H3Cアクセスコントローラ

Aruba ClearPassサーバーによるアクセス認証

設定例

Copyright©2022 New H3C Technologies Co.,Ltd.無断転載を禁ず。

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の承諾なく、いかなる形式または手段によっても複製または譲渡することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の商標または登録商標です。

このドキュメントの情報は、予告なしに変更されることがあります。

目次

前提条件	4
例·ClearPassベースのMAC認証の設定	4
ネットワーク構成	
使用されているソフトウェアバージョン	5
制約事項とガイドライン	5
手順	5
ACの設定	5
スイッナの設定	6 -
ClearPassサーハーの設定	/۱
設たの唯認 構成ファイル	11
例·ClearPassベースの802 1X FAP-PFAP認証の設定	14
ネットワーク構成	1 1
使用されているソフトウェアバージョン	
制約事項とガイドライン	14
手順	14
ACの設定	15
スイッチの設定	
ClearPassサーバーの設定	
設定の催認 構成ファイル	
_{備成} の 個 い し た た た の に の の の の の の の の の の の の の	22
例.VLANのよいACL 割り当てを使用した Clear ass ~ A0002.1 A 認証の	
	- 23
ネットワーク構成 使用されているソフトウェアバージョン	
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン	
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順	
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定	23 24 24 24 24
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定	23 24 24 24 24 25
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定	23 24 24 24 24 24 24 24 25 26
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認	23 24 24 24 24 24 24 25 25 26 34
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル	23 24 24 24 24 24 25 26 26 34 36
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassベースのポータル認証の設定	23 24 24 24 24 24 25 26 26 34 37
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassベースのポータル認証の設定 ネットワーク構成	23 24 24 24 24 24 25 26 34 36 36 37
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassベースのポータル認証の設定 ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン	23 24 24 24 24 25 26 34 36 37 37 38 38
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassベースのポータル認証の設定 ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順	23 24 24 24 24 25 25 26 34 36 37 37 38 38 38 38
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定	23 24 24 24 24 25 26 34 36 37 37 38 38 38 38 38 38
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassベースのポータル認証の設定 キットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定	23 24 24 24 24 25 25 26 34 36 37 37 37 38 38 38 38 38 38 40
ネットワーク構成	23 24 24 24 24 24 25 26 34 36 37 37 38 38 38 38 38 38 40 40
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassベースのポータル認証の設定 シットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 この設定 スイッチの設定 この設定 スイッチの設定 この設定 スイッチの設定 この設定 スイッチの設定 この設定 公の設定 この設定	23 24 24 24 24 25 25 26 34 36 37 37 38 38 38 38 38 38 40 40 40 40
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassベースのポータル認証の設定 キットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ここの 成定の設定 スイッチの設定 目の設定 単約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル	23 24 24 24 24 25 25 26 34 36 37 37 38 38 38 38 38 38 40 40 40 40 47 50
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassベースのポータル認証の設定 キットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル	$\begin{array}{c} 23 \\ 24 \\ 24 \\ 24 \\ 24 \\ 25 \\ 26 \\ 36 \\ 36 \\ 37 \\ 37 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38$
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassベースのポータル認証の設定 キットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーからユーザーを強制的にログオフする キットワーク構成	$\begin{array}{c} 23 \\ 24 \\ 24 \\ 24 \\ 24 \\ 25 \\ 26 \\ 36 \\ 36 \\ 36 \\ 37 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38$
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassベースのポータル認証の設定 キットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーからユーザーを強制的にログオフする ホットワーク構成 使用されているソフトウェアバージョン 単約時でレイバーグジョン	$\begin{array}{c} 23 \\ 24 \\ 24 \\ 24 \\ 24 \\ 25 \\ 26 \\ 36 \\ 36 \\ 36 \\ 37 \\ 37 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38$
ネットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassベースのポータル認証の設定 キットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順 ACの設定 スイッチの設定 ClearPassサーバーの設定 設定の確認 構成ファイル 例:ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassサーバーの設定 設定の確認 構成ファイル Ø:ClearPassサーバーからユーザーを強制的にログオフする ホットワーク構成 使用されているソフトウェアバージョン 制約事項とガイドライン 手順	$\begin{array}{c} 23 \\ 24 \\ 24 \\ 24 \\ 24 \\ 25 \\ 26 \\ 36 \\ 36 \\ 36 \\ 37 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38 \\ 38$

Cの設定	52
、イッチの設定	53
learPassサーバーの設定	54
設定の確認	59
ーーー 構成ファイル	62

はじめに

次の情報では、ワイヤレスクライアントの認証にAruba ClearPassサーバーを使用するようにH3Cアク セスコントローラを設定する例を示します。サポートされている機能には、MAC認証、802.1X認証、ポー タル認証、許可VLANおよびACL割り当て、RADIUS DAEによるユーザーの強制オフラインなどがあり ます。

前提条件

次の情報は、指定されたバージョンを実行しているH3Cアクセスコントローラ、H3Cアクセスポイント、およびAruba ClearPassサーバーに適用されます。例の手順と情報は、H3Cアクセスコントローラ、H3Cアクセスポイント、およびAruba ClearPassサーバーのソフトウェアまたはハードウェアの条件によって、多少異なる場合があります。詳細については、アクセスコントローラ、アクセスポイント、およびサーバーのマニュアルを参照してください。

設定例はラボ環境で作成および検証され、すべてのデバイスおよびサーバーは出荷時のデフォルト設定で起動されました。ライブネットワークで作業する場合は、すべての操作がネットワークに与える潜在的な影響を理解してください。

次の情報は、H3C AAA、802.1X、MAC認証、ポータル、WLANアクセス認証、およびWLANアクセス機能とAruba ClearPassサーバーに関する基本的な知識があることを前提としています。

例:ClearPassベースのMAC認証の設定

ネットワーク構成

図1に示すように、ACはスイッチを介してClearPassサーバーに到達できます。次の要件を満たすように

デバイスを設定します:

- ACは、ClearPassサーバーをRADIUSサーバーとして使用して、次のMAC認証を実行します。 クライアント。
- クライアントのMACアドレスは、MAC認証のユーザー名とパスワードの両方として使用されます。
 図1 ネットワーク図



使用されているソフトウェアバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成および確認されています。

ハードウェア	ソフトウェアのバージョン
WX5540Hアクセスコントローラ	R5444P03
WA5320アクセスポイント	R5444P03
Aruba ClearPassサーバー	CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf

制約事項とガイドライン

- ACで、MAC認証用のユーザーアカウントフォーマットを指定します。この例では、クライアントの MACアドレスがユーザー名とパスワードとして使用されます。RADIUSサーバーのユーザー名と パスワードの構成がACの構成と一致していることを確認してください。
- APの背面パネルに表示されているシリアルIDを使用して、APを指定します。
- 一部のエンドポイントでは、デフォルトでランダムMACアドレスが使用されます。このようなエンドポイントのMAC認証を成功させるには、エンドポイントがランダムMACアドレスを使用しないようにします。

手順

()重要:

この設定例では、ClearPassサーバーでのMAC認証によるクライアントの認証に関連する主な設定だけを説明します。基本的なネットワーク設定および基本的なWLAN設定については、デバイスおよびサ ーバーのマニュアルを参照してください。

