭하여 저장합니다.

CLI 명령:

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

2단계. LDAP 서버 그룹을 구성합니다.

Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > LDAP > Server Groups(서버 그룹)로 이동하고 +ADD(추가)를 클릭합니다

+ AAA Wizard		
Servers / Groups AAA Method Lis	st AAA Advanced	
+ Add × Delete		
RADIUS	rvers Server Groups	
TACACS+		
LDAP	Name	Server 1 Ser
	Idapgr	AD N/A
	I ■ ■ 1 ■ I I ▼ items p	er page

이름을 입력하고 이전 단계에서 구성한 LDAP 서버를 추가합니다.

Name*	Idapgr	
Group Type	LDAP	
Available Servers	Assigned Servers	
NAS	> AD	Ā
	<	~

>>

«

Update and apply(업데이트 및 적용)를 클릭하여 저장합니다.

CLI 명령:

aaa group server ldap ldapgr server AD 3단계. AAA 인증 방법 구성

Configuration(컨피그레이션) > Security(보안) > AAA > AAA method List(AAA 방법 목록) > Authentication(인증)으로 이동하고 +Add(추가)를 클릭합니다

Configuration	AAA					
+ AAA Wizard						
Servers / Groups AAA Metho	d List AAA Advance	d				
Authentication	→ Add × Dele	te				
Authorization						
Accounting	Name	✓ Туре	\sim	Group Type	¥.	Group1
Accounting	default	login		local		N/A
	ldapauth	login		group		ldapgr

이름을 입력하고 **로그인** 유형을 선택한 다음 이전에 구성된 LDAP 서버 그룹을 가리킵니다.

Quick Setup: AAA Authentication

Method List Name*	Idapauth	
Туре*	login v i	
Group Type	group 🔹	
Fallback to local		
Available Server Groups	Assigned Server Groups	
an a		

CLI 명령:

aaa authentication login ldapauth group ldapgr 4단계. AAA 권한 부여 방법 구성

Configuration(컨피그레이션) > Security(보안) > AAA > AAA method list(AAA 메서드 목록) > Authorization(권한 부여)으로 이동하고 +Add(추가)를 클릭합니다

Configuration - > Security - > AAA						
+ AAA Wizard						
Servers / Groups AAA Method List AAA Advar	nced					
Authentication	+ A	dd X Delete				
Authorization						
Accounting		Name v	Туре	Group Type	×	Group1
		default	credential-download	group		Idapgr
		Idapauth	credential-download	group		ldapgr
	н. н	1 ► ► 10 ¥ items per	page			

선택한 이름의 credential-download 유형 규칙을 생성하고 이전에 생성한 LDAP 서버 그룹을 가리 킵니다

Quick Setup: AAA Authoriza	tion
Method List Name*	Idapauth
Type*	credential-download 🔻 i
Group Type	group v i
Fallback to local	
Authenticated	
Available Server Groups	Assigned Server Groups
radius Idap tacacs+	Idapgr <

CLI 명령:

aaa authorization credential-download ldapauth group ldapgr 5단계. 로컬 인증 구성

Configuration(컨피그레이션) > Security(보안) > AAA > AAA Advanced(AAA 고급) > Global Config(전역 컨피그레이션)로 이동합니다.

로컬 인증 및 로컬 권한 부여를 **방법 목록**으로 설정하고 이전에 구성한 인증 및 권한 부여 방법을 선 택합니다.

+ AAA Wizard		
Servers / Groups AAA Method List	AA Advanced	
Global Config	Local Authentication	Method List 👻
RADIUS Fallback	Authentication Method List	Idapauth 🔻
Attribute List Name	Local Authorization	Method List
Device Authentication	Authorization Method List	Idapauth v
AP Policy	Radius Server Load Balance	DISABLED
Password Policy	Interim Update	
AAA Interface	Show Advanced Settings >>>	

CLI 명령:

Configuration - > Security - > AAA

aaa local authentication ldapauth authorization ldapauth 6단계. webauth 매개변수 맵을 구성합니다

Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고 전역 맵을 편집합 니다

Configuration	Security -> Web Auth
+ Add	
Par	rameter Map Name
glot	bal
⊨	▶ ▶ 10 🔻 items per page

192.0.2.1과 같은 가상 IPv4 주소를 구성해야 합니다(특정 IP/서브넷은 라우팅 불가 가상 IP에 예약 됨).

Edit Web Auth Parameter General Advanced global Parameter-map name Banner Type 💿 None 🔿 Banner Text 🔷 Banner Title 🔷 File Name 100 Maximum HTTP connections Init-State Timeout(secs) 120 Туре webauth v 192.0.2.1 Virtual IPv4 Address --- Select ---Trustpoint Ŧ Virtual IPv4 Hostname Virtual IPv6 Address XXXXXXXX Web Auth intercept HTTPs Watch List Enable 600 Watch List Expiry Timeout(secs) Captive Bypass Portal **Disable Success Window Disable Logout Window**

720

Apply(적용)를 클릭하여 저장합니다.

Sleeping Client Timeout (minutes)

Disable Cisco Logo

Sleeping Client Status

CLI 명령:

parameter-map type webauth global type webauth virtual-ip ipv4 192.0.2.1 7단계.webauth WLAN 구성

Configuration(컨피그레이션) > WLANs(WLAN)로 이동하고 +Add(추가)를 클릭합니다

Ed	it WLAN				
		A Changing	WLAN parameters while it	t is enabled will result in loss of connec	ctivity for clients connected to it.
(General	Security	Add To Policy Tags		
			A Please ad	d the WLANs to Policy Tags for them t	to broadcast.
	Profile	Name*	webauth	Radio Policy	All
	SSID*		webauth	Broadcast SSID	
WLAN ID*		ID*	2]	
	Status		ENABLED		

이름을 구성하고 활성화 상태인지 확인한 다음 보안 탭으로 이동합니다.

레이어 2 하위 탭에서 보안이 없으며 빠른 전환이 비활성화되어 있는지 확인합니다.

Edit WLAN					
	A Changi	ing WLAN paramet	ters while it is enabled will result ir	n loss of connectivity for clients conr	ected to it.
General	Security	Add To Poli	cy Tags		
Layer2	Layer3	ААА			
Layer 2 Se	curity Mode		None	Lobby Admin Access	
MAC Filter	ing			Fast Transition	Disabled 🔻
OWE Trans	sition Mode			Over the DS Reassociation Timeout	20

Layer**3 탭**에서 **웹 정책**을 활성화하고 매개변수 맵을 global로 설정하고 인증 목록을 이전에 구성한 aaa 로그인 방법으로 설정합니다.

Edit WLAN

A Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected					
General	Security	Add To	Policy Tags		
Layer2	Layer3	AAA			
Web Po	licy			Show Advanced Settings >>>	
Web Au	th Parameter	Мар	global v		
Authenti	cation List		Idapauth v		
For Loca the confi exists or	l Login Methoc guration 'aaa a the device	l List to work, uthorization r	please make sure network default local'		

Apply(적용)를 클릭하여 **저장합니다**

CLI 명령:

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 dotlx security web-auth security web-auth authentication-list ldapauth security web-auth parameter-map global no shutdown 8단계.SSID가 브로드캐스트되는지 확인합니다

Configuration(**컨피그레이션) > Tags(태그)**로 이동하고 SSID가 현재 SSID로 서비스하는 정책 프로 파일에 포함되어 있는지 확인합니다(아직 태그를 구성하지 않은 경우 새 새 컨피그레이션의 기본 정책 태그). 기본적으로 default-policy-tag는 수동으로 포함할 때까지 생성한 새 SSID를 브로드캐스 트하지 않습니다.

이 문서에서는 정책 프로필의 컨피그레이션을 다루지 않으며 컨피그레이션의 해당 부분에 대해 잘 알고 있다고 가정합니다.

dot1x SSID로 LDAP 구성(로컬 EAP 사용)

9800에서 802.1X SSID에 대한 LDAP를 구성하려면 일반적으로 로컬 EAP도 구성해야 합니다. RADIUS를 사용하는 경우 LDAP 데이터베이스와의 연결을 설정하는 RADIUS 서버이며 이 문서의 범위를 벗어납니다.이 구성을 시도하기 전에 먼저 WLC에 구성된 로컬 사용자로 로컬 EAP를 구성 하는 것이 좋습니다. 이 문서의 끝에 있는 참조 섹션에 구성 예가 나와 있습니다. 완료되면 사용자 데이터베이스를 LDAP로 이동할 수 있습니다.

1단계. 로컬 EAP 프로파일 구성

Configuration(컨피그레이션) > Local EAP(로컬 EAP)로 이동하고 +Add(추가)를 클릭합니다



프로필의 이름을 선택합니다. 적어도 PEAP를 활성화하고 신뢰 지점 이름을 선택합니다. 기본적으 로 WLC에는 자체 서명 인증서만 있으므로 어떤 인증서를 선택하든(일반적으로 TP-self-signedxxxx가 가장 적합한 것) 문제가 되지 않지만 새로운 스마트폰 OS 버전에서 자체 서명 인증서를 신 뢰하는 횟수가 줄어들기 때문에 신뢰할 수 있는 공개 서명 인증서 설치를 고려하십시오.

Edit Local EAP Profiles

Profile Name*	PEAP
LEAP	
EAP-FAST	
EAP-TLS	
PEAP	
Trustpoint Name	TP-self-signed-3059

Configuration(컨피그레이션) > Security(보안) > AAA> Servers/Groups(서버/그룹) > LDAP로 이동 하고 + Add(추가)를 클릭합니다

¢	cisco	Cisco Em 17.3.2a	bedded Wireles	s Controller o	n Catalyst Ad	ccess Poin	ts
Q	Search Menu Iter	ms	Configuration - >	Security - > A	AA		
	Dashboard		+ AAA Wizard	l			
	Monitoring	>	Servers / Groups	AAA Methoo	I List AAA Ad	dvanced	
2) 2	Configuration	>	+ Add	imes Delete			
ত্যি	Administratior	ı >	RADIUS			Servers	Server Groups
©	Licensing		TACACS+				Name
×	Troubleshooti	ing	LDAP				NAS

LDAP 서버의 이름을 선택하고 세부 정보를 입력합니다. 각 필드에 대한 설명은 이 문서의 "LDAP 서버 세부사항 이해" 섹션을 참조하십시오.

Edit AAA LDAP Server

Server Name*	AD		
Server Address*	192.168.1.192	< ! Provid	le a valid Server
Port Number*	389	audress	
Simple Bind	Authenticated v		
Bind User name*	Administrator@lab.cor		
Bind Password *	•		
Confirm Bind Password*	•		
User Base DN*	CN=Users,DC=lab,DC		
User Attribute	•		
User Object Type		+	
	User Object Type	~]	Remove
	Person		×
Server Timeout (seconds)	0-65534		
Secure Mode			
Trustpoint Name	•		

Update and apply to device(업데이트 및 디바이스에 적용)를 클릭하여 저장합니다.

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

3단계. LDAP 서버 그룹을 구성합니다.

Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > LDAP > Server Groups(서버 그룹)로 이동하고 +ADD(추가)를 클릭합니다

Configuration * > Security * :	AAA		
+ AAA Wizard			
Servers / Groups AAA Me	thod List AAA Advanced		
+ Add × Delete			
RADIUS	Servers Server Groups		
TACACS+			
LDAP	Name	Server 1	Ser
	ldapgr	AD	N/A
		10 🔻 items per page	

이름을 입력하고 이전 단계에서 구성한 LDAP 서버를 추가합니다.

Name*	ldapgr	
Group Type	LDAP	
Available Servers	Assigned Servers	
NAS	> AD	~

>>

«

Update and apply(업데이트 및 적용)를 클릭하여 저장합니다.

CLI 명령:

aaa group server ldap ldapgr server AD 4단계. AAA 인증 방법 구성

Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 방법 목록) > Authentication(인증)으로 이동하고 +Add(추가)를 클릭합니다

dot1x 유형 인증 방법을 구성하고 로컬로만 지정합니다. LDAP 서버 그룹을 가리키고 싶겠지만 여 기서 802.1X 인증자 역할을 하는 것은 WLC 자체입니다(사용자 데이터베이스가 LDAP에 있지만 권

한 부여 방법 작업).

Quick Setup: AAA Authentication					
Method List Name*	Idapauth				
Type*	dot1x	v (i)			
Group Type	local	v (i)			
Available Server Groups		Assigned Server Groups			
radius Idap tacacs+ Idapgr	> < >> «				

CLI 명령:

aaa authentication dot1x ldapauth local 5단계. AAA 권한 부여 방법 구성

Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여)으로 이동하고 +Add(+추가)를 클릭합니다

인증 방법의 credential-download 유형을 생성하고 LDAP 그룹을 가리키도록 합니다.

Quick Setup:	AAA Authori	ization
--------------	-------------	---------

Method List Name*	Idapauth	
Type*	credential-download v	
Group Type	group v i	
Fallback to local		
Authenticated		
Available Server Groups	Assigned Server Groups	
radius Idap tacacs+	Idapgr	

CLI 명령:

aaa authorization credential-download ldapauth group ldapgr 6단계. 로컬 인증 세부 정보 구성

Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > AAA advanced(AAA 고급)로 이동합니다

인증과 권한 부여를 모두 위해 Method List(방법 목록)를 선택하고 로컬로 가리키는 dot1x 인증 방법과 LDAP로 향하는 credential-download 권한 부여 방법을 선택합니다

Configuration - > Security - > AAA		
+ AAA Wizard		
Servers / Groups AAA Method List AAA Adva	nced	
Global Config	Local Authentication	Method List 🔹
RADIUS Fallback	Authentication Method List	Idapauth 🔻
Attribute List Name	Local Authorization	Method List v
Device Authentication	Authorization Method List	Idapauth 🔻
AP Policy	Radius Server Load Balance	DISABLED
Password Policy	Interim Update	
AAA Interface	Show Advanced Settings >>>	

CLI 명령:

aaa local authentication ldapauth authorization ldapauth 7단계. dot1x WLAN 구성

Configuration(컨피그레이션) > WLAN(WLAN)으로 이동하고 +Add(추가)를 클릭합니다

프로파일 및 SSID 이름을 선택하고 활성화되었는지 확인합니다.

Edit	WLAN				
		A Changing	g WLAN parameters while i	t is enabled will result in loss of connec	ctivity for clients connected to it.
Ge	neral	Security	Add To Policy Tags		
			A Please ad	ld the WLANs to Policy Tags for them t	to broadcast.
	Profile	Name*	LDAP	Radio Policy	All
	SSID*		LDAP	Broadcast SSID	
	WLAN	ID*	1]	
	Status				

레이어 2 보안 탭으로 이동합니다.

WPA+WPA2를 레이어 2 보안 모드로 선택

WPA 매개변수에서 WPA2 및 AES가 활성화되어 있는지 **확인하고 802.1X를 활성화합니다**

	A Changi	ng wLAN para	imeters while it is enabled will result	in loss of connectivity for clients con	inected to it.
General	Security	Add To F	Policy Tags		
Layer2	Layer3	ААА			
Layer 2 Se	ecurity Mode		WPA + WPA2 🔻	Lobby Admin Access	
MAC Filter	ing			Fast Transition	Adaptive Enab
Protecte	d Manageme	ent Frame		Over the DS	
				Reassociation Timeout	20
PMF			Disabled v	MPSK Configuration	
WPA Par	ameters			MPSK	
WPA Polic	y				
WPA2 Poli	icy				
GTK Rando	omize				
OSEN Poli	су				
WPA2 Enc	cryption		AES(CCMP128)		
			CCMP256		
			GCMP128		
			GOMP250		
Auth Key M	vigmt		✓ 802.1x		
			FT + 802.1x		
			FT + PSK		
			802.1x-SHA256		

AAA 하위 탭으로 이동합니다.

이전에 생성한 dot1x 인증 방법을 선택하고 로컬 EAP 인증을 활성화한 다음 첫 번째 단계에서 구성 된 EAP 프로파일을 선택합니다.

Edit WLAN			
	A Chang	jing WLAN pa	arameters while it is enabled will result in loss of connectivity for clients connected to it.
General	Security	Add To	Policy Tags
Layer2	Layer3	AAA	
Authentic	cation List		Idapauth v (i)
Local EA	P Authentica	tion	
EAP Prof	ile Name		PEAP v

Apply(적용)를 클릭하여 저장합니다.

CLI 명령:

wlan LDAP 1 LDAP local-auth PEAP security dot1x authentication-list ldapauth no shutdown 8단계.WLAN이 브로드캐스트되는지 확인합니다.

Configuration(**컨피그레이션) > Tags(태그)**로 이동하고 SSID가 현재 SSID로 서비스하는 정책 프로 파일에 포함되어 있는지 확인합니다(아직 태그를 구성하지 않은 경우 새 새 컨피그레이션의 기본 정책 태그). 기본적으로 default-policy-tag는 수동으로 포함할 때까지 생성한 새 SSID를 브로드캐스 트하지 않습니다.

이 문서에서는 정책 프로필의 컨피그레이션을 다루지 않으며 컨피그레이션의 해당 부분에 대해 잘 알고 있다고 가정합니다.

Active Directory를 사용하는 경우 "userPassword" 특성을 전송하도록 AD 서버를 구성해야 합니다. 이 특성을 WLC로 전송해야 합니다. AD 서버가 아닌 WLC가 검증을 하기 때문입니다. 비밀번호가 일반 텍스트로 전송되지 않으므로 LDAP 데이터베이스를 사용하여 확인할 수 없으므로 PEAPmschapv2 메서드로 인증하는 데 문제가 있을 수도 있습니다. PEAP-GTC 메서드만 특정 LDAP 데 이터베이스에서 작동합니다.

LDAP 서버 세부사항 이해

9800 웹 UI의 필드 이해

다음은 9800에 구성된 LDAP 서버로 작동하는 매우 기본적인 Active Directory의 예입니다

Edit AAA LDAP Server

Server Name*	AD]
Server Address*	192.168.1.192	Provide a valid Server address
Port Number*	389	aduress
Simple Bind	Authenticated v	
Bind User name*	Administrator@lab.cor	
Bind Password *	•]
Confirm Bind Password*	•]
User Base DN*	CN=Users,DC=lab,DC]
User Attribute	•	
User Object Type		+
	User Object Type	√] Remove
	Person	×
Server Timeout (seconds)	0-65534]
Secure Mode		
Trustpoint Name	•	

이름과 IP는 충분히 설명이 가능합니다.

포트: 389는 LDAP의 기본 포트이지만 서버에서 다른 포트를 사용할 수 있습니다.

단순 바인딩: 현재 인증되지 않은 바인드를 지원하는 LDAP 데이터베이스가 있는 경우는 매우 드뭅 니다(즉, 인증 양식 없이 누구나 LDAP 검색을 수행할 수 있습니다). 인증된 단순 바인딩은 가장 일 반적인 인증 유형이며 Active Directory에서 기본적으로 허용하는 것입니다. 관리자 계정 이름과 암 호를 입력하여 사용자 데이터베이스에서 검색할 수 있습니다.

바인드 사용자 이름: Active Directory에서 관리자 권한이 있는 사용자 이름을 가리켜야 합니다. AD는 "user@domain" 형식을 허용하지만 다른 많은 LDAP 데이터베이스에서는 사용자 이름에 "CN=xxx,DC=xxx" 형식을 사용합니다. AD가 아닌 다른 LDAP 데이터베이스의 예는 이 문서의 뒷부 분에 나와 있습니다.

바인딩 암호: 이전에 입력한 관리자 사용자 이름의 비밀번호를 입력합니다.

사용자 기본 DN: 여기에 검색이 시작되는 LDAP 트리의 위치인 "search root(검색 루트)"를 입력합 니다. 이 예에서는 LDAP 도메인의 예가 lab.com이므로 DN이 "CN=Users,DC=lab,DC=com"인 "Users" 그룹 아래에 모든 사용이 있습니다. 이 사용자 기본 DN을 찾는 방법의 예는 이 섹션의 뒷부 분에서 제공됩니다.

사용자 특성: 이는 비워둘 수도 있고 어떤 LDAP 필드가 LDAP 데이터베이스의 사용자 이름으로 간 주되는지를 나타내는 LDAP 특성 맵을 가리킬 수도 있습니다. 그러나 Cisco 버그 ID로 인해 <u>CSCv11813</u> 그러나 WLC는 CN 필드와의 인증을 시도합니다.

사용자 개체 유형: 이렇게 하면 사용자로 간주되는 객체의 유형이 결정됩니다. 일반적으로 이것은 "사람"입니다. AD 데이터베이스가 있고 컴퓨터 계정을 인증하면 "컴퓨터"일 수 있지만, LDAP에서 많은 사용자 지정을 제공합니다.

보안 모드에서는 Secure LDAP over TLS를 활성화하며 TLS 암호화에 인증서를 사용하려면 9800에서 신뢰 지점을 선택해야 합니다.

sAMAaccountName 특성을 사용하는 LDAP 802.1x 인증

이 개선 사항은 17.6.1 버전에 도입되었습니다.

사용자에 대해 "userPassword" 특성을 구성합니다.

1단계. Windows 서버에서 ActiveDirectory 사용자 및 컴퓨터로 이동합니다.

Active Directory Users and Computers

File Action View Help

NTDS Quotas
 TPM Devices

|= ⇒| 2 📰 📋 🗐 Q 🕞 🛛 🖬 🐍 🗽 🗑 🖉 🎘 Active Directory Users and Com Name Туре Description > 📔 Saved Queries Administrator User Built-in account for ad... ✓ iii cciew.local Allowed RO... Security Group... Members in this group c... > 📔 Builtin Cert Publish... Security Group... Members of this group ... > Computers 💐 Cloneable D... Security Group... Members of this group t... > 📓 Domain Controllers DefaultAcco... User A user account manage... > 📔 ForeignSecurityPrincipal: Roperational Content of the security Group... Members in this group c... > 🚞 Keys A DnsAdmins Security Group... DNS Administrators Gro... > 📔 LostAndFound > Managed Service Accourt > Program Data > 📔 System 📋 Users

	🚜 DnsUpdateP	Security Group	DNS clients who are per
	💐 Domain Ad	Security Group	Designated administrato
	💐 Domain Co	Security Group	All workstations and ser
	💐 Domain Con	Security Group	All domain controllers i
	💐 Domain Gue	Security Group	All domain guests
	💐 Domain Users	Security Group	All domain users
	💐 Enterprise A	Security Group	Designated administrato
	💐 Enterprise K	Security Group	Members of this group
	🗟 Enterprise R	Security Group	Members of this group
	KGroup Polic	Security Group	Members in this group c
	🛃 Guest	User	Built-in account for gue
	🛃 kanu	User	
	🧟 Key Admins	Security Group	Members of this group
	🛃 krbtgt	User	Key Distribution Center
	Reprotected Us	Security Group	Members of this group
	RAS and IAS	Security Group	Servers in this group can
	Read-only D	Security Group	Members of this group
	🧟 Schema Ad	Security Group	Designated administrato
	sony s	User	
	📥 tejas	User	
	🛃 test	User	
	stest123	User	
	k 🛃 🕺	User	
	& vk1	User	
	Synopesh G.	User	
L			

2단계. 해당 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다

> 🧮 Managed Service Accourt	🚜 DnsUpdate	Security Group	DNS clients who are per
> 📔 Program Data	💐 Domain Ad.	Security Group	Designated administrato
> 📔 System	💐 Domain Co.	Security Group	All workstations and ser
📔 Users	💐 Domain Cor	n Security Group	All domain controllers i
> 🧮 NTDS Quotas	💐 Domain Gu	e Security Group	All domain guests
> 🧮 TPM Devices	🚇 Dom 🖅 💷	C	All -1-main users
	at Enter	Сору	nated administrato
	💐 Enter	Add to a group	pers of this group
	A Enter	Name Mappings	pers of this group
	🖧 Grou	Disable Account	pers in this group c
	ᡖ Guest	Reset Password	in account for gue
	🛃 kanu	Maria	
	🧟 Key A	Nove	pers of this group
	🛃 krbtg	Open Home Page	istribution Center
	A Prote	Send Mail	pers of this group
	🚉 RAS a	All Tasks	s in this group can
	Read-		pers of this group
	A Scher	Cut	nated administrato
	🛃 sony	Delete	
	🛃 tejas	Rename	
	🖁 test		
	🖁 test12	Properties	
	🛃 vk	Help	
	& vk1	User	
	🛃 Yogesh G.	User	

3단계. 속성 창에서 속성 편집기를 선택합니다

/k1 Properties

Published C	ertifi	cates	Member Of	Pa	asswor	d Replica	tion	Dial-in	Object
Security		En	vironment		Sess	ions		Remote co	ontrol
General	Ad	dress	Account	P	rofile	Teleph	none	s Orga	nization
Remote	Des	ctop Se	rvices Profile		C	DM+		Attribute I	Editor

Attributes:

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



4단계. "userPassword" 특성을 구성합니다. 16진수 값으로 구성해야 하는 사용자의 비밀번호입니

다.

vk1 Properties

? X Published Certificates Member Of Password Replication Dial-in Object

Security	Environment	Sessi	ons	Remote control
G Ad	A	n	Televier	
Multi-value	d Octet String Edito	r		×
Attribute:	userPassword			
Values:				
				Add
				Remove
				Edit
		(ОК	Cancel

/k1 Properties

	1000
· · ·	~
	e 2

Published Certif	icates	Member Of	Password	Replication	Dial-in	Object
Security	En	vironment	Sessio	ns l	Remote co	ontrol
G-nord A	ddmaaa	Account	Desfile	Telephonee	0	nization
Multi-valu	ed Octe	et String Edito	or			\times
Octet String	Attribu	te Editor				×
Attribute:		userPassw	ord			_
Value format	:	Hexadecim	nal			~
Value:						
43 69 73	63 6I	7 31 32 33				^
				I		
						~
Clear				OK	Cance	el
			0	n l	Cancer	
	O	к с	ancel	Apply		Help

확인을 클릭하여 올바른 비밀번호가 표시되는지 확인합니다

v	k1	p	ro	pe	rti	es
w.	P. 1		10	P	1 61	

Security Fr	Member Ot	Password Replic	ation	Dial-in Remote co	Obje
Concert Address		Destile Telev		Correction Correction	
Multi-valued Octo	et String Edito	or			×
Attribute:	userPassword				
Values:					
Cisco 123			ר	Add	
				Remove	•
				Edit	
		ОК		Cancel	
0	K C	ancel A	noly		Haln

5단계. Apply(적용)를 클릭한 다음 OK(확인)를 클릭합니다

blished Co	ertificates	Member Of	F Passwo	ord Replica	ation	Dial-in	Object
Security	Er	nvironment	Sea	ssions	R	emote co	ontrol
ieneral	Address	Account	Profile	Telep	hones	Organ	nization
Remote	Desktop Se	ervices Profile	e I	COM+	A	ttribute E	ditor
Attributes:							
Attribute		Value					^
uid		<not se<="" td=""><td>t></td><td></td><td></td><td></td><td></td></not>	t>				
uidNumb	er	<not se<="" td=""><td>:t></td><td></td><td></td><td></td><td></td></not>	:t>				
unicodeP	wd	<not se<="" td=""><td>:t></td><td></td><td></td><td></td><td></td></not>	:t>				
unixHome	Directory	<not se<="" td=""><td>:t></td><td></td><td></td><td></td><td></td></not>	:t>				
unixUser	Password	<not se<="" td=""><td>:t></td><td></td><td></td><td></td><td></td></not>	:t>				
url							
		<not se<="" td=""><td>:t></td><td></td><td></td><td></td><td></td></not>	:t>				
userAcco	untControl	<not se<br="">0x1020</not>	:t>)0 = (NORI	MAL_ACC	OUNT	DONT_	J
userAcco userCert	ountControl	<not se<br="">0x1020 ≺not se</not>	et>)0 = (NORI et>	MAL_ACC	OUNT	DONT_)
userAcco userCert userCertif	ountControl	<not se<br="">0x1020 <not se<br=""><not se<="" td=""><td>et>)0 = (NOR et> et></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td>J</td></not></not></not>	et>)0 = (NOR et> et>	MAL_ACC	OUNT	DONT_	J
userAcco userCert userCertif userParar	ountControl icate meters	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<="" td=""><td>st>)0 = (NOR st> st> st></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td>J</td></not></not></not></not>	st>)0 = (NOR st> st> st>	MAL_ACC	OUNT	DONT_	J
userAcco userCert userCertif userParar userPass	ountControl licate meters word	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco1</not></not></not></not>	et>)0 = (NORI et> et> et> 23	MAL_ACC	OUNT	DONT_	J
userAcco userCerti userCertif userParar userPass userPKC	ountControl licate meters word \$12	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco11 <not se<="" td=""><td>et>)0 = (NORI et> et> et> 23 et></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not>	et>)0 = (NORI et> et> et> 23 et>	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userPass userPKC userPrinc	ountControl ficate meters word \$12 ipalName	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco11 <not se<br="">vk1@c</not></not></not></not></not>	et>)0 = (NORI et> et> et> 23 et> ciew.local	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userPass userPKC userPrinc userShare	icate meters word 512 ipalName edFolder	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco11 <not se<br="">vk1@c <not se<="" td=""><td>et>)0 = (NORI et> et> et> 23 et> sciew.local et></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not></not>	et>)0 = (NORI et> et> et> 23 et> sciew.local et>	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userPass userPKC userPrinc userShare <	icate meters word 512 ipalName edFolder	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco11 <not se<br="">vk1@c <not se<="" td=""><td>et>)0 = (NORI et> et> et> 23 et> cciew.local et></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not></not>	et>)0 = (NORI et> et> et> 23 et> cciew.local et>	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userPass userPKC: userPrinc userShare <	icate meters word \$12 ipalName edFolder	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco11 <not se<br="">vk1@c <not se<="" td=""><td>t>)0 = (NORI t> t> t> 23 t> ciew.local t></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not></not>	t>)0 = (NORI t> t> t> 23 t> ciew.local t>	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userPass userPKCS userPrinc userShan <	icate meters word S12 ipalName edFolder	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco11 <not se<br="">vk1@c <not se<="" td=""><td>t>)0 = (NORI t> t> t> 23 t> ciew.local t></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not></not>	t>)0 = (NORI t> t> t> 23 t> ciew.local t>	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userPass userPKC3 userPrinc userShare <	icate meters word S12 ipalName edFolder	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco11 <not se<br="">vk1@c <not se<="" td=""><td>et>)0 = (NORI et> et> et> 23 et> eciew.local et></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not></not>	et>)0 = (NORI et> et> et> 23 et> eciew.local et>	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userParar userPKCS userPrinc userShan < Edit	ountControl icate meters word S12 ipalName edFolder	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco12 <not se<br="">vk1@c <not se<="" td=""><td>t>)0 = (NORI t> t> t> 23 t> ciew.local t></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not></not>	t>)0 = (NORI t> t> t> 23 t> ciew.local t>	MAL_ACC	OUNT	DONT_	
userAcco userCertif userParar userParar userPKC3 userPrinc userShan < Edit	ountControl icate meters word S12 ipalName edFolder	<not se<br="">0x1020 <not se<br=""><not se<br=""><not se<br="">Cisco12 <not se<br="">vk1@c <not se<="" td=""><td>t>)0 = (NORI t> t> t> 23 t> ciew.local t></td><td>MAL_ACC</td><td>OUNT</td><td>DONT_</td><td></td></not></not></not></not></not></not>	t>)0 = (NORI t> t> t> 23 t> ciew.local t>	MAL_ACC	OUNT	DONT_	

6단계. 사용자에 대한 "sAMAccountName" 특성 값을 확인하고 인증을 위한 사용자 이름을 지정합 니다.

vk1 Properties

Published Certificates			Member Of	Pa	assword	tion	Dial-in Object				
Security	Security Environment				Sessions			Remote control			
General	Ad	dress	Account	P	Profile Telephone			s Organization			
Remote	rvices Profile		C	DM+	1	Attribute B	Editor				

Attributes:

secretary	<not set=""></not>	
securityIdentifier	<not set=""></not>	
seeAlso	<not set=""></not>	
serialNumber	<not set=""></not>	
servicePrincipalName	<not set=""></not>	
shadowExpire	<not set=""></not>	
shadowHag	<not set=""></not>	
shadowinactive	<not set=""></not>	
shadowLastChange	<not set=""></not>	
shadowMin	<not set=""></not>	~
<	Chor Ser>	>
Edit		Filter

WLC 구성:

?

1단계. LDAP 특성 맵 생성

2단계. "sAMAccountName" 특성을 구성하고 "username"으로 입력합니다.

3단계. LDAP 서버 컨피그레이션에서 생성된 특성 MAP을 선택합니다.

ldap attribute-map VK

map type sAMAccountName username

ldap server ldap

ipv4 10.106.38.195

attribute map VK

bind authenticate root-dn vkl password 7 00271A1507545A545C $\,$

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

search-filter user-object-type Person

웹 인터페이스에서 확인:

Cisco Catalyst 9800-2	10 Wireless Controller		Welcome adminnw	**	Search APs and Clients Q
Q Search Manu Items	n*> Security*> AAA				
Dashboard	ard				
Monitoring Monitoring	AAA Method List	AAA Advanced			
Configuration >					
C Licensing	Servers	Server Groups	Server Address	Port Number	Simple Bind
LDAP X Troubleshooting		ldap	10.106.38.195	389	Authenticated
		< 1 P P 10 V Items per	r page		1 - 1 of 1

	Last logiti	1975			
		Edit AAA LDAP Server			
		Server Name*	ldap		
AAA Advanced		Server Address*	10.106.38.195		
		Port Number*	389		
		Simple Bind	Authenticated 🔻		
Server Groups		Bind User name*	vk1		
ne T	Server Address	Bind Password *	•		
	10.106.38.195	Confirm Bind Password*	•		
1 F F 10 v items pe	er page	User Base DN*	CN=users,DC=cciew,DC		
		User Attribute	VK 🔹		
		User Object Type	+		
			User Object Type	T	Remove
			Person		×
		Sequer Timeout	20		
		(seconds)	30		

다음을 확인합니다.

컨피그레이션을 확인하려면 이 문서의 명령과 함께 CLI 명령을 다시 확인하십시오.

LDAP 데이터베이스는 일반적으로 인증 로그를 제공하지 않으므로 진행 상황을 알기 어려울 수 있 습니다. LDAP 데이터베이스에 대한 연결이 설정되어 있는지 확인하기 위해 추적 및 스니퍼 캡처를 수행하는 방법을 보려면 이 문서의 Troubleshoot(문제 해결) 섹션을 참조하십시오.

문제 해결

이 문제를 해결하려면 이를 두 부분으로 나누는 것이 좋습니다. 첫 번째 부분은 로컬 EAP 부분의 유 효성을 검사하는 것입니다. 두 번째는 9800이 LDAP 서버와 제대로 통신하는지 확인하는 것입니다.

컨트롤러에서 인증 프로세스를 확인하는 방법

클라이언트 연결의 "디버그"를 가져오기 위해 방사성 추적을 수집할 수 있습니다.

Troubleshooting(트러블슈팅) > Radioactive Trace(방사능 추적)로 이동합니다. 클라이언트 MAC 주 소를 추가하고(클라이언트가 자체 MAC이 아닌 임의의 MAC을 사용할 수 있다는 점에 유의하십시 오. 클라이언트 장치 자체의 SSID 프로파일에서 이를 확인할 수 있습니다) start를 누릅니다.

연결 시도를 재현한 후에는 "Generate(생성)"를 클릭하여 마지막 X분 동안의 로그를 얻을 수 있습니 다. 일부 LDAP 로그 **라인**이 표시되지 않으므로 internal을 클릭해야 합니다.

다음은 웹 인증 SSID에서 성공적으로 인증한 클라이언트의 무선 추적 예입니다. 명확성을 위해 일 부 불필요한 부품이 제거되었습니다. 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}: [dot11validate] [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 00000000000000000000021CA610D7 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-mgrfeat_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 000000000000000000C1CA610D7 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: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 (WNCD[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 (WNCD[0]) 2021/01/19 21:57:55.905157 {wncd_x_R0-0}{1}: [mmclient] [9347]: (debug): MAC: 2elf.3a65.9c09 Received mobile_announce_nak, sub_type: 1 of XID (0) from (WNCD[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: 0x9000006, 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-qosclient] [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}: [avcafc] [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 $\label{eq:loss_loss} 2021/01/19\ 21:57:55.962883\ \{wncd_x_R0-0\}\{1\}:\ [client-iplearn]\ [9347]:\ (note):\ MAC:$ 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::2clf: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}: [authmgr] [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: 2e1f.3a65.9c09 Dest MAC: 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}: [clientiplearn] [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}: [clientiplearn] [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[2elf.3a65.9c09][192.168.1.17]Retrieved useragent = 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): [2elf.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): [2elf.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): [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 21:58:00.996508 {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 21:58:00.996524 {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 21:58:05.808144 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:05.808226 {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 21:58:05.808251 {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 21:58:05.860465 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.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[2elf.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[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 21:58:05.860559 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]Retrieved useragent = 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[2elf.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[2elf.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[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/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[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 21:58:06.628832 {wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2elf.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): [2elf.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): [2elf.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): [2elf.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): [2elf.3a65.9c09:capwap_90000004] DC Profile-name has been changed to Samsung Galaxy Sl0e 2021/01/19 21:58:06.633231 {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 21:58:06.719502 {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 21:58:06.719521 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2elf.3a65.9c09][192.168.1.17]HTTP GET request 2021/01/19 21:58:06.719591 {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 21:58:06.719646 {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 21:58:06.720038 {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 useragent = 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-evg] [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): [2elf.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): [2elf.3a65.9c09:capwap_90000004] Received User-Name Nico for client 2elf.3a65.9c09 2021/01/19 21:58:16.375294 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2elf.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: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[2elf.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: 2elf.3a65.9c09 L3 Authentication Successful. ACL:[] 2021/01/19 21:58:16.378426 {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_DONE 2021/01/19 21:58:16.379181 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2elf.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: 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 21:58:16.379358 {wncd_x_R0-0}{1}: [ewlc-qosclient] [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 21:58:16.379442 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2elf.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: 2elf.3a65.9c09 2021/01/19 21:58:16.380729 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [Applied attribute :bsn-vlaninterface-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: 2elf.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: 2elf.3a65.9c09 2021/01/19 21:58:16.381152 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2elf.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: 2elf.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 2elf.3a65.9c09

9800에서 LDAP 연결을 확인하는 방법

LDAP로 향하는 트래픽을 확인하기 위해 9800에 내장된 캡처를 사용할 수 있습니다.

WLC에서 캡처를 가져오려면 Troubleshooting(문제 해결) > Packet Capture(**패킷 캡처)로 이동하고** +Add(추가)를 클릭합니다. 업링크 포트를 선택하고 캡처를 시작합니다.

¢	cisco Cisco C 17.3.2a	talyst 9800-CL Wireless Controller	
Q	Search Menu Items	Troubleshooting - > Packet Capture	
	Dashboard	+ Add × Delete	
	Monitoring	Capture V Name Interface	'
Ľ	Configuration	I⊲ ⊲ 0 ⊨ ⊨I 10 v items per page	
ঠ্য	Administration		
©	Licensing		
X	Troubleshooting		

다음은 사용자 Nico에 대한 성공 인증 **예입니다**

Idap						
D.	Time	Source	Destination	Protocol	Length La	Info
869	5 22:58:16.412748	192.168.1.15	192.168.1.192	LDAP	108	bindRequest(1) "Administrator@lab.com" simple
869	7 22:58:16.414425	192.168.1.192	192.168.1.15	LDAP	88	bindResponse(1) success
869	22:58:16.419645	192.168.1.15	192.168.1.192	LDAP	128	searchRequest(2) "CN=Users,DC=lab,DC=com" wholeSubtree
870	22:58:16.420536	192.168.1.192	192.168.1.15	LDAP	1260	<pre>searchResEntry(2) "CN=Nico,CN=Users,DC=lab,DC=com" searchResDone(2) success [1 result]</pre>
870	22:58:16.422383	192.168.1.15	192.168.1.192	LDAP	117	bindRequest(3) "CN=Nico,CN=Users,DC=lab,DC=com" simple
870	2 22:58:16.423513	192.168.1.192	192.168.1.15	LDAP	88	bindResponse(3) success

처음 2개의 패킷은 LDAP DB에 대한 WLC 바인딩을 나타냅니다. 즉, 검색을 수행하기 위해 admin 사용자로 데이터베이스에 인증하는 WLC입니다.

이 2개의 LDAP 패킷은 기본 DN(여기서 CN=Users,DC=lab,DC=com)에서 검색을 수행하는 WLC를 나타냅니다. 패킷의 내부에는 사용자 이름에 대한 필터가 포함되어 있습니다(여기서 "Nico"). LDAP 데이터베이스는 사용자 특성을 성공으로 반환합니다

마지막 2개의 패킷은 해당 사용자 비밀번호로 인증하려고 시도하는 WLC를 나타냅니다.

1. EPC를 수집하고 "sAMAccountName"이 필터로 적용되었는지 확인합니다.

			· — ·		
	55 16:23:25.359966 10.106.38.195	10.127.209.57	LDAP	bindResponse(1) success	1
	57 16:23:25.359966 10.127.209.57	10.106.38.195	LDAP	<pre>searchRequest(2) "CN=users,DC=cciew,DC=local" wholeSubtree</pre>	48
4	58 16:23:25.360973 10.106.38.195	10.127.209.57	LDAP	searchResEntry(2) "CN=vk1, CN=Users, DC=cciew, DC=local" searchResDone(2) success [2 resu	48
	247 16:23:40.117990 10.127.209.57	10.106.38.195	LDAP	bindRequest(1) "vk1" simple	1
	248 16:23:40.119988 10.106.38.195	10.127.209.57	LDAP	bindResponse(1) success	
1	250 16+22+40 1200R0 10 127 200 57	18 186 28 105	LDAD	coarchRequest(2) "CN-users DC-sciew DC-local" wholeSubtree	1
	Frame 57: 151 bytes on wire (1208 bits), 151 byt	es captured (1208 bits)			
	Ethernet II, Src: cc:7f:76:65:42:6b (cc:7f:76:65	:42:6b), Dst: Cisco_33:28:	ff (00:25:45:33:28:ff)		
	802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 263				
	Internet Protocol Version 4, Src: 10.127.209.57,	Dst: 10.106.38.195			
	Transmission Control Protocol, Src Port: 64371,	Dst Port: 389, Seq: 26, Ar	:k: 23, Len: 81		
5	Lightweight Directory Access Protocol				
	 LDAPMessage searchRequest(2) "CN=users,DC=cci 	ew,DC=local" wholeSubtree			
	messageID: 2				
	 protocolOp: searchRequest (3) 				
	v searchRequest				
	baseObject: CN=users,DC=cciew,DC=local	t			
	scope; wholeSubtree (2)				
	derefAliases: neverDerefAliases (0)				
	sizeLimit: 0				
	timeLimit: 0				
	typesOnly: False				
	 Filter: (sAMAccountName=vkokila) 				
	v filter; and (0)				
	v and: (sAMAccountName=vkokila)				
	v and: 1 item				
	✓ Filter: (sAMAccountName=vko	kila)			
	v and item: equalityMatch ((3)			
	<pre>v equalityMatch</pre>				
	attributeDesc: sAMAG	countName			
	assertionValue: vko	kila			

필터에 "cn"이 표시되고 "sAMAccountName"이 사용자 이름으로 사용 중인 경우 인증이 실패합니다

WLC cli에서 Idap 맵 특성을 다시 구성합니다.

2. 서버에서 일반 텍스트로 "userPassword"를 반환하지 않으면 인증이 실패합니다.

+	1197 16:25:05.708962 10.127.209.57	10.106.38.195	LDAP	searchRequest(3) "CN=users,DC=cciew,DC=local" wholeSubt	tree		
	1198 16:25:05.709954 10.106.38.195	10.127.209.57	LDAP	<pre>searchResEntry(3) "CN=vk1, CN=Users, DC=cciew, DC=local"</pre>	searchResDone(3) success	[2 res_	48
-	v PartialAttributeList item userPassword						-
	type: userPassword						
	vals: 1 item						7.1
	AttributeValue: Cisco123						
	 PartialAttributeList item givenName 						
	type: givenName						1
	<pre>v vals: 1 item</pre>						
	AttributeValue: vk1						
	 PartialAttributeList item distinguished 	lame					
	type: distinguishedName						
	vals: 1 item						
	AttributeValue: CN=vk1,CN=Users,DC	<pre>cciew,DC=local</pre>					
	 PartialAttributeList item instanceType 						
	type: instanceType						
	vals: 1 item						
	AttributeValue: 4						
	 PartialAttributeList item whenCreated 						
	type: whenCreated						

3. 서버에서 ldp.exe 도구를 사용하여 기본 DN 정보를 검증합니다.



🔝 Ldp		—	×
Connection Browse View	Options Utilities Help		
Connect			
Bind Ctrl+B			
New Carlo N			
New Ctri+iN Save			
Save As			
Exit			1
🚰 Ldp			×
Connection Browse View	Options Utilities Help		
	Bind X		
	User: administrator		
	Password:		
	Domain: CCIEW		
	Bind type		
	Bind as currently logged on user Bind with credentials		
	O Advanced (DIGEST)		
	Encrypt traffic after bind		
	Advanced Cancel OK		



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

Connection Browse View Options Utilities Help

DC=cciew,DC=local adminCount: 1; CN=Builtin,DC=cciew,DC=local CN=Computers,DC=cciew,DC=local OU=Domain Controllers, DC=cciew, DC=local CN=ForeignSecurityPrincipals,DC=cciew,DC=loca 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=lo 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=Administrator, CN=Users, DC=cciew, DC=le CN=Allowed RODC Password Replication Grou CN=Cert Publishers, CN=Users, DC=cciew, DC= CN=Cloneable Domain Controllers.CN=Users. CN=DefaultAccount, CN=Users, DC=cciew, DC= CN=Denied RODC Password Replication Group CN=DnsAdmins, CN=Users, DC=cciew, DC=loc CN=DnsUpdateProxy, CN=Users, DC=cciew, DC CN=Domain Admins, CN=Users, DC=cciew, DC CN=Domain Computers, CN=Users, DC=cciew, CN=Domain Controllers, CN=Users, DC=cciew, CN=Domain Guests, CN=Users, DC=cciew, DC= CN=Domain Users, CN=Users, DC=cciew, DC=I CN=Enterprise Admins, CN=Users, DC=cciew, D CN=Enterprise Key Admins, CN=Users, DC=ccie CN=Enterprise Read-only Domain Controllers, CN=Group Policy Creator Owners, CN=Users, D CN=Guest, CN=Users, DC=cciew, DC=local CN=kanu, CN=Users, DC=cciew, DC=local CN=Key Admins, CN=Users, DC=cciew, DC=loc CN=krbtgt,CN=Users,DC=cciew,DC=local

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-abed-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_PASSWD); 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 entri 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=lo CN=Allowed RODC Password Replication Grou CN=Cert Publishers, CN=Users, DC=cciew, DC=	snowinAdvancedviewOniy. 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;
 CN=Cloneable Domain Controllers, CN=Users, CN=DefaultAccount, CN=Users, DC=cciew, DC= CN=Denied RODC Password Replication Group CN=DnsAdmins, CN=Users, DC=cciew, DC= CN=DnsUpdateProxy, CN=Users, DC=cciew, DC CN=Domain Admins, CN=Users, DC=cciew, DC CN=Domain Computers, CN=Users, DC=cciew, CN=Domain Guests, CN=Users, DC=cciew, DC= CN=Domain Users, CN=Users, DC=cciew, DC= CN=Domain Users, CN=Users, DC=cciew, DC= CN=Enterprise Admins, CN=Users, DC=cciew, DC= CN=Enterprise Read-only Domain Controllers, CN=Group Policy Creator Owners, CN=Users, D CN=Guest, CN=Users, DC=cciew, DC=local CN=Key Admins, CN=Users, DC=cciew, DC=local CN=Key Admins, CN=Users, DC=cciew, DC=local CN=Krbtgt, CN=Users, DC=cciew, DC=local CN=RAS and IAS Servers, CN=Users, DC=cciew, DC= 	Expanding base 'CN=vk1,CN=Users,DC=cciew,DC=locaf 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); lastLogor: 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 objectGuID: 1814f794-025e-4378-abed-66ff78a4a4d3; objectSuID: 1814f794-025e-4378-abed-66ff78a4a4d3; objectSuID: 1814f794-025e-4378-abed-66ff78a4a4d3;
 CN=Read-only Domain Controllers, CN=Users, CN=Schema Admins, CN=Users, DC=cciew, DC CN=sony s, 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 	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. 서버 통계 및 특성 MAP 확인

C9800-40-K9#show ldap server all

Server Information for ldap

======		===	==	==	==	==	= =	=:	= =	=	=	=	=	=	=	=	
Server	nam	e							:	l	d	a	р				

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

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

참조

<u>9800 컨피그레이션의 로컬 EAP 예</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.