Configuration de l'intégration tierce ISE 2.0 avec Aruba Wireless

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Défis liés à l'assistance tierce
Sessions
Redirection d'URL
COA Solution our ISE
Solution sur 15E
<u>Cisco ISE</u>
Etape 1. Ajout d'un contrôleur sans fil Aruba aux périphériques réseau
Etape 2. Configurer le profil d'autorisation
Etape 3. Configurer les regies à autorisation
Point d'accès Aruba
Étape 1. Configuration du portail captif
Etape 2. Configuration du serveur RADIUS
Etape 3. Configuration SSID
Vérifier
Étape 1. Connexion au SSID mgarcarz aruba avec EAP-PEAP
Étape 2. Redirection du trafic du navigateur Web pour le BYOD
Etape 3. Exécution de Network Setup Assistant
Autres flux et assistance CoA
CWA avec CoA
Dépannage
Portail captif Aruba avec adresse IP au lieu du nom de domaine complet
Aruba Captive Portal - Politique d'accès incorrecte
Numéro de port Aruba CoA
Redirection sur certains périphériques Aruba
Informations connexes

Introduction

Ce document décrit comment dépanner la fonctionnalité d'intégration tierce sur Cisco Identity Services Engine (ISE).

Remarque : sachez que Cisco n'est pas responsable de la configuration ou de l'assistance des périphériques d'autres fournisseurs.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration Aruba IAP
- Flux BYOD sur ISE
- Configuration ISE pour l'authentification par mot de passe et certificat

Composants utilisés

Ce document décrit comment dépanner la fonctionnalité d'intégration tierce sur Cisco Identity Services Engine (ISE).

Il peut être utilisé comme guide pour l'intégration avec d'autres fournisseurs et flux. ISE version 2.0 prend en charge l'intégration tierce.

Il s'agit d'un exemple de configuration qui présente comment intégrer un réseau sans fil géré par Aruba IAP 204 avec ISE pour les services BYOD (Bring Your Own Device).

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

- Logiciel Aruba IAP 204 6.4.2.3
- Cisco ISE, version 2.0 et ultérieure

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Il existe deux réseaux sans fil gérés par Aruba AP.

Le premier (mgarcarz_byod) est utilisé pour l'accès EAP-PEAP (Extensible Authentication Protocol-Protected EAP) 802.1x.

Après une authentification réussie, le contrôleur Aruba doit rediriger l'utilisateur vers le flux NSP (Native Supplicant Provisioning) du portail ISE BYOD.

L'utilisateur est redirigé, l'application Network Setup Assistant (NSA) est exécutée et le certificat est provisionné et installé sur le client Windows.

L'autorité de certification interne ISE est utilisée pour ce processus (configuration par défaut).

NSA est également responsable de la création du profil sans fil pour le deuxième SSID (Service Set Identifier) géré par Aruba (mgarcarz_byod_tls), qui est utilisé pour l'authentification EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) 802.1x.

Par conséquent, l'utilisateur de l'entreprise peut intégrer son périphérique personnel et obtenir un accès sécurisé au réseau de l'entreprise.

Cet exemple peut être facilement modifié pour différents types d'accès, par exemple :

- · Authentification Web centralisée (CWA) avec service BYOD
- authentification 802.1x avec posture et redirection BYOD
- Généralement, pour l'authentification EAP-PEAP, Active Directory est utilisé (pour que cet

article soit court, des utilisateurs ISE internes sont utilisés)

 Généralement, pour le serveur SCEP (Simple Certificate Enrollment Protocol) externe de mise en service de certificats, généralement le service NDES (Network Device Enrollment Service) de Microsoft, afin de garder cet article court, l'autorité de certification ISE interne est utilisée.

Défis liés à l'assistance tierce

L'utilisation de flux d'invité ISE (tels que BYOD, CWA, NSP, Client Provisioning Portal (CPP)) avec des périphériques tiers pose des problèmes.

Sessions

Cisco Network Access Devices (NAD) utilise Radius cisco-av-pair appelé audit-session-id afin d'informer le serveur AAA (Authentication, Authorization, and Accounting) de l'ID de session.

Cette valeur est utilisée par ISE afin de suivre les sessions et de fournir les services corrects pour chaque flux. Les autres fournisseurs ne prennent pas en charge la paire cisco-av.

ISE doit s'appuyer sur les attributs IETF reçus dans la demande d'accès et la demande de comptabilisation.

Après réception de la demande d'accès, ISE crée un ID de session Cisco synthétisé (à partir de Calling-Station-ID, NAS-Port, NAS-IP-Address et shared secret). Cette valeur a une signification locale uniquement (non envoyée via le réseau).

Par conséquent, il est prévu que chaque flux (BYOD, CWA, NSP, CPP) associe les attributs corrects. ISE peut ainsi recalculer l'ID de session Cisco et effectuer une recherche afin de le mettre en corrélation avec la session correcte et de poursuivre le flux.

Redirection d'URL

ISE utilise Radius cisco-av-pair appelé url-redirect et url-redirect-acl afin d'informer NAD que le trafic spécifique doit être redirigé.

Les autres fournisseurs ne prennent pas en charge la paire cisco-av. En général, ces périphériques doivent donc être configurés avec une URL de redirection statique qui pointe vers un service spécifique (profil d'autorisation) sur ISE.

Une fois que l'utilisateur a initié une session HTTP, ces NAD redirigent vers l'URL et joignent également des arguments supplémentaires (comme l'adresse IP ou l'adresse MAC) afin de permettre à ISE d'identifier une session spécifique et de poursuivre le flux.

CoA

ISE utilise Radius cisco-av-pair appelé subscriber:command, subscriber:reauthenticate-type afin d'indiquer les actions que NAD doit entreprendre pour une session spécifique.

Les autres fournisseurs ne prennent pas en charge la paire cisco-av. En général, ces périphériques utilisent RFC CoA (3576 ou 5176) et l'un des deux messages définis :

- demande de déconnexion (également appelée paquet de déconnexion) : celle-ci est utilisée pour déconnecter la session (très souvent pour forcer la reconnexion)
- Push CoA : utilisé pour modifier l'état de la session de manière transparente sans déconnexion (par exemple, session VPN et nouvelle liste de contrôle d'accès appliquée)

ISE prend en charge Cisco CoA avec paire cisco-av, ainsi que RFC CoA 3576/5176.

Solution sur ISE

Afin de prendre en charge les fournisseurs tiers, ISE 2.0 a introduit un concept de profils de périphériques réseau qui décrit le comportement spécifique des fournisseurs - la prise en charge des sessions, de la redirection d'URL et de la CoA.

Les profils d'autorisation sont de type spécifique (profil de périphérique réseau) et, une fois l'authentification effectuée, le comportement ISE est dérivé de ce profil.

Par conséquent, les périphériques d'autres fournisseurs peuvent être gérés facilement par ISE. La configuration sur ISE est également flexible et permet d'ajuster ou de créer de nouveaux profils de périphériques réseau.

Cet article présente l'utilisation du profil par défaut pour le périphérique Aruba.

Plus d'informations sur la fonctionnalité :

Profils de périphériques d'accès réseau avec Cisco Identity Services Engine

Cisco ISE

Étape 1. Ajout d'un contrôleur sans fil Aruba aux périphériques réseau

Accédez à Administration > Network Resources > Network Devices. Choisissez le profil de périphérique correct pour le fournisseur sélectionné, dans ce cas : ArubaWireless. Assurez-vous de configurer le secret partagé et le port CoA, comme indiqué dans les images.

Network Devices List > aruba

Network Devices

		* Name	aruba		
		Description			
	* IP Addres	s: 10.62.148.118	/ 32		
		* Device Profile	ArubaWireless	• • •	
		Model Name			
		Software Version	•		
•	Network De	vice Group			
	Location	All Locations	Set To Defa	ult	
C	evice Type	All Device Types	Set To Defa	ult	
✓	▼ RADIUS	Authentication Settings			
		Enable Authe	entication Settings		
			Protocol	RADIUS	
			* Shared Secret	•••••	Show
			Enable KeyWrap	i)	
		* K	ey Encryption Key		Show
		* Message Authe	nticator Code Key		Show
			Key Input Format	ASCII HEXADEC	IMAL
			CoA Port	3799	Set To Default

Si aucun profil n'est disponible pour le fournisseur souhaité, vous pouvez le configurer sous Administration > Network Resources > Network Device Profiles.

Étape 2. Configurer le profil d'autorisation

Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles et sélectionnez le même profil de périphérique réseau qu'à l'étape 1. ArubaSans fil. Le profil configuré est Aruba-redirect-BYOD with BYOD Portal et comme illustré dans les images.

Authorization Profiles > A	ruba-redirect-BYOD
Authorization Prof	file
* Name	Aruba-redirect-BYOD
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	The Aruba Wireless V 🕀
▼ Common Tasks Web Redirection (Native Supplicant	CWA, MDM, NSP, CPP) Provisioning Value BYOD Portal (default)
▼ Advanced Attribute	es Settings
Select an item	
▼ Attributes Details	
Access Type = ACCES	SS_ACCEPT

Partie manquante de la configuration de redirection Web, où le lien statique vers le profil d'autorisation est généré. Bien qu'Aruba ne prenne pas en charge la redirection dynamique vers le portail invité, un lien est attribué à chaque profil d'autorisation, qui est ensuite configuré sur Aruba et comme illustré dans l'image.

▼ Common Tasks	
Native Supplicant Provisioning	Value BYOD Portal (default)
The network device profile selected above	requires the following redirect URL to be configured manually on the network access device in order to enforce web redirection:
https://iseHost:8443/portal/g?p=1	OlmawmklleZQhapEvlXPAoELx

Étape 3. Configurer les règles d'autorisation

Accédez à Policy > Authorization Rules et la configuration est comme indiqué dans l'image.

~	Basic_Authenticated_Access	if	Employee AND (EAP-TLS AND EndPoints:BYODRegistration EQUALS Yes)	then	PermitAccess
~	ArubaRedirect	if	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	then	Aruba-redirect-BYOD

Tout d'abord, l'utilisateur se connecte au SSID mgracarz_aruba et ISE renvoie le profil d'autorisation Aruba-redirect-BYOD qui redirige le client vers le portail BYOD par défaut. Une fois le processus BYOD terminé, le client se connecte à EAP-TLS et l'accès complet au réseau lui est accordé.

Dans les versions plus récentes d'ISE, la même stratégie peut ressembler à ce qui suit :

Fill Fill	ofiling Posture Client Provisio	oning + Polic	cy Elements							Click here to do visibility se	etup Do not show	this again.	×
Status	Policy Set Name	Descript	ion	Condi	itions					Allowed Pro	otocols / Serve	r Sequenc	e Hits
Search													
0	Aruba			ĥ	Aruba-Aruba-Essid-Nar	me EQUALS mgarcarz_	aruba			Default Net	work Access	× •	•
> Authenticatio	on Policy (1)												
> Authorization	Policy - Local Exceptions												
> Authorization	Policy - Global Exceptions												
	B // (0)												
 Authorization 	Policy (3)												
Autnorization	1 Policy (3)						Results						
+ Status	s Rule Name	Condit	ions				Results Profiles			Security Groups		Hits	Actions
Authonization Status Search	s Rule Name	Condit	ions				Results Profiles			Security Groups		Hits	Actions
Authonization Search	s Rule Name	Condit	ions	m∙ExternalGr	roups EQUALS example	.com/Builtin/Administrate	Results Profiles			Security Groups		Hits	Actions
Autonization Autonization Search	Rule Name Authorized	Condit	ions ه example.co کړ EndPoints-E	m-ExternalGr BYODRegistr	roups EQUALS example ration EQUALS Yes	o.com/Builtin/Administrate	Results Profiles		+	Security Groups		Hits	Actions
+ Status Search	Rule Name	Condit	ions example.co t: EndPoints-E Network Act	m∙ExternalGr BYODRegistr: cess-EapAutl	roups EQUALS example ation EQUALS Yes hentication EQUALS EA	p.com/Builtin/Administrate	Results Profiles		+	Security Groups	. +	Hits	Actions
Authonization Status Search O	Rule Name Authorized Redirect	Condit AND E:	example.co EndPoints-E Network Ac Aruba-Aruba-Essid-N	m-ExternalGr BYODRegistra cess-EapAuth lame EQUAL	roups EQUALS example ration EQUALS Yes hentication EQUALS EA LS mgarcarz_aruba	9.com/Builtin/Administrato	Results Profiles (* PermilAccess * Aruba_Redirect	(_BYOD)	+	Security Groups Select from list Select from list	• *	Hits	Actions ¢

Point d'accès Aruba

Étape 1. Configuration du portail captif

Afin de configurer le portail captif sur Aruba 204, naviguez vers Security > External Captive Portal et ajoutez un nouveau. Entrez ces informations pour une configuration correcte et comme indiqué dans l'image.

- Type : Authentification Radius
- IP ou nom d'hôte : serveur ISE
- URL : lien créé sur ISE dans la configuration du profil d'autorisation ; il est spécifique à un profil d'autorisation particulier et peut être trouvé ici dans la configuration de redirection Web

https://iseHost:8443/portal/g?p=10lmawmklleZQhapEvlXPAoELx									
The network device profile selected above req	uires the following redirect URL to be cor	nfigured manually on the network access device in order to enforce web redirection:							
Native Supplicant Provisioning	Value BYOD Portal (default)	v							

• Port : numéro de port sur lequel le portail sélectionné est hébergé sur ISE (par défaut : 8443), comme illustré dans l'image.

mgarcarz_ise20		
Туре:	Radius Authentication 💌	
IP or hostname:	mgarcarz-ise20.example.	
URL:	/portal/g?p=Kjr7eB7RrrLl	
Port:	8443	
Use https:	Enabled 💌	
Captive Portal failure:	Deny internet	
Automatic URL Whitelisting:	Disabled 💌	
Redirect URL:		(optional)
		OK Cancel

Étape 2. Configuration du serveur RADIUS

Naviguez jusqu'à Security > Authentication Servers pour vous assurer que le port CoA est le même que celui configuré sur ISE comme indiqué dans l'image.

Par défaut, sur Aruba 204, il est défini sur 5999, mais il n'est pas conforme à la RFC 5176 et ne fonctionne pas non plus avec ISE.

Security

uthentication Servers	Users for Interna	l Server	Roles	Blacklistin
Edit				
Name:	mgarcarz_ise20			
IP address:	10.48.17.235			
Auth port:	1812			
Accounting port:	1813			
Shared key:	••••			
Retype key:	••••			
Timeout:	5	sec.		
Retry count:	3			
RFC 3576:	Enabled 💌			
Air Group CoA port:	3799			
NAS IP address:	10.62.148.118	(optiona	l)	
NAS identifier:		(optiona	il)	
Dead time:	5	min.		
DRP IP:				
DRP Mask:				
DRP VLAN:				
DRP Gateway:				

Remarque : dans Aruba version 6.5 et plus récente, cochez également la case « Portail captif ».

Étape 3. Configuration SSID

• L'onglet Sécurité est tel qu'illustré dans l'image.

Ed	it mgarcarz_aruba							
1	WLAN Settings	2 VLAN	3 Security 4 Ac					
Se	curity Level							
1	lore	Key management:	WPA-2 Enterprise					
		Termination:	Disabled 🔹					
	- Enternice	Authentication server 1:	mgarcarz_ise20 👱 Edit					
	Enterprise	Authentication server 2:	Select Server 💌					
	Personal	Reauth interval:	0 hrs. 💌					
	Open	Authentication survivability:	Disabled 🔽					
		MAC authentication:	Perform MAC authentication before 802.1X					
L	ess	Accounting:	Use authentication servers					
S	ecure	Accounting interval:	0 min.					
		Blacklisting:	Disabled					
		Fast Roaming						
		Opportunistic Key Caching(OKC):	: 🗆					
		802.11r:						
		802.11k:						
		802.11V:						

 Onglet Access : sélectionnez Network-based Access Rule afin de configurer le portail captif sur SSID.

Utilisez le portail captif configuré à l'étape 1. Cliquez sur New, choisissez Rule type : Captive portal, Splash page type : External comme indiqué dans l'image.

1	WLAN Setting	ings		VLAN	3 Security	4	Access				
Ac	Access Rules										
More Control		Acce	ess Rules (3) nforce captive portal low any to all destinations								
	- Role-based		Allow TCP on ports 1-20000 on server 10.48.17.235								
	\ominus - Network-base	Edit Rule	e Enfo	orce captive portal	Splash page type:		Captive portal profile:				
- Unrestricted		Captive portal		al <u> </u>	External _		mgarcarz_ise20 🔽 Edit				
L	ess										

En outre, autoriser tout le trafic vers le serveur ISE (ports TCP dans la plage 1-20000), tandis que

la règle configurée par défaut sur Aruba : Allow any to all destinations semble ne pas fonctionner correctement comme indiqué dans l'image.

1 WLAN Settings			2 VLAN	3	Sec	curity		4 Access				mgarcarz_
Acc	cess Rules											
Mo Co	ore ntrol - Role-based		Access Rules (3) → Enforce captiv ● Allow any to a ● Allow TCP on p	e portal Il destinations ports 1-20000 on serve	er 10.48	3.17.235						
) - Network-base	rk-base Edit Rule Allow TCP on po Rule type:		orts 1-20000 on server 10.48.17.235 Service:			Action:		Destination:			
	- Unrestricted	Access	s control 🗾	Network		custom		Allow	-	to a particular server		•
Le	ess ntrol			Application Application catego Web category Web reputation	ory	Protocol: TCP Port(s): 1-20000				IP: 10.48.17.235		
		Options	5:	Log		Classify media		DSCP tag				
											ОК	Cancel

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Connexion au SSID mgarcarz_aruba avec EAP-PEAP

La première connexion d'authentification sur ISE apparaît. La stratégie d'authentification par défaut a été utilisée, le profil d'autorisation Aruba-redirect-BYOD a été renvoyé comme indiqué dans l'image.

cisco Identity Se	ervices Engine	Home	 Operations 	Policy	Guest Access	Administration	Work Centers			
RADIUS Livelog	TACACS Livelog	Reports	▶ Troubleshoot	Adaptive Netw	ork Control					
Mi	isconfigured Supplic 1	ants 🕡		Misconfigured Network Devices (i) O			RADIUS Drops ® 12			Client Stopped Respond O
📓 Show Live Sessions 🛛 🖗 Add or Remove Columns 🕶 🏀 Refresh 🛛 😮 Reset Repeat Counts										
Time	▼ Status All ▼ Det.	R. [dentity 🕐	Endpoint ID 🛞	Authenticat	ion Policy ()	Authorization Policy	Authorization Profiles	Network Device	Event ()
2015-10-29 22:2	23:37 🕦 🔒	0 0	isco C	0:4A:00:14:6E:3	1 Default >>	Dot1X >> EAP-TLS	Default >> Basic_Authenticated	PermitAccess		Session State is Started
2015-10-29 22:2	3:37 🗹 🛛	c	isco C	0:4A:00:14:6E:3	1 Default >>	Dot1X >> EAP-TLS	Default >> Basic_Authenticated	PermitAccess	aruba	Authentication succeeded
0015 10 00 00 1	0.00	0	isco (0:44:00:14:6E:3	Default >>	Dot1X >> Default	Default >> ArubaRedirect	Anuba-redirect-BVOD	aruba	Authentication succeeded

ISE renvoie un message d'acceptation d'accès Radius avec succès EAP. Notez qu'aucun attribut supplémentaire n'est renvoyé (pas de paire av Cisco url-redirect ou url-redirect-acl) comme indiqué dans l'image.

No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, l=307)	cisco	
136	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=103, l=193)		
137	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=104, l=344)	cisco	
138	10.48.17.235	10.62.148.118	RADIUS	267	Access-Challenge(11) (id=104, l=225)		
139	10.62.148.118	10.48.17.235	RADIUS	450	Access-Request(1) (id=105, l=408)	cisco	
140	10.48.17.235	10.62.148.118	RADIUS	283	Access-Challenge(11) (id=105, l=241)		
141	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=106, l=344)	cisco	
142	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=106, l=193)		
143	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=107, l=344)	cisco	
149	10.48.17.235	10.62.148.118	RADIUS	363	Access-Accept(2) (id=107, l=321)	cisco	
150	10.62.148.118	10.48.17.235	RADIUS	337	Accounting-Request(4) (id=108, l=295)	cisco	048D88888142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		
Pack	et identifier: Ox	-, 6b (107)					
Leng	th: 321						
Auth	enticator: 1173a3	d3ea3d0798fe30fdac	cf644f19				
Гтhi	s is a response t	o a request in fra	me 143]				
[Tim	ne from request: C	.038114000 seconds]				
⊽Attr	ibute Value Pairs		-				
D AV	P: l=7 t=User-Na	me(l): cisco					
⊳ AV	P: l=67 t=State(24): 52656175746853	3657373696f	6e3a3061	3330313165625862		
⊳ AV	P: l=87 t=Class(25): 434143533a306	13330313165	62586269	7544413379554e6f		
⊳ AV	P: l=6 t=EAP-Mes	sage(79) Last Segme	ent[1]				
Þ AV	P: l=18 t=Messag	e-Authenticator(80)	: e0b74092	cacf8880	3dcd37032b761513		
⊳ AV	P: l=58 t=Vendor	-Specific(26) v=Mid	crosoft(311)			
⊳ AV	P: l=58 t=Vendor	-Specific(26) v=Mid	crosoft(311)			

Aruba indique que la session est établie (l'identité EAP-PEAP est cisco) et que le rôle sélectionné est mgarcarz_aruba, comme indiqué dans l'image.



Ce rôle est responsable de la redirection vers la fonctionnalité ISE (portail captif sur Aruba).

Dans l'interface de ligne de commande d'Aruba, il est possible de confirmer l'état d'autorisation actuel de cette session :

IP	MAC	ACLs	Contract	Location	Age	Sessions	Flags	Vlan	FM
10.62.148.118	04:BD:88:C3:88:14	105/0	0/0	0	 1	0/65535	 Р		 N
1010211101110	0110010010010111	100/0	0,0	Ū	-	0,00000	•	-	
10.62.148.71	C0:4A:00:14:6E:31	138/0	0/0	0	0	6/65535		1	в
0.0.0.0	C0:4A:00:14:6E:31	138/0	0/0	0	0	0/65535	Р	1	В
172.31.98.1	04:BD:88:C3:88:14	105/0	0/0	0	1	0/65535	Р	3333	В
0.0.0.0	04:BD:88:C3:88:14	105/0	0/0	0	0	0/65535	Р	1	Ν
04:bd:88:c3:88:	14#								

Et afin de vérifier l'ID ACL 138 pour les autorisations actuelles :

<#root>

04:bd:88:c3:88:14#

show datapath acl 138

Datapath ACL 138 Entries _____ Flags: P - permit, L - log, E - established, M/e - MAC/etype filter S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6 K - App Throttle, d - Domain DA _____ 1: any any 17 0-65535 8209-8211 P4 2: any 172.31.98.1 255.255.255 6 0-65535 80-80 PSD4 3: any 172.31.98.1 255.255.255 6 0-65535 443-443 PSD4 4: any mgarcarz-ise20.example.com 6 0-65535 80-80 Pd4 5: any mgarcarz-ise20.example.com 6 0-65535 443-443 Pd4 6: any mgarcarz-ise20.example.com 6 0-65535 8443-8443 Pd4 hits 37 7: any 10.48.17.235 255.255.255.255 6 0-65535 1-20000 P4 hits 18 <....some output removed for clarity ... >

Cela correspond à ce qui a été configuré dans l'interface utilisateur graphique pour ce rôle, comme illustré dans l'image.

Security								
Authentication Servers Users for I	nternal Server R	toles	Blacklisting	Firewall Settings	Inbound Firewall	Walled Garde	n	
Roles	Access Rules for	mgai	rcarz_aruba					
default_wired_port_profile → Enforce captive portal wired-instant → Allow any to all destinations ArubaAAA → Allow TCP on ports 1-20000 on server 10.48.17.235 wcecot_BYOD_aruba → Minow TCP on ports 1-20000 on server 10.48.17.235								
New Delete	New Edit D)elete						

Étape 2. Redirection du trafic du navigateur Web pour le BYOD

Une fois que l'utilisateur a ouvert le navigateur Web et saisi une adresse, la redirection s'effectue comme indiqué dans l'image.



En examinant les captures de paquets, il est confirmé qu'Aruba usurpe la destination (5.5.5.5) et renvoie la redirection HTTP vers ISE.

Notez qu'il s'agit de la même URL statique que celle configurée dans ISE et copiée sur Captive Portal sur Aruba, mais que plusieurs arguments supplémentaires sont ajoutés comme suit et comme illustré dans l'image :

- cmd = connexion
- mac = c0:4a:00:14:6e:31
- essid = mgarcarz_aruba
- ip = 10.62.148.7
- apname = 4bd88c38814 (mac)
- url = <u>http://5.5.5.5</u>

📕 *W	ireless Network Connection	[Wireshark 1.10.3 (SVN Rev 53	022 from /trur	ık-1.10)]	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics Telepho	ny <u>T</u> ools <u>I</u>	Internals <u>H</u> elp	
0 0) 🧵 🔳 🙇 🖻 🛅	🗶 🔁 🔍 🗢 🔿 🗳) 7 L	E 🗐 Q, Q, Q, 🗹 🗸 🛛 🥵 % 🕱	
Filter:	http			Expression Clear Apply Save	
No.	Source	Destination	Protocol L	ength Info	
7	24 10.62.148.71	5.5.5.5	HTTP	335 GET / HTTP/1.1	
7	26 5.5.5.5	10.62.148.71	HTTP	498 HTTP/1.1 302	
7	52 10.62.148.71	23.62.99.25	HTTP	151 GET /ncsi.txt HTTP/1.1	
1	55 23.62.99.25	10.62.148.71	нттр	515 HTTP/1.1 302	
 Fra Eth Int Tra Hyp 	ame 726: 498 bytes o nernet II, Src: 04:b ernet Protocol Vers ansmission Control P pertext Transfer Pro	n wire (3984 bits), d:88:c3:88:14 (04:bo ion 4, src: 5.5.5.5 protocol, src Port: P ptocol	498 bytes :88:c3:88 (5.5.5.5) ttp (80),	captured (3984 bits) on interface 0 114), Dst: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31) , Dst: 10.62.148.71 (10.62.148.71) Dst Port: 53939 (53939), Seq: 1, Ack: 282, Len: 444	<u> </u>
± F	HTTP/1.1 302\r\n				E
S	Server:\r\n				
0	Date: Thu, 01 Jan 19	070 05:36:56 GMT\r\n			
	ache-Control: no-ca	iche,no-store,must-re	validate,	post-check=0,pre-check=0\r\n	
	[truncated] Location	nttps://mgarcarz-1	se20.exam	ipie.com:8443/portal/g?p=10imawmkile2QnapEvixPAOELx&cmd=log1n&m	ac=c0:4a:0
1	r\n				
ſ	HTTP response 1/1]				-
•		III			P.
00b0 00c0 00d0 00f0 0100 0110 0120 0130 0140 0150 0160 0170	70 72 65 2d 63 68 61 74 69 6f 6a 3a 67 61 72 63 61 72 63 61 72 61 61 72 63 61 72 63 61 72 64 65 2e 67 72 74 61 62 2f 63 63 30 3a 65 5a 63 61 63 30 3a 31 26 63 61 72 74 61 62 74 61 62 74 61 62 74 61 62 74 61 63 30 3a 33 31 26 63 33 31 26 61 72 74 61 61 72 73 57 61 72 33 31 34 38 30 34 25 33 41 38 <td>65 63 6b 3d 30 0d 0 20 68 74 74 70 73 2 69 73 65 32 3 7a 2d 69 73 65 32 3 67 36 61 38 34 3 67 3f 70 3d 31 4f 6 6 6 38 34 3 67 3f 70 3d 31 4f 6 6 6 38 38 34 3 66 64 3d 36 67 6 34 66 66 64 34 66 76 6 34 61 3a 30 30 3a 30 3a 37 73 69 64 3d 66 70 3 2e 37 31 26 61 70 62 64 25 33<td>a 4c 6f 6 a 2f 2f 6 0 2e 65 7 4 33 2f 7 c 6d 61 7 c 58 50 4 9 6e 26 6 1 34 3a 3 7 61 72 6 d 31 30 2 e 61 6d 6 8 25 33 4</td><td><pre>3 pre-chec k=0Loc d ation: h ttps://m 8 garcarz- ise20.ex 0 ample.co m:8443/p 7 ortal/g? p=101maw 1 mklleZQh apEvlXPA d oELx&cmd =login&m 6 ac=c0:4a :00:14:6 3 e:31&ess id=mgarc e arz_arub a&ip=10. 5 62.148.7 1&apname 1 =04%3Abd %3A88%3A</pre></td><td></td></td>	65 63 6b 3d 30 0d 0 20 68 74 74 70 73 2 69 73 65 32 3 7a 2d 69 73 65 32 3 67 36 61 38 34 3 67 3f 70 3d 31 4f 6 6 6 38 34 3 67 3f 70 3d 31 4f 6 6 6 38 38 34 3 66 64 3d 36 67 6 34 66 66 64 34 66 76 6 34 61 3a 30 30 3a 30 3a 37 73 69 64 3d 66 70 3 2e 37 31 26 61 70 62 64 25 33 <td>a 4c 6f 6 a 2f 2f 6 0 2e 65 7 4 33 2f 7 c 6d 61 7 c 58 50 4 9 6e 26 6 1 34 3a 3 7 61 72 6 d 31 30 2 e 61 6d 6 8 25 33 4</td> <td><pre>3 pre-chec k=0Loc d ation: h ttps://m 8 garcarz- ise20.ex 0 ample.co m:8443/p 7 ortal/g? p=101maw 1 mklleZQh apEvlXPA d oELx&cmd =login&m 6 ac=c0:4a :00:14:6 3 e:31&ess id=mgarc e arz_arub a&ip=10. 5 62.148.7 1&apname 1 =04%3Abd %3A88%3A</pre></td> <td></td>	a 4c 6f 6 a 2f 2f 6 0 2e 65 7 4 33 2f 7 c 6d 61 7 c 58 50 4 9 6e 26 6 1 34 3a 3 7 61 72 6 d 31 30 2 e 61 6d 6 8 25 33 4	<pre>3 pre-chec k=0Loc d ation: h ttps://m 8 garcarz- ise20.ex 0 ample.co m:8443/p 7 ortal/g? p=101maw 1 mklleZQh apEvlXPA d oELx&cmd =login&m 6 ac=c0:4a :00:14:6 3 e:31&ess id=mgarc e arz_arub a&ip=10. 5 62.148.7 1&apname 1 =04%3Abd %3A88%3A</pre>	
0170 0180 0190 01a0 01b0 01c0 01d0 01e0 01f0	05 35 25 35 41 38 61 6d 65 36 69 6e 41 38 38 25 33 41 70 38 38 25 33 41 70 38 38 25 33 41 70 38 38 25 33 41 70 38 38 25 33 41 70 38 38 25 33 41 70 38 38 25 33 41 70 30 73 65 63 74 75 72 62 35 26 35 6e 65 63 74 69 67 70d 0a 74 69 67	36 23 33 41 31 34 24 31 34 26 73 74 61 6e 74 20 4 31 34 26 73 77 69 7 72 65 6c 6f 67 69 7 72 65 6c 6f 67 69 7 74 70 25 32 41 25 3 74 70 25 32 46 0d 0 2e 35 25 32 46 0d 0 6e 3a 20 63 6c 6f 7	0 76 63 63 3 33 25 3 4 63 68 6 e 2e 61 7 3 6f 6d 2 2 46 25 3 a 43 6f 6 3 65 0d 0	a me=inst ant-C3%3 9 A88%3A14 &switchi 2 p=secure login.ar 6 ubanetwo rks.com& 2 url=http %3A%2F%2 e F5.5.5.5 %2FCon a nection: close	

Grâce à ces arguments, ISE peut recréer l'ID de session Cisco, trouver la session correspondante sur ISE et continuer avec le flux BYOD (ou tout autre flux configuré).

Pour les périphériques Cisco, audit_session_id serait normalement utilisé, mais cela n'est pas pris en charge par d'autres fournisseurs.

Afin de confirmer qu'à partir des débogages ISE, il est possible de voir la génération de la valeur audit-session-id (qui n'est jamais envoyée sur le réseau) :

<#root>

AcsLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID= c04a00146e31,FramedIPAddress=10.62.148.71,MessageFormatter::appendValue() attrName: cisco-av-pair appending value:

audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M

Et ensuite, corrélation de cela après l'enregistrement de l'appareil sur le BYOD Page 2 :

<#root>

AcsLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID= c04a00146e31,FramedIPAddress=10.62.148.71,Log_Message=[2015-10-29 23:25:48.533 +01:00 0000011874 88010 INF0

```
(endpoint), ConfigVersionId=145, UserName=cisco, MacAddress=c0:4a:00:14:6e:31,
IpAddress=10.62.148.71, AuthenticationIdentityStore=Internal Users,
PortalName=BYOD Portal (default), PsnHostName=mgarcarz-ise20.example.com,
GuestUserName=cisco, EPMacAddress=C0:4A:00:14:6E:31, EPIdentityGroup=RegisteredDevices
Staticassignment=true, EndPointProfiler=mgarcarz-ise20.example.com, EndPointPolicy=
Unknown, NADAddress=10.62.148.118, DeviceName=ttt, DeviceRegistrationStatus=Registered
AuditSessionId=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7G1HXj1M,
cisco-av-pair=
```

```
audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M
```

MyDevices: Successfully registered/provisioned the device

Dans les demandes suivantes, le client est redirigé vers la page 3 du BYOD, où NSA est téléchargé et exécuté.



Étape 3. Exécution de Network Setup Assistant

NSA a la même tâche que le navigateur Web. Tout d'abord, il doit détecter l'adresse IP d'ISE. Cela est possible via la redirection HTTP.

Étant donné que cette fois l'utilisateur n'a pas la possibilité de taper une adresse IP (comme dans le navigateur Web), ce trafic est généré automatiquement.

La passerelle par défaut est utilisée (également enroll.cisco.com peut être utilisé) comme indiqué dans l'image.

*Wireless Network Connection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]								
<u>File Edit View Go Capture Analyze Statistics Telephony</u> <u>T</u> ools <u>I</u> nternals <u>H</u> elp								
◉ ◉ ∡ ■ ∅ ⊏ Ё ೫ ₴ ९ ᆃ ⇔ ݷ ₮ ⊻ ◻(ᆿ) ୧ ୧ ୯ ୯ ₩ ⊠ № % छ								
Filter: http Expression Clear Apply Save								
No. Source Destination Protocol Length Info								
182 10.62.148.71 10.62.148.100 HTTP 223 GET /auth/discovery HTTP/1.1								
184 10.62.148.100 10.62.148.71 HTTP 520 HTTP/1.1 302								
Frame 182: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface 0 Ethernet II, Src: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31), Dst: Cisco_f2:b1:42 (c4:0a:cb:f2:b1:42) Internet Protocol Version 4, Src: 10.62.148.71 (10.62.148.71), Dst: 10.62.148.100 (10.62.148.100) Transmission Control Protocol, Src Port: 55937 (55937), Dst Port: http (80), Seq: 1, Ack: 1, Len: 169 Hypertext Transfer Protocol GET /auth/discovery HTTP/1.1\r\n User-Agent: Mozilla/4.0 (windows NT 6.1; compatible; Cisco NAC Web Agent v.)\r\n								
Accept: */*\r\n								
HOST: 10.62.148.100\r\n								
Cache-Control: no-cache\r\n \n\n								
\LVU [Eu]] request UPT: http://10.62.148.100/auth/discoverv]								
[HTTP request 1/1]								
[Response in frame: 184]								

La réponse est exactement la même que pour le navigateur Web.

De cette façon, NSA peut se connecter à ISE, obtenir un profil xml avec configuration, générer une requête SCEP, l'envoyer à ISE, obtenir un certificat signé (signé par l'autorité de certification interne ISE), configurer le profil sans fil et enfin se connecter au SSID configuré.

Collecter les journaux du client (sous Windows, ils se trouvent dans %temp%/spwProfile.log). Certains résultats sont omis pour des raisons de clarté :

<#root>

```
Logging started

SPW Version: 1.0.0.46

System locale is [en]

Loading messages for english...

Initializing profile

SPW is running as High integrity Process - 12288

GetProfilePath: searched path = C:\Users\ADMINI~1.EXA\AppData\Local\Temp\ for file name = spwProfile.xm

GetProfilePath: searched path = C:\Users\ADMINI~1.EXA\AppData\Local\Temp\Low for file name = spwProfile

Profile xml not found Downloading profile configuration...

Downloading profile configuration...

Discovering ISE using default gateway

Identifying wired and wireless network interfaces, total active interfaces: 1

Network interface - mac:CO-4A-00-14-6E-31, name: Wireless Network Connection, type: wireless

Identified default gateway: 10.62.148.100

Identified default gateway: 10.62.148.100, mac address: CO-4A-00-14-6E-31
```

redirect attempt to discover ISE with the response url

DiscoverISE - start Discovered ISE - : [mgarcarz-ise20.example.com, sessionId: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7 DiscoverISE - end

Successfully Discovered ISE: mgarcarz-ise20.example.com, session id: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ

GetProfile - start GetProfile - end

Successfully retrieved profile xml

using V2 xml version parsing wireless connection setting

Certificate template: [keysize:2048, subject:OU=Example unit,O=Company name,L=City,ST=State,C=US, SAN:M2

set ChallengePwd

creating certificate with subject = cisco and subjectSuffix = OU=Example unit,O=Company name,L=City,ST= Installed [LAB CA, hash: fd 72 9a 3b b5 33 72 6f f8 45 03 58 a2 f7 eb 27^M ec 8a 11 78^M] as rootCA

Installed CA cert for authMode machineOrUser - Success

HttpWrapper::SendScepRequest

- Retrying: [1] time, after: [2] secs , Error: [0], msg: [Pending] creating response file name C:\Users\ADMINI~1.EXA\AppData\Local\Temp\response.cer

Certificate issued - successfully

ScepWrapper::InstallCert start

ScepWrapper::InstallCert: Reading scep response file

[C:\Users\ADMINI~1.EXA\AppData\Local\Temp\response.cer].
ScepWrapper::InstallCert GetCertHash -- return val 1
ScepWrapper::InstallCert end

Configuring wireless profiles...

Configuring ssid [mgarcarz_aruba_tls]

```
WirelessProfile::SetWirelessProfile - Start
```

Wireless profile: [mgarcarz_aruba_tls] configured successfully

Connect to SSID

```
Successfully connected profile: [mgarcarz_aruba_tls]
WirelessProfile::SetWirelessProfile. - End
```

Ces journaux sont exactement les mêmes que pour le processus BYOD avec les périphériques Cisco.



À ce stade, l'utilisateur peut voir que le système tente de s'associer à un SSID final. Si vous disposez de plusieurs certificats utilisateur, vous devez sélectionner le certificat correct (comme illustré).

Select Certificate		×
User name on certificate:		
cisco@example.com		-
cisco@example.com administrator@example.com	n	
cisco Issuer:	LABICA	
Expiration date:	7/17/2016 12:29:41 PM	
	OK Cancel View Certif	icate

Une fois la connexion établie, les rapports NSA sont tels qu'ils apparaissent dans l'image.



Cela peut être confirmé sur ISE : le deuxième journal atteint l'authentification EAP-TLS, qui correspond à toutes les conditions pour Basic_Authenticated_Access (EAP-TLS, Employee et BYOD Registered true).

1	dentity Se	ervices Engine	Home	 Operations 	 Policy 	Guest Access	Administration	Work Centers					
	RADIUS Livelog	TACACS Livelog	Reports	Troubleshoot	Adaptive Net	twork Control							
	Мі	isconfigured Supp	licants (i		Mis	sconfigured Netw	ork Devices 🏾 🔅	RADIU	RADIUS Drops				
		1				0		1	12		0		
	🗿 Show Live Se	📓 Show Live Sessions 🖗 Add or Remove Columns 🔻 🚸 Refresh 🔞 Reset Repeat Counts 🖉 Refresh 📴 Refresh 👔											
	Time	▼ Status All ▼ D	et R. (Identity ()	Endpoint ID 🕐	Authenticati	on Policy ①	Authorization Policy 🕐	Authorization Profiles	Network Device	Event (
	2015-10-29 22:2	3:37 🕦	Q 0	cisco C	0:4A:00:14:6E:	31 Default >> D	Oot1X >> EAP-TLS	Default >> Basic_Authenticated	PermitAccess		Session State is Started		
	2015-10-29 22:2	3:37 🔽	Q I	cisco C	0:4A:00:14:6E:	31 Default >> D	Oot1X >> EAP-TLS	Default >> Basic_Authenticated	PermitAccess	aruba	Authentication succeeded		
	2015-10-29 22:1	9:09 🔽	o I	cisco C	0:4A:00:14:6E:	31 Default >> D	ot1X >> Default	Default >> ArubaRedirect	Aruba-redirect-BYOD	aruba	Authentication succeeded		

En outre, l'affichage de l'identité du point de terminaison peut confirmer que l'indicateur BYOD Registered du point de terminaison a la valeur true, comme illustré dans l'image.

EndPoints	En	dpoint List													
Users			Endpoin		Endpoints by Policy Service Node										
Latest Manual Network Scan Results	etwork Scan Results				ndows7-Workstati.	rkstatl: 100%									
	2	Refresh + Ad	ld 📋 Trash ▾ Ư Eo	dit MDM Actio	ns 👻 Refresh N	DM Partner Endp	oint Import	 Export • 						Ŧ	Filter • • •
		Endpoint Profile	MAC Address	Vendor(OUI)	Logical Profiles	Hostname	MDM Server	Device Identifier	IP Address	Static Assignment	Static Group Assignment	Portal User	Device Registration	BYOD Registration	Profile Server
	×	Endpoint Prof	MAC Address			Hostname	MDM Sen	Device Ide	IP Address	Static Ass	Static Gro	Portal User	•	BYOD Re	Profile Server
		Windows7- Workstation	C0:4A:00:14:6E:31	TP-LINK TE		mgarcarz-pc			10.62.148.71	false	true	cisco	Registered	Yes	mgarcarz-ise

Sur le PC Windows, un nouveau profil sans fil a été créé automatiquement comme favori (et configuré pour EAP-TLS) et comme illustré.

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Add Remove Move down	Adapter propert	mgarcarz_aruba_tls Wi	reless Network Properties	×
Networks you can view, modify, an	nd reorder (4)	Connection Security		_
Ingarcaiz_aiuba_us	Security: WPA	Can giby hanas	(UD42 Selection -	
mancart subs	Security WD.	seconcy type:	wPA2-Enterprise +	
	secondy, new	Encryption type:	AES 💌	
pgruszcz_WLANI	Security: WPA	Channel & mathematics	thanking mathead	
moarcarz byod	Security: WPA	Mercenth: Smart Ca	nd or other certificat * Cattions	
		Provide and Coa	octorys	
· •		time I'm logged or	edentials for this connection each n	
		Advanced setting	s	

À ce stade, Aruba confirme que l'utilisateur est connecté au SSID final.



Le rôle qui est créé automatiquement et nommé de la même manière que Réseau fournit un accès réseau complet.

Security					
Authentication Servers Users for I	Internal Server	Roles	Blacklisting	Firewall Settings	Inbound Firewall
Roles	Access Rules	for mga	rcarz_aruba_t	tls	
default_wired_port_profile wired-instant ArubaAAA wcecot_BYOD_aruba mgarcarz_aruba	 Allow any te 	o all des	tinations		
mgarcarz_aruba_tls					
New Delete	New Edit	Delete			

Autres flux et assistance CoA

CWA avec CoA

Alors que dans le flux BYOD, il n'y a pas de messages CoA, le flux CWA avec le portail d'invité auto-enregistré est présenté ici :

Les règles d'autorisation configurées sont comme indiqué dans l'image.

~	Guest_Authenticate_internet	if	GuestEndpoints AND Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then	PermitAccess
~	Guest_Authenticate_Aruba	if	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then	Aruba-redirect-CWA

L'utilisateur se connecte au SSID avec l'authentification MAB et une fois qu'il tente de se connecter à une page Web, la redirection vers le portail d'invité auto-enregistré se produit, où l'invité peut créer un nouveau compte ou utiliser le compte actuel.

CISCO Sponsored Guest Portal

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:	
cisco	
Password:	
	•
	Sign On
	Don't have an account?

Une fois que l'invité est correctement connecté, un message CoA est envoyé d'ISE au périphérique réseau afin de modifier l'état d'autorisation.

cisco	Sponsored Guest Portal
Welcom	ne Message
Click Con	ntinue to connect to the network.
You're ver	ry close to gaining network access.
	Continue

Il peut être vérifié sous Opérations > Authentifications et comme montré dans l'image.

cisco	C0:4A:00:15:76:34	Windows7-Workstat Default >> MAB	Default >> Guest_Authenticate_internet	Authorize-Only succeeded	PermitAccess
	C0:4A:00:15:76:34			Dynamic Authorization succe	
cisco	C0:4A:00:15:76:34			Guest Authentication Passed	
C0:4A:00:15:7	6 C0:4A:00:15:76:34	Default >> MAB >> .	Default >> Guest_Authenticate_Aruba	Authentication succeeded	Aruba-redirect-CWA

Message CoA dans les débogages ISE :

<#root>

```
2015-11-02 18:47:49,553 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]
Processing incoming attribute vendor , name
```

۰,

```
DynamicAuthorizationFlow.cpp:708
2015-11-02 18:47:49,567 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]
Processing incoming attribute vendor , name
Acct-Session-Id, value=04BD88B88144-
C04A00157634-7AD
.,DynamicAuthorizationFlow.cpp:708
2015-11-02 18:47:49,573 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-
```

```
DynamicAuthorizationFlow, DEBUG, 0x7fc0e9cb2700, cntx=0000000561, sesn=c59aa41a-e029-4ba0-a31b
-44549024315e, CallingStationID=c04a00157634, [DynamicAuthorizationFlow::createCoACmd]
Processing incoming attribute vendor , name cisco-av-pair, v
alue=audit-session-id=0a3011ebisZXyp0DwqjB6j64GeFiF7RwvyocneEia17ckjtU1HI.,DynamicAuthorizationFlow.cpp
2015-11-02 18:47:49,584 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::
setConnectionParams]
```

defaults from nad profile : NAS=10.62.148.118, port=3799, timeout=5,

retries=2

```
,DynamicAuthorizationRequestHelper.cpp:59
2015-11-02 18:47:49,592 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::set
ConnectionParams] NAS=10.62.148.118, port=3799, timeout=5, retries=1,
DynamicAuthorizationRequestHelper.cpp:86
2015-11-02 18:47:49,615 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::onLocalHttpEvent]:
```

invoking DynamicAuthorization, DynamicAuthorizationFlow.cpp:246

et Disconnect-ACK d'Aruba :

<#root>

2015-11-02 18:47:49,737 DEBUG [Thread-147][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-DynamicAuthorizationFlow,DEBUG,0x7fc0e9eb4700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b -44549024315e,

CallingStationID=c04a00157634

,[DynamicAuthorizationFlow:: onResponseDynamicAuthorizationEvent] Handling response ID c59aa41a-e029-4ba0-a31b-44549024315e, error cause 0,

Packet type 41(DisconnectACK).

DynamicAuthorizationFlow.cpp:303

Les captures de paquets avec CoA Disonnect-Request (40) et Diconnect-ACK (41) se présentent comme illustré.

😣 🖱 💷 aruba_Endpoint_CWA.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]																		
	ک 🔳 🔰 🌒		K C	Q	۲	> 3	• T	₹		,		1	+ +	X	\mathbf{Y}	-6	💥 🛛 😨	
Filter:	udp.port==3799				*	Expres	sion	Clear	Apply	Save								
No.	Time	Source		Destina	ation		Prot	ocol		Len	gth				Info			
14	4 17:47:49.654868	10.48.17.235	5	10.62.1	48.11	8	RADIU	JS						100 [Discon	nect-	Request(40) (id=1, l=	=58)
14	7 17:47:49.707216	10.62.148.11	.8	10.48.1	7.235		RADIU	JS						74 [Discon	nect-	ACK(41) (id=1, l=32)	
<pre>▶Frame 144: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) ▶Ethernet II, Src: Vmware_99:6d:34 (00:50:56:99:6d:34), Dst: Cisco_1c:e8:00 (00:07:4f:1c:e8:00) ▶Internet Protocol Version 4, Src: 10.48.17.235 (10.48.17.235), Dst: 10.62.148.118 (10.62.148.118) ▶User Datagram Protocol, Src Port: 16573 (16573), Dst Port: radius-dynauth (3799) ▼Radius Protocol</pre>																		
Pack	et identifier: 0x1	1 (1)																
Lena	th: 58	- (-/																
Authenticator: 517f99c301100cb16f157562784666cb <u>[The response to this request is in frame 147]</u> VAttribute Value Pairs AVP: l=6 t=NAS-IP-Address(4): 10.62.148.118 AVP: l=14 t=Calling-Station-Id(31): c04a00157634 AVP: l=18 t=Message-Authenticator(80): d00e10060c68b99da3146b8592c873be																		

Remarque : RFC CoA a été utilisé pour l'authentification liée au profil de périphérique Aruba (paramètres par défaut). Pour l'authentification liée au périphérique Cisco, il aurait été de type Cisco CoA réauthentifier.

Dépannage

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

Portail captif Aruba avec adresse IP au lieu du nom de domaine complet

Si Captive Portal sur Aruba est configuré avec une adresse IP au lieu du nom de domaine complet d'ISE, PSN NSA échoue :

<#root>
Warning - [HTTPConnection]
Abort the HTTP connection due to invalid certificate

CN

La raison en est une validation stricte des certificats lorsque vous vous connectez à ISE. Lorsque vous utilisez l'adresse IP afin de vous connecter à ISE (à la suite de l'URL de redirection avec l'adresse IP au lieu de FQDN) et sont présentés avec le certificat ISE avec le nom du sujet = la validation FQDN échoue.

Remarque : le navigateur Web continue avec le portail BYOD (avec un avertissement qui

Noit être approuvé par l'utilisateur).

Aruba Captive Portal - Politique d'accès incorrecte

Par défaut, la politique d'accès Aruba configurée avec Captive Portal autorise les ports TCP 80, 443 et 8080.

NSA ne peut pas se connecter au port TCP 8905 pour obtenir le profil xml d'ISE. Cette erreur est signalée :

```
<#root>
Failed to get spw profile url using - url
[
https://mgarcarz-ise20.example.com:8905
/auth/provisioning/evaluate?
typeHint=SPWConfig&referrer=Windows&mac_address=C0-4A-00-14-6E-31&spw_version=
1.0.0.46&session=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7G1HXj1M&os=Windows All]
- http Error: [2]
HTTP response code: 0
]
GetProfile - end
Failed to get profile. Error: 2
```

Numéro de port Aruba CoA

Par défaut, Aruba fournit un numéro de port pour le port 5999 CoA Air Group CoA. Malheureusement, Aruba 204 n'a pas répondu à ces demandes (comme indiqué).

Event	5417 Dynamic Authorization failed
Failure Reason	11213 No response received from Network Access Device after sending a Dynamic Authorization request

Steps

11201 Received disconnect dynamic authorization request

- 11220 Prepared the reauthenticate request
- 11100 RADIUS-Client about to send request (port = 5999, type = RFC 5176)
- 11104 RADIUS-Client request timeout expired (0 Step latency=10009 ms)

11213 No response received from Network Access Device after sending a Dynamic Authorization request

La capture de paquets se déroule comme illustré dans l'image.



► AVP: l=18 t=Message-Authenticator(80): 1959020d15fe2b0584b3a887c1e3c366

La meilleure option à utiliser ici peut être le port CoA 3977, comme décrit dans la RFC 5176.

Redirection sur certains périphériques Aruba

Sur Aruba 3600 avec v6.3, on remarque que la redirection fonctionne légèrement différemment que sur les autres contrôleurs. La capture des paquets et l'explication sont disponibles ici.

770 09:29:40.5119110 10.75.94.213	173.194.124.52	HTTP	1373 GET / HTTP/1.1
772 09:29:40.5210656 173.194.124.52	10.75.94.213	HTTP	416 HTTP/1.1 200 Ok (text/html)
794 09:29:41.698257010.75.94.213	173.194.124.52	HTTP	63 GET /&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5 HTTP/1.1
797 09:29:41.7563060 173.194.124.52	10.75.94.213	HTTP	485 HTTP/1.1 302 Temporarily Moved

<#root>

packet 1: PC is sending GET request to google.com packet 2: Aruba is returning HTTP 200 OK with following content: <meta http-equiv='refresh' content='1; url=http://www.google.com/</pre>

&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5

'>\n
packet 3: PC is going to link with Aruba attribute returned in packet 2:
http://www.google.com/

&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5

packet 4: Aruba is redirecting to the ISE (302 code): https://10.75.89.197:8443/portal/g?p=4voD8q6W5Lxr8hpab77gL8VdaQ&cmd=login&

mac=80:86:f2:59:d9:db&ip=10.75.94.213&essid=SC%2DWiFi&apname=LRC-006&apgroup=default&url=http%3A%2F%2Fwatered approximate the state of the state of

Informations connexes

- Guide de l'administrateur de Cisco Identity Services Engine, version 2.0
- Profils de périphériques d'accès réseau avec Cisco Identity Services Engine
- <u>Assistance et documentation techniques Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.