ACの設定

```
#ClearPassという名前のRADIUSスキームを作成し、ユーザー認証とアカウンティング用に8.1.1.171の
ClearPassサーバーを指定して、暗号化された文字列h3cを共有キーに設定します。
#
radius scheme clearpass
  primary authentication 8.1.1.171
  primary accounting 8.1.1.171
  key authentication cipher $c$3$y9gLDgP10B8T9ry5u3AHTHOadEYI7g==
  key accounting cipher $c$3$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ==
  user-name-format without-domain
#
#ユーザー認証、認可、アカウンティングにRADIUSスキームのclearpassを使用するように、ISPドメイン
のclearpassを設定します。
#
domain clearpass
  authentication default radius-scheme clearpass
  authorization default radius-scheme clearpass
  accounting default radius-scheme clearpass
#
#クライアントのMACアドレスをMAC認証のユーザー名とパスワードの両方として使用するようにACを設
```

定します。MACアドレスは、ハイフンなしの16進数表記で、小文字の文字が使用されます(このステップの 設定はデフォルトの設定です)。

[AC]mac-authentication user-name-format mac-address without-hyphen lowercase

```
#サービステンプレートh3c-macauthを作成し、そのSSIDをh3c-macauthに設定し、認証モードをMAC
認証に設定して、認証ドメインclearpassを指定します。
```

```
#
wlan service-template h3c-macauth
ssid h3c-macauth
client-security authentication-mode mac
mac-authentication domain clearpass
service-template enable
```

#

```
#手動APを設定し、サービステンプレートh3c-macothをAPの無線にバインドします。
```

#

```
wlan ap ap1 model WA5320
```

serial-id 219801A0YD8171E04018

radio 1

radio enable

service-template h3c-macauth vlan 1308

radio 2

radio enable

service-template h3c-macauth vlan 1308

#

```
#スイッチに接続されているポートのリンクタイプをトランクに設定し、クライアントのVLAN内のト
ラフィックがポートを通過できるようにします。
```

#

interface Ten-GigabitEthernet1/0/26 port link-type trunk port trunk permit vlan all #

スイッチの設定

```
#VLAN 1308とVLAN-interface 1308を作成し、VLANインターフェースにIPアドレスを割り当てます。ス
イッチはこのVLANを使用してクライアントへのパケットを転送します。ACに接続されているポートのリン
クタイプをトランクに設定し、クライアントのVLAN内のトラフィックがポートを通過できるようにします。
[Switch] vlan 1308
#
interface Ten-GigabitEthernet0/0/35
  port link-type trunk
  port trunk permit vlan all
#
interface Vlan-interface1308
  ip address 40.8.0.1 255.255.0.0
#vlan1308という名前のDHCPアドレスプールを作成し、DHCPアドレスプールにサブネット40.8.0.0/16と
ゲートウェイIPアドレス40.8.0.1を指定します。この例では、DNSサーバーのアドレスは次のとおりです。
40.8.0.1(ゲートウェイアドレス)。ネットワーク上のDNSサーバーの実際のアドレスに置き換える必要があ
ります。
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
 return
```

ClearPassサーバーの設定

1. ClearPassサーバーにログインします。

#サーバーのWebインターフェースにアクセスするには、WebブラウザのアドレスバーにClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。

図2 ClearPassへのログイン

aruba	
	<u>-</u> ? Ø
	Wired Wineless VPN
	ClearPass
	AAA/Policy Device Goest Device Security Measurement Constantion Measurement Health Excitations
	nallegenetik vituwarung nallegenetik treakti Likulainge
	Rat-base Policies, Enterprise-grade AAA with Device Profiling
	ClearPass Onboard Nobic Devices Previousning ClearPass Insight Advanced Analytics, In-depth Reporting, Compliance &
	Regulation

ClearPass Policy Managerをクリックします。表示されたページで、ログインユーザー名とパス ワードを入力し、Log Inをクリックします。

図3 ClearPass Policy Managerへのログイン

You have 83 day(s) to activate the product Admin Login Usemame: Password: Log In
You have 83 day(s) to activate the product Admin Login Username: Password: Log In
You have 83 day(s) to activate the product Admin Login Username: Password: Log In
Admin Login
Admin Login Username: Password: Log In
Username: Password: Log In
Log In

ClearPass Policy ManagerにACを追加します。
 #左側のナビゲーションペインで、Configuration > Network > Devicesを選択します。開いたペー

ジで、右上隅にあるAddをクリックします。

- a. ACでIPアドレス40.1.1.56/24を指定します。 ClearPassサーバーがこのIPアドレスに到達できることを確認します。
- b. RADIUS共有秘密を設定します。

ここで指定した共有シークレットが、AC上のRADIUSサーバーに指定した共有キーと同じである ことを確認します。この例では、共有シークレットはh3cです。

- c. ベンダー名H3Cを選択します。
- d. Addをクリックします。

図4 デバイスの追加

aruba	ClearPass Policy Manager	Menu 🗮
Bashboard Monitoring	Configuration > Network > Devices Network Devices	🗭 Add
Configuration Configuration Configuration Services	A Network Access Device (VAD) must belong to the global list of devices in the ClearRess database in order to connect to ClearRess.	 Export All Discovered Devices
Q Methods Q Sources D Identity Single Sign On (550)	FRen V contains V Cont	Show 20 v records
Call Users Call Users Call Control (Control (Control)) Call Control (Control) Call Control (Control)	2. Device SMMP Read Settings SLIStettings CUIStettings	Copy.] Export Delete
Roles Rele Mappings Beforcement	Description:	
Opolicies Opolicies Opolicies Opolicies Opolicies Opolicies	AUUUS shared skotet: Verify: TACAS= Shared Skotet: Verify: Verify: Verify: Verify: Verify:	
Opevice Groups Opevice Groups	Enable PadSec:	
A FUILY SHITUBUUT	Add Cancel	

3. ユーザーの追加:

#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いた ページで、右上隅にあるAddをクリックします。

a. ユーザーID、名前、およびパスワードをクライアントのMACアドレスに設定します。MACアドレス の形式がACと同じであることを確認します。

この例では、MACアドレスはハイフンなしの16進数表記で、文字は小文字です。

- b. 事前定義済ロールEmployeeまたはユーザー定義済ロールを選択します。この例では、事前定 義済ロールEmployeeが選択されています。
- c. Addをクリックします。

```
図5 ユーザーの追加
```

aruba			ClearPass Policy Manager		Menu 🗮			
Dashboard	Configuration > Identity > L							
Monitoring	Local Users				🛶 Add			
Configuration	•				Export All			
Service Templates & Wizards								
- C Services	ClearPass Policy Manager lis	ts all local users in the Loc.	al Users page.					
- Authentication								
- 🛱 Methods	Filter: User ID	vilcontains vil	Go Gear Elter	-	Show 20 v records			
- 🛱 Sources	# User 1D	Add Local User		Role	Status			
Identity				[Employee]	Enabled			
Dingle Sign-On (SSO)		User ID:	(fcdbb3d4d88c	[Employee]	Enabled			
Tocal Users		Name:	fcdbb3d4d88c	[Employee]	Enabled			
The Static Host Lists	a. Dieader	Password:		Teacherse 2	Enabled			
12 Roles	4. U yuandong			[Employee]	Enabled			
C Role Mappings	5. U yuandong	verity Password:		[Employee]	Enabled			
- 🕆 Posture	Showing 1-5 of 5	Enable User:	Check to enable user)		Export Delete			
🖯 💲 Enforcement		Change Password:	(Check to force change password on next TACACS+ login)					
Q Policies		Role:	[Employee]					
Network								
- Q Devices								
- 🛱 Device Groups								
Proxy Targets								
- 🛱 Event Sources								
- Q Network Scan								
- La Policy Simulation								
			Add Cancel					

4. サービスを追加します。

#左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、 右上隅のAddをクリックします。

図6 Serviceページ

aruba				ClearPass Polic	y Manager		Menu 🗮
Dashboard	O Configur	ation » S	ervices				
Monitoring	 Service 	es					👍 Add
Configuration	•						Export All
- 🛱 Service Templates & Wizards - 🋱 <mark>Services</mark>	This page	e shows	the current	list and order of services that ClearPass follows during auth	entication and authorization.		
E 🔒 Authentication	Filter: N	ame		v contains v + Go C	lear Filter		Show 50 v records
- Q Methods			Order •	Name	Туре	Template	Status
- Q Identity	1.	0	9	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	0
- 🛱 Single Sign-On (SSO)	2.	0	8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0
- 🛱 Local Users	3.	0	7	[Insight Operator Logins]	Application	Aruba Application Authentication	0
- C Endpoints	4.		6	[Guest Operator Logins]	Application	Aruba Application Authentication	0
- i Static Host Lists	5.		5	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0
A Role Mannings	6.	0	4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	ø
Posture	7.	0	3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	ø
Enforcement	8.	0	2	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	0
- 🗘 Policies	9.		1	dafu-802.1×	RADIUS	802.1X Wireless - Identity Only	0
- Q Profiles → Network - Q Devices - Q Device Groups - Q Proxy Targets - Q Event Sources - Q Network Scan - Q Policy Simulation	Showing	1-9 of 9					Reorder Copy Export Delete

Serviceタブで、TypeフィールドからMAC Authenticationを選択し、名前をMAC ACCESSとします。

図7 Serviceの追加

aruba		ClearPass Policy Mar	ager		Menu 🚍
Dashboard	 Configuration > Services > Add 				
Monitoring	 Services 				
Configuration	Service Authentication Role	es Enforcement Summary			
Configuration Scarde Templates & Witards Service Templates & Witards Service Templates & Witards Services Serv	Servic Authentication Ref Type: MACA Type T	s Enforcement Summary utherification Utherification Sector Sector	ng Proxy Service Rule Operator BELONICS_TO BELONICS_TO EQUALS	Value Ethernet (15), Wirelesse 002.11 (19) Login-Vare (1), Call-Check (10) % (Radius:IETF:User-Name,)	Ra 2 Rg 9 Rg 9
Administration	Back to Services			Next → S	ave Cancel

Authentication タブで、Authentication MethodsのAllow All MAC AUTHを選択します。 Authentication Sourcesフィールドのデフォルト値を使用します。

aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Services » Add	
🖂 Monitoring	• Services	
Configuration	Service Authentication Roles Enforcement Summary	
Q Service Templates & Wilards Q Service Q Service Q Service Q Service Q Service Q Sources Q So	Authentication Methods: [Align Ali MAC AUTH] Hove Up : More Down . Common Common View Details Modify	Add New Authentication Method
- ↓ Local Users - ↓ Ecal Users - ↓ Static Host Lists - ↓ Roles - ↓ Role Mappings - ♥ Posture - ● \$Enforcement	Authentication Sources: [Endpoints Reporting Local SQL OB] Move Up : Move Up : Move Down . New Details Modely View Details	Add New Authentication Source
- Q Policies	Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes	
Profiles Profiles Profiles Optices		
Administration	Back to Services	Next → Save Cancel

RoleタブとEnforcementタブで、パラメータの既定の設定を使用し、Saveをクリックします。

Configuration > ServicesページでReorderをクリックして、MAC ACCESSという名前のサービスを最初に移動します。

図9 サービスの順序変更

aruba				ClearPass Policy	Manager		Menu
Dashboard	O Configur	ation »	Services				
Monitoring	 Service 	ces					🚽 Add
Configuration	0						A Import
Service Templates & Wizards	This pag	e show	s the current	list and order of services that ClearPass follows during authe	ntication and authorization.		E copore
Direction Services							
Authentication	Filter: N	lame		v contains v Go Cle	ar Filter		Show 50 v rec
- Cr Methods			Order v	Name	Type	Template	Status
- Q Sources	1.		10	MAC ACCESS	BADIUS	MAC Authentication	0
A Single Sign-On (SSO)	2	0	0	h3c Guest Access	RADIUS	RADIUS Enforcement / Generic)	0
- tä Local Users	3	0	8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0
- 🛱 Endpoints	4	0	7	[Insight Operator Logins]	Application	Aruba Application Authentication	0
—党 Static Host Lists	-	0	6	[Guest Operator Logins]	Application	Acuba Application Authentication	
- 🛱 Roles	5.	0	6	(Aruba Davice Access Service)	TACACS	TACACS+ Enforcement	
- Q Role Mappings	7	0	4	[AirGroup Authorization Service]	PADTUS	RADIUS Enforcement (Generic)	
T Posture		- n	3	[Rolicy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
ži Policies	0.	l n	2	changer 205.1x	PADIUS	Anuba 802 1X Wireless	
- C Profiles			2	dofu-203-1x	RADIUS	202 1X Wireless	
- Network			1	0800-60211X	KADIO3	602.1X Wileless - Identity Only	
- 🛱 Devices	Showing	1-10 c	of 10			Reo	der Copy Export Delet
- 🋱 Device Groups							
- 🛱 Proxy Targets							
🖧 Event Sources							
Q Network Scan							
Delicy Simulation							

設定の確認

- 1. クライアントで、サービスh3c-macothに関連付けられ、IPアドレスを取得してゲートウェイにping を実行できることを確認します(詳細は省略)。
- 2. ACで、WLANクライアント情報およびオンラインMAC認証ユーザーに関する情報を表示して、クラ イアントがオンラインになったことを確認します。

[AC] display wlan client Total number of clients: 1

MAC address	User name	AP name	R	IP address VLAN
cdb-b3d4-d88c	fcdbb3d4d88c	ap1	2	40.8.0.129 1308

[AC] display wlan client verbose Total number of clients: 1

l otal number of clients: 1	
MAC address	: fcdb-b3d4-d88c
IPv4 address	: 40.8.0.129
IPv6 address	: N/A
Username	: fcdbb3d4d88c
AID	: 1
AP ID	: 26
AP name	: ap1
Radio ID	: 2
SSID	: h3c-macauth
BSSID	: ac74-0906-e872
VLAN ID	: 1308
Sleep count	: 0
Wireless mode	: 802.11gn
Channel bandwidth	: 20MHz
20/40 BSS Coexistence Managemen	it : Not supported
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Not supported
STBC RX capability	: Supported
STBC TX capability	: Supported
LDPC RX capability	: Supported
Block Ack	: N/A
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7,
	8, 9, 10, 11, 12, 13, 14,15
Supported rates	: 11, 12, 18, 24, 36, 48, 54 Mbps

QoS mode	: WMM
Listen interval	: 10
RSSI	: 0
Rx/Tx rate	: 0/0 Mbps
Authentication method	: Open system
Security mode	: PRE-RSNA
AKM mode	: Not configured
Cipher suite	: N/A
User authentication mode	: MAC
WPA3 status	: N/A
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Authorization CAR	: N/A
Roam status	: N/A
Key derivation	: N/A
PMF status	: N/A
Forwarding policy name	: Not configured
Online time	: Odays Ohours Ominutes 15seconds
FT status	: Inactive
[AC] display mac-authentication con	nection
[AC] display mac-authentication cont Total connections: 1	nection
[AC] display mac-authentication con Total connections: 1 User MAC address	rection : fcdb-b3d4-d88c
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name	nection : fcdb-b3d4-d88c : ap1
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID	nection : fcdb-b3d4-d88c : ap1 : 2
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID	nection : fcdb-b3d4-d88c : ap1 : 2 : b3c-macauth
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VI AN	hection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization ACL number	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : N/A
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization ACL number Authorization user profile	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : N/A : N/A
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization ACL number Authorization user profile Authorization CAR	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : N/A : N/A : N/A
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization VLAN Authorization ACL number Authorization user profile Authorization CAR Authorization URL	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : N/A : N/A : N/A : N/A
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization ACL number Authorization user profile Authorization CAR Authorization URL Termination action	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : N/A : N/A : N/A : N/A : N/A : N/A
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization VLAN Authorization ACL number Authorization user profile Authorization CAR Authorization URL Termination action Session timeout last from	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : N/A : N/A : N/A : N/A : N/A : N/A : N/A : N/A : N/A
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization VLAN Authorization ACL number Authorization user profile Authorization CAR Authorization URL Termination action Session timeout last from Session timeout period	nection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : N/A : N/A
[AC] display mac-authentication cont Total connections: 1 User MAC address AP name Radio ID SSID BSSID Username Authentication domain Initial VLAN Authorization VLAN Authorization VLAN Authorization ACL number Authorization URL Termination action Session timeout last from Session timeout period Online from	rection : fcdb-b3d4-d88c : ap1 : 2 : h3c-macauth : ac74-0906-e872 : fcdbb3d4d88c : clearpass : 1308 : 1308 : 1308 : N/A : N/A

Online duration : 0h 0m 27sClearPassサーバーで、オンラインユーザー情報を表示します。
 #左側のナビゲーションペインで、Monitoring > Live Monitoring > Access Trackerを選択しま

す。

#表示されたページで、ユーザーfcdbb3d4d88cが認証に合格したことを確認します。

図10 オンラインユーザーの表示

aruba		ClearPass Policy Manager					
Dashboard Monitoring	Monitoring > Live Monitoring > Ac Access Tracker oct 27, 20	Monitoring > Live Monitoring > Access Tracker Access Tracker or 27, 2021 16:39:52 CST					
	The Access Tracker page provides	a real-time display of per-session acces	s activity on the selected server o	or domain.	foday	Edit	
Manalysis & Trending Manalysis & Trending Profiler and Network Scan Metwork Scan Results	Filter: Usemame Server	Contains V Source	Go Clear Filter Username	Service	Login Status	Show 50 v records Request Timestamp v	
Discovered Devices Audit Viewer Bevent Viewer Data Filters Blacklisted Users							

構成ファイル

```
• AC:
  #
  radius scheme clearpass
    primary authentication 8.1.1.171
    primary accounting 8.1.1.171
    key authentication cipher $c$3$y9gLDgP10B8T9ry5u3AHTHOadEYI7g==
    key accounting cipher $c$3$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ==
    user-name-format without-domain
  #
  domain clearpass
    authentication default radius-scheme clearpass
    authorization default radius-scheme clearpass
    accounting default radius-scheme clearpass
  #
  wlan service-template h3c-macauth
    ssid h3c-macauth
    client-security authentication-mode mac
    mac-authentication domain clearpass
    service-template enable
  #
  wlan ap ap1 model WA5320
    serial-id 219801A0YD8171E04018
    radio 1
      radio enable
      service-template h3c-macauth vlan 1308
    radio 2
      radio enable
      service-template h3c-macauth vlan 1308
  #
  interface Ten-GigabitEthernet1/0/26
  port link-type trunk
  port trunk permit vlan all
• Switch:
  #
  vlan 1308
  #
  interface Ten-GigabitEthernet0/0/35
    port link-type trunk
    port trunk permit vlan all
  #
  interface Vlan-interface1308
```

```
ip address 40.8.0.1 255.255.0.0
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
return
```

例:ClearPassベースの802.1X EAP-PEAP認 証の設定

ネットワーク構成

図11に示すように、ACはスイッチを介してClearPassサーバーに到達できます。次の要件を満たすよう にデバイスを設定します:

- ACはClearPassサーバーをRADIUSサーバーとして使用して、次の802.1X認証を実行します。 クライアント。
- 認証方式はEAP-PEAPです。



使用されているソフトウェアバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成および確認されています。

ハードウェア	ソフトウェアのバージョン
WX5540Hアクセスコントローラ	R5444P03
WA5320アクセスポイント	R5444P03
Aruba ClearPassサーバー	CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf

制約事項とガイドライン

APの背面パネルに表示されているシリアルIDを使用して、APを指定します。



()重要:

この設定例では、ClearPassサーバーでの802.1X EAP-PEAP認証によるクライアントの認証に関連する主な設定だけを説明します。基本的なネットワーク設定および基本的なWLAN設定については、デバ

イスおよびサーバーのマニュアルを参照してください。

ACの 設定

```
#ClearPassという名前のRADIUSスキームを作成し、ユーザー認証とアカウンティング用に8.1.1.171の
ClearPassサーバーを指定して、暗号化された文字列h3clに共有キーを設定します。
#
radius scheme clearpass
  primary authentication 8.1.1.171
  primary accounting 8.1.1.171
  key authentication cipher $c$3$y9gLDgP10B8T9ry5u3AHTHOadEYI7g==
  key accounting cipher $c$3$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ==
  user-name-format without-domain
#
#ユーザー認証、認可、アカウンティングにRADIUSスキームのclearpassを使用するように、ISPドメイン
のclearpassを設定します。
#
domain clearpass
  authentication default radius-scheme clearpass
  authorization default radius-scheme clearpass
  accounting default radius-scheme clearpass
#
#EAPリレーを使用して802.1Xクライアントを認証するようにACを設定します。
[AC] dot1x authentication-method eap
#サービステンプレートh3c-dot1xを作成し、そのSSIDをh3c-dot1xに設定し、認証モードを802.1X認証に
設定して、認証ドメインclearpassを指定します。
#
wlan service-template h3c-dot1x
  ssid h3c-dot1x
  akm mode dot1x
  cipher-suite ccmp
  security-ie rsn
  client-security authentication-mode dot1x
  dot1x domain clearpass
  service-template enable
#
#手動APを設定し、サービステンプレートh3c-dot1xをAPの無線にバインドします。
#
wlan ap ap1 model WA5320
  serial-id 219801A0YD8171E04018
  radio 1
    radio enable
    service-template h3c-dot1x vlan 1308
  radio 2
    radio enable
    service-template h3c-dot1x vlan 1308
#
#スイッチに接続されているポートのリンクタイプをトランクに設定し、クライアントのVLAN内のトラフィック
がポートを通過できるようにします。
```

```
#
interface Ten-GigabitEthernet1/0/26
    port link-type trunk
    port trunk permit vlan all
#
```

スイッチの設定

```
#VLAN 1308とVLAN-interface 1308を作成し、VLANインターフェースにIPアドレスを割り当てます。ス
イッチはこのVLANを使用してクライアントへのパケットを転送します。ACに接続されているポートのリン
クタイプをトランクに設定し、クライアントのVLAN内のトラフィックがポートを通過できるようにします。
[Switch] vlan 1308
#
interface Ten-GigabitEthernet0/0/35
  port link-type trunk
  port trunk permit vlan all
#
interface Vlan-interface1308
  ip address 40.8.0.1 255.255.0.0
#vlan1308という名前のDHCPアドレスプールを作成し、DHCPアドレスプールにサブネット40.8.0.0/16と
ゲートウェイIPアドレス40.8.0.1を指定します。この例では、DNSサーバーのアドレスは次のとおりです。
40.8.0.1(ゲートウェイアドレス)。ネットワーク上のDNSサーバーの実際のアドレスに置き換える必要があ
ります。
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
return
#
```

ClearPassサーバーの設定

1. ClearPassサーバーにログインします。

#サーバーのWebインターフェースにアクセスするには、WebブラウザのアドレスバーにClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。



aruba	
	₽ ≈ Ø
	Wired Wireless VPN
	ClearPass
	AAA/Policy Device Guest Device Security Management Obbarding Management Health Exchange
	ClearPass Policy Manager ClearPass Guest Rele-based Polices, Enterprise-grade AAA with Device Guest Management
	- running
	ClearPass Onboard Robile Devices Provisioning ClearPass Insight Advanced Analytics, In-depth Reporting, Compliance &
	Regulation

ClearPass Policy Managerをクリックします。表示されたページで、ログインユーザー名とパスワ

ードを入力し、Log Inをクリックします。

図13 ClearPass Policy Managerへのログイン

aruba	ClearPass Policy Manager
	You have 83 day(s) to activate the product
	Admin Login
	Password:
	Log In
© Copyright 2020 Hewlett Packard Enterprise Development LP	

- ClearPass Policy ManagerにACを追加します。
 #左側のナビゲーションペインで、Configuration > Network > Devicesを選択します。開いたページ で、右上隅にあるAddをクリックします。
 - a. ACでIPアドレス40.1.1.56/24を指定します。 ClearPassサーバーがこのIPアドレスに到達できることを確認します。
 - b. RADIUS共有秘密を設定します。 ここで指定した共有シークレットが、AC上のRADIUSサーバーに指定した共有キーと同じであることを確認します。この例では、共有シークレットはh3cです。
 - **c.** ベンダー名H3Cを選択します。
 - d. Addをクリックします。

図14 デバイスの追加

aruba			ClearPass Pol	icy Manager				Menu 🗮
Dashboard	Configuration » N	Configuration * Network * Devices						
Monitoring	Network De	vices						🐥 Add
Configuration	•							Export All
Service Templates & Wizards								Discovered Devices
- 🛱 Services	A Network Access	Device (NAD) must belong to the g	lobal list of devices in the Clean	Pass database in order (to connect to ClearPa	55.		
Authentication	Filter: Name	✓ contains ✓	Go	Clear Filter				Show 20 v records
Sources	# Add	Device				0		
Identity Single Sign On (SSO)	1.	Derne						
- Q Local Users	2.	evice SNMP Read Settings SN	IMP Write Settings CLI Settin	ngs OnConnect Enfo	rcement Attribute	15		
- 🛱 Endpoints	3. Nai	me:	AC					
- 🛱 Static Host Lists 🛱 Roles	Showing 1-	or Subnet Address:	40.1.1.56/24 (e.g., 192.168.1.10 or 192.16	8.1.1/24 or 192.168.1.	1-20 or 2001:db8:a0	(b:12f0::1)		
Role Mappings	De	scription:						
E Posture								
Benforcement	RA	DIUS Shared Secret:		Verify:	[
C Profiles	TAC	CACS+ Shared Secret:	[Verify:				
Network	Ver	ndor Name:	H3C .					
- O Devices	Ena	able RADIUS Dynamic Authorization:	H3C					
- D Proxy Targets	Ena	able RadSec:	0					
_ Q Event Sources								
🖧 Network Scan								
- D Policy Simulation								
						Add Cancel		

3. ユーザーの追加:

#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたペ ージで、右上隅にあるAddをクリックします。

- a. ユーザーID、名前、およびパスワードをh3c1xに設定します。
- b. 事前定義済ロールEmployeeまたはユーザー定義済ロールを選択します。この例では、事前定 義済ロールEmployeeが選択されています。
- c. Addをクリックします。

図15 ユーザーの追加

aruba		ClearPass Policy Manager					
Dashboard	Configuration » Identity » Los	al Users					
Monitoring C	Local Users				🛶 Add		
Configuration	2				A Import		
Ca Service Templates & Wizards					Account Settings		
- O Services	ClearPass Policy Manager lists	s all local users in the Loc	al Users page.				
- Authentication							
- 🛱 Methods	Filter: User ID	vil containe vi	Go Clear Filter		Show 20 v records		
- 🛱 Sources	# User ID a	Add Local User		Role	Status		
E G Identity		The second	-	[Employee]	Enabled		
g single sign-On (SSO)	2 C fodbh3dada	User ID:	h3c1x	[Employee]	Enabled		
CT Endpoints	2 D b2coortal	Name:	h3c1x	[Employee]	Enabled		
i'i Static Host Lists	1 D teader	Password:		landocrala	Enabled		
- La Roles	4. C leader	Varifi Protword		(Conclosed)	Enabled		
- 🛱 Role Mappings	5. U yuandongq	verity Passiford.		[Employee]	Enabled		
	o. U yuandongq	Enable User:	(Check to enable user)	[Employee]	Enabled		
3 Benforcement	Showing 1-6 of 6	Change Password:	Check to force change password on next TACACS+ login)				
- Q Policies		Role:	[Employee]				
- A Promes			Attributes				
- Devices		Attribute	Value	1			
Device Groups		1. Click to add					
- 🛱 Proxy Targets							
- G Event Sources							
- Q Network Scan							
- A Policy Sindlation							
			Add Cancel				
Administration							

4. サービスを追加します。

#左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、 右上隅のAddをクリックします。 図16 サービスページ

図17 サービスの追加

aruba		ClearPass Policy Manager							
Dashboard	O Configur	ration > 3	Services						
Monitoring	• Servio	ces					Add		
O Service Templates & Wizards	This pag	e shows	the current	list and order of services that ClearPass follows during auth	entication and authorization.		E Lipote		
Authentication	Filter: N	lame		✓ contains ✓ → Go C	lear Filter		Show 50 v reco		
- Li Methods - La Sources			Order •	Name	Туре	Template	Status		
Q Identity	1.	0	9	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	0		
- Ö Single Sign-On (SSO)	2.	0	8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0		
- 🛱 Local Users	3.	0	7	[Insight Operator Logins]	Application	Aruba Application Authentication	۲		
- 🛱 Endpoints	4.		6	[Guest Operator Logins]	Application	Aruba Application Authentication	0		
- 🛱 Static Host Lists	5.		5	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0		
- Q Roles	6.	0	4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0		
Posture	7.	0	3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0		
\$ Enforcement	8.	0	2	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	0		
- C Policies	9.	0	1	dafu-802.1x	RADIUS	802.1X Wireless - Identity Only	0		
-	Showing	1-9 of 9	,			R	order Copy Export Delet		
🛱 Event Sources 🛱 Network Scan 🛱 Policy Simulation									

Serviceタブで、Typeフィールドから802.1X Wireless-Identity Onlyを選択し、h3cの名前を 802.1Xに設定します。

aruba				ClearPass Po	licy Manager			Mer	nu =
Dashboard	Confi	iguration > Services	» Add						
Monitoring O	Ser	vices							
Configuration O	Ser	vice Authentical	tion Roles Enforcement	Summary					
Service Templates & Wizards	Туре		802.1X Wired - Identity Only	~					_
Authentication	Name	e:	802.1X for h3c						
A Methods G Sources	Desc	ription:	802.1X Wired Access Serv Only	rice - Identity					
- I's Single Sign-On (SSO)	Monit	tor Mode:	Enable to monitor netw	ork access without enforcement	ent				
्री Local Users	More	Options:	Authorization Profile	e Endpoints 🗆 Accounting Prox	xy				
- 🛱 Endpoints					Service R	ule			
- 🖧 Static Host Lists	Match	hes O ANY or 🖲	ALL of the following conditions						
- La Role Mappings		Туре		Name	4	Operator	Value		
- TP Posture	1.	Radius:IETF		NAS-Port-Type		EQUALS	Ethernet (15)	9	6 1
3 8 Enforcement	2.	Radius:IETF		Service-Type		BELONGS_TO	Login-User (1), Framed-User (2), Authentical	.e- 9	10 10
- A Policies	3.	Click to add					Silly (Sy		
 Ansendet O Device Groups O Povice Groups O Proy Targets O Proy Targets O Henror Scan O Henror Scan 									t
Administration O	< B	ack to Services					Next→ Sa	ve 📕	Cancel

AuthenticationタブのAuthentication Methodsフィールドで[EAP MSCHAPv2]と[EAP PEAP]を選択しAuthentication Sourcesフィールドで[Local User Repository]を選択します。

19

図18 認証の構成

aruba	ClearPass Policy Manager	Menu
Dashboard O	Configuration » Services » Add	
Monitoring 0	Services	
Configuration O	Service Authentication Roles Enforcement Summary	
Q Service Templates & Wizards Q Service Q Service Q Hethods Q Hethods Q Hethods Q Enritly Q Services Q Ionnity Q Single Sign-On (SSO)	Authentication Methods: [EAP MASCHAPV2] More Down j More Down j Mo	Add New Authentication Method
Count offers Count offers	Authentication Sources: [Local User Reporting] [Local SQL 08] Move Up 1 Move Doms] Commove View Details Modify	Add New Authentication Source
- Li Profiles	Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes	
Q Profile Profile Devices Q Device Groups Q Device Groups Q Device Sources Provy Targets D Internots Scan Q Policy Simulation	Service Certificate: -Select to Add- v	View Certificate Details
Administration 0	K Back to Services	Next → Save Cancel

RolesタブとEnforcementタブで、パラメータの既定の設定を使用し、Saveをクリックします。

Configuration > Servicesページで、Reorderをクリックして、h3cの802.1Xという名前のサービスを最初に移動します。

図19 サービスの順序変更

aruba		ClearPass Policy Manager						
Dashboard	o Configura	ation > Services						
Monitoring	 Servic 	es				🚽 Add		
Configuration	0					Export All		
Ö Service Templates & Wizards				Service "802.1X for h3c" has be	en added			
🔅 Services	This seaso		list and order of environmental class form follows during a state	ation and a standarding				
Authentication	inis page	e shows the current	list and order of services that clearrass rollows during autor	entication and authorization.				
- 🛱 Methods	-			-				
- 🋱 Sources	Filter: Na	ame	✓ contains ✓	ear Filter		Show bu v records		
🗃 🚨 Identity		Order •	Name	Туре	Template	Status		
—⊈ Single Sign-On (SSO)	1.	0 110	802.1X for h3c	RADIUS	802.1X Wired - Identity Only	0		
- Local Users	2.	10	MAC ACCESS	RADIUS	MAC Authentication	0		
- ICE Endpoints	3.	9	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	0		
- I Static Host Lists	4.	0 8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0		
T Role Mappings	5.	0 7	[Insight Operator Logins]	Application	Aruba Application Authentication	0		
- I Posture	6.	6	[Guest Operator Logins]	Application	Aruba Application Authentication	0		
🗟 🛱 Enforcement	7.	0 5	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0		
- Dicies	8.	0 4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0		
- trofiles	9.	0 3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0		
- **• Network	10.	2	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	0		
- C Device Groups	11.	0 1	dafu-802.1x	RADIUS	802.1X Wireless - Identity Only	0		
- I'l Proxy Targets	Chauden	1 11 411				Baseles Press) France (Street		
Le Event Sources	Snowing	1-11 01 11				Reorder Copy Export Denote		
Q Network Scan								
- Dicy Simulation								

設定の確認

- 1. クライアントで、サービスh3c-dot1xに関連付けられ、802.1X認証を通過してIPアドレスを取得 できることを確認します(詳細は省略)。
- ACで、WLANクライアント情報とオンライン802.1Xユーザー情報を表示して、クライアントがオン ラインになったことを確認します。
 [AC] display wlan client Total number of clients: 1 MAC address User name AP name R IP address VLAN fcdb-b3d4-d88c h3c1x ap1 2 40.8.0.129 1308

[AC] display wlan client verbose	
lotal number of clients: 1	
MAC address	: fcdb-b3d4-d88c
IPv4 address	: 40.8.0.129
IPv6 address	: N/A
Username	: h3c1x
AID	:1
AP ID	: 26
AP name	: ap1
Radio ID	: 2
SSID	: h3c-dot1x
BSSID	: ac74-0906-e874
VLAN ID	: 1308
Sleep count	: 0
Wireless mode	: 802.11gn
Channel bandwidth : 20MHz	
20/40 BSS Coexistence Management	: Not supported
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Not supported
STBC RX capability	: Supported
STBC TX capability	: Supported
LDPC RX capability	: Supported
Block Ack	: N/Å
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7,
	8, 9, 10, 11, 12, 13, 14,15
Supported rates	: 11, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	10
RSSI	· 0
Rx/Tx rate	: 0/0 Mbps
Authentication method	· Open system
Security mode	· RSN
AKM mode	· 802 1X
Cipher suite	COMP
User authentication mode	· 802 1X
WPA3 status	: Disabled
Authorization ACL ID	· N/A
Authorization user profile	: N/A
Authorization CAR	· N/A
Roam status	· N/A
Koy dorivation	
DME status	· NI/A
Fiver Status	. N/A : Not configured
	: Not configured
	. Judys onours onninutes Toseconus
FT Status	
[AC] display dot1x connection	
Total connections: 1	
User MAC address · fcdb-b3d4-d88c	
AP name : ap1	
Radio ID · 2	

SSID : h3c-dot1x BSSID : ac74-0906-e874 Username : h3c1x Authentication domain : clearpass IPv4 address : 40.8.0.129

Authentication method	: EAP
Initial VLAN	: 1308
Authorization VLAN	: 1308
Authorization ACL number	: N/A
Authorization user profile	: N/A
Authorization CAR	: N/A
Termination action	: N/A
Session timeout last from	: N/A
Session timeout period	: N/A
Online from	: 2019/03/16 11:14:25
Online duration	: 0h 0m 19s

3. ClearPassサーバーで、オンラインユーザー情報を表示します。

#左側のナビゲーションペインで、Monitoring > Live Monitoring > Access Trackerを選択します。 #表示されたページで、クライアントが802.1X EAP-PEAP認証を通過したことを確認します。

図20オンラインユー	ザーの	表示
------------	-----	----

aruba		Menu						
E Dashboard	Monitoring > Live Monitoring > Acc Access Tracker oct 27, 202	Monitoring » Live Monitoring » Access Tracker Access Tracker or 27, 2021 16:39:52 CST						
Politoting Politoting Access Tracker Access Tracker OnGuard Activity	The Access Tracker page provides	a real-time display of per-session access	activity on the selected server o	er domain.	Dday	Edit		
System Honito System Honito Portifier and Itetwork Scan Endpoint Profile Proceent Profile Proceent Profile Proceent Profile Proceent Profile Profile	Filter: (Usemane v	Contains V (Go Clear Filter Username	Service	Login Status	Show (50 v) records		

構成ファイル

AC:

#

radius scheme clearpass primary authentication 8.1.1.171 primary accounting 8.1.1.171 key authentication cipher \$c\$3\$y9gLDgP10B8T9ry5u3AHTHOadEYI7g== key accounting cipher \$c\$3\$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ== user-name-format without-domain

#

domain clearpass

authentication default radius-scheme clearpass authorization default radius-scheme clearpass accounting default radius-scheme clearpass

#

dot1x authentication-method eap

#

wlan service-template h3c-dot1x

ssid h3c-dot1x

- akm mode dot1x
- cipher-suite ccmp

security-ie rsn client-security authentication-mode dot1x dot1x domain clearpass service-template enable # wlan ap ap1 model WA5320 serial-id 219801A0YD8171E04018 radio 1 radio enable service-template h3c-dot1x vlan 1308 radio 2 radio enable service-template h3c-dot1x vlan 1308 # interface Ten-GigabitEthernet1/0/26 port link-type trunk port trunk permit vlan all スイッチ: # vlan 1308 # interface Ten-GigabitEthernet0/0/35 port link-type trunk port trunk permit vlan all # interface Vlan-interface1308 ip address 40.8.0.1 255.255.0.0 # dhcp server ip-pool vlan1308

```
gateway-list 40.8.0.1
network 40.8.0.0 mask 255.255.0.0
dns-list 40.8.0.1
#
```

return

•

例:VLANおよびACL割り当てを使用した ClearPassベースの802.1X認証の設定

ネットワーク構成

図21に示すように、ACはスイッチを介してClearPassサーバーに到達できます。次の要件を満たすよう にデバイスを構成します:

- ACはClearPassサーバーをRADIUSサーバーとして使用して、次の802.1X認証を実行します。 クライアント。
- 認証方式はEAP-PEAPです。

 クライアントが802.1X認証を通過すると、ClearPassサーバーはクライアントにVLANとACLを割り 当てます。クライアントの初期VLANは1308で、認可VLANは1309です。



使用されているソフトウェアバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成および確認されています。

ハードウェア	ソフトウェアのバージョン
WX5540Hアクセスコントローラ	R5444P03
WA5320アクセスポイント	R5444P03
Aruba ClearPassサーバー	CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf

制約事項とガイドライン

APの背面パネルに表示されているシリアルIDを使用して、APを指定します。

手順

()重要:

この設定例では、ClearPassサーバーでの802.1Xによるクライアントの認証、および認証されたクライ アントへのVLANとACLの割り当てに関連する主な設定だけを説明します。基本的なネットワーク設定と 基本的なWLAN設定については、デバイスとサーバーのマニュアルを参照してください。

ACの設定

ClearPassという名前のRADIUSスキームを作成し、ユーザー認証とアカウンティング用に8.1.1.171の ClearPassサーバーを指定して、暗号化された文字列h3cを共有キーに設定します。

#

radius scheme clearpass primary authentication 8.1.1.171 primary accounting 8.1.1.171 key authentication cipher \$c\$3\$y9gLDgP10B8T9ry5u3AHTHOadEYI7g== key accounting cipher \$c\$3\$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ== user-name-format without-domain #

```
#ユーザー認証、認可、アカウンティングにRADIUSスキームのclearpassを使用するように、ISPドメイン
        のclearpassを設定します。
        #
        domain clearpass
          authentication default radius-scheme clearpass
          authorization default radius-scheme clearpass
          accounting default radius-scheme clearpass
        #
       #EAPリレーを使用して802.1Xクライアントを認証するようにACを設定します。
       [AC] dot1x authentication-method eap
       #サービステンプレートh3c-dot1xを作成し、そのSSIDをh3c-dot1xに設定し、認証モードを802.1X認証
       に設定して、認証ドメインclearpassを指定します。
        #
        wlan service-template h3c-dot1x
          ssid h3c-dot1x
          akm mode dot1x
          cipher-suite ccmp
          security-ie rsn
          client-security authentication-mode dot1x
          dot1x domain clearpass
          service-template enable
        #
       #手動APを設定し、サービステンプレートh3c-dot1xをAPの無線にバインドします。
        #
        wlan ap ap1 model WA5320
          serial-id 219801A0YD8171E04018
          radio 1
            radio enable
            service-template h3c-dot1x vlan 1308
          radio 2
            radio enable
            service-template h3c-dot1x vlan 1308
        #
       #スイッチに接続されているポートのリンクタイプをトランクに設定し、クライアントのVLAN内のトラフィック
        がポートを通過できるようにします。
        [AC] vlan 1308 to 1309
        #
        interface Ten-GigabitEthernet1/0/26
          port link-type trunk
          port trunk permit vlan all
        #
        # ACL 3001を設定します。
        #
        acl advanced 3001
          rule 0 deny ip destination 40.8.0.119 0
          rule 5 permit ip
        #
スイッチの設定
```

#VLAN 1308と1309、およびVLANインターフェース1308と1309を作成し、VLANインターフェースにIP アドレスを割り当てます。スイッチは、認証を通過する前にVLAN 1308を使用してクライアントにパケット

```
を転送し、認証を通過した後にVLAN 1309を使用してクライアントにパケットを転送します。ACに接続さ
れているポートのリンクタイプをトランクに設定し、クライアントのVLAN内のトラフィックがポートを通過で
きるようにします。
[Switch] vlan 1308 to 1309
#
interface Ten-GigabitEthernet0/0/35
  port link-type trunk
  port trunk permit vlan all
#
interface Vlan-interface1308
  ip address 40.8.0.1 255.255.0.0
#
interface Vlan-interface1309
  ip address 40.9.0.1 255.255.0.0
#クライアントにIPアドレスを割り当てるためのDHCPアドレスプールvlan1308およびvlan1309を設定しま
す。
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
dhcp server ip-pool vlan1309
  gateway-list 40.9.0.1
  network 40.9.0.0 mask 255.255.0.0
  dns-list 40.9.0.1
#
```

ClearPassサーバーの設定

1. ClearPassサーバーにログインします。

#サーバーのWebインターフェースにアクセスするには、WebブラウザのアドレスバーにClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。

```
図22 ClearPassへのログイン
```



ClearPass Policy Managerをクリックします。表示されたページで、ログインユーザー名とパスワードを入力し、Log Inをクリックします。

aruba	ClearPass Policy Manager
	You have 83 day(s) to activate the product
	Activate Now
	Admin Login
	Username:
	Log In
Copyright 2020 Hewlett Packard Enterprise Development LP	

図23 ClearPass Policy Managerへのログイン

- ClearPass Policy ManagerにACを追加します。
 #左側のナビゲーションペインで、Configuration > Network > Devicesを選択します。開いたページで、右上隅にあるAddをクリックします。
 - a. ACでIPアドレス40.1.1.56/24を指定します。 ClearPassサーバーがこのIPアドレスに到達できることを確認します。
 - b. RADIUS共有秘密を設定します。

ここで指定した共有シークレットが、AC上のRADIUSサーバーに指定した共有キーと同じである ことを確認します。この例では、共有シークレットはh3cです。

- **c.** ベンダー名H3Cを選択します。
- d. Addをクリックします。

図24 デバイスの追加

aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration = Network = Devices	
Monitoring	Network Devices	🛶 Add
Configuration	Community of the second s	Evport All
Service Templates & Wizards		Discovered Devices
- 🛱 Services	A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.	
E 🔒 Authentication		
- Q Methods	Filter: Name v contains v Go Clear Filter	Show 20 v records
0 Identity	# Add Device 0	
Single Sign-On (SSO)	1. Dwice SUBP and Settings SUBP Wile Settings CLI Settings Opcompet Enforcement Attributes	
- C Local Users	2. Levice Simp Read Settings Simp Write Settings CLL Settings OnConnect Enforcement Authorites	
- 🛱 Endpoints	3. Name: AC	
- C Static Host Lists	Showing 1- P or Subnet Address: 40.11.5624 (a. a. 192.168.1.10 or 102.168.1.1/24 or 192.168.1.1/24 or 192.168.1.1/24 or 2001.db8:a0b:12f0::1)	
12 Role Mappings	Description:	
E B Posture		
🗄 💈 Enforcement		
- 🗘 Policies	RADIUS Shared Secret: Verify:	
Profiles	TACACS+ Shared Secret: Verify:	
- The Network	Vendor Name: H3C Vendor Name:	
Device Groups	Enable RADIUS Dynamic Authorization:	
- C Proxy Targets	Enable RadSec:	
- 🛱 Event Sources		
Retwork Scan		
- La Policy Simulation		
	Add Cancel	

3. ユーザーの追加:

#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたペ ージで、右上隅にあるAddをクリックします。

- a. ユーザーID、名前、およびパスワードをh3c1xに設定します。
- b. 事前定義済ロールEmployeeまたはユーザー定義済ロールを選択します。この例では、事前定 義済ロールEmployeeが選択されています。
- c. Addをクリックします。

図25 ユーザーの追加

aruba			ClearPass Policy Manager		Menu 🗮
Dashboard	Configuration » Identity » I	ocal Users			
Monitoring	 Local Users 				🚽 Add
Se Configuration	0				A Import
C Service Templates & Wizards					Account Settings
- i's Services	ClearPass Policy Manager I	sts all local users in the Loc	al Users page.		
- Authentication					
- 🗘 Methods	Filter: User ID	vil containe vil	Go Clear Eiltor		Show 20 v records
- 🛱 Sources		Add Local User		Pole	Statur
🚽 🧕 Identity				[Ferelevel]	Status
Single Sign-On (SSO)		User ID:	h3c1x	(Employee)	Enabled
Q Local Users	2. 0 1000030-	Name:	h3c1x	[Employee]	Enabled
- Q Endpoints	3. 🗆 h3cporta	Paremordu		[Employee]	Enabled
- Ch Boles	4. Li leader	Pasanoru.		leader-role	Enabled
-C Role Mappings	5. U yuandon	gqi Verify Password:		[Employee]	Enabled
- IP Posture	6. 🗌 yuandon	Enable User:	(Check to enable user)	[Employee]	Enabled
a S Enforcement	Showing 1-6 of 6	Change Password:	(Check to force change password on next TACACS+ login)		Export Delete
- Q Policies		Role:	[Employee]		
			Attributes		
Q Devices		Attribute	Value	() · · · · · · · · · · · · · · · · · ·	
Device Groups		1. Click to add			
- Q Proxy Targets					
- Li Event Sources					
- Salicy Simulation					
ap roncy on one of					
			Add Cancel		
		The second s			
Administration	0				
Automation and a second					

4. enforcementプロファイルを追加します。

#左側のナビゲーションペインで、Configuration > Enforcement > Profilesを選択します。開いたペ ージで、右上隅にあるAddをクリックします。

図26 Enforcementプロファイルの追加

aruba			C	learPass Policy Manager	,	Menu 🔳
Dashboard O	Configurat	tion » I	Enforcement » Profiles			
Monitoring 0	Enforce	eme	at Profiles			Add
& Configuration	Linores	enner	it fromes			Import
A Service Templates & Wizards	Each only		t calles contains opforcomont profiles that ma	tch conditions (calo northern and time) to a	stions (anforesement availies)	Export All
- D Services	Egenemon		a poncy contains can be contain promos that ma	ter conditions (role) postare, one time, to o	terms (endocement bromes)	
E Authentication	Elitor: Nar	10.0	v containe v h2d	Go Clear Filter	Show 20	▼ records
🖧 Methods	Pilcer. [ive		· [contains ·]risq		Received at the	
- 🛱 Sources			Name A	Туре	Description	
🖹 🚨 Identity	1.	0	ACL for h3c	RADIUS	pun	
-g single sign-on (SSO)	2,	0	disconnect for h3c	RADIUS_COA	puii	10.0
- La Local Users	3.	-	[H3C - Bounce Switch Port]	RADIUS_COA	System-defined profile to bounce the switch port on H3C products (including HPE FlexNetwork / Comwa	are).
-r'i Static Host Lists	4.	U	[H3C - Disable Switch Port]	RADIUS_CoA	System-defined profile to disable the switch port on H3C products (including HPE FlexNetwork / Comwa	are).
- C Roles	5.	-	h3c Guest Bandwidth Limit	Post_Authentication	System-defined profile to set Guest bandwidth limits	
Role Mappings	6.		h3c Guest Do Expire	Post_Authentication	Enforcement profile for Guest do expire functionality	
E 🕂 Posture	7.		h3c Guest Expire Post Login	Post_Authentication	Enforcement profile for Guest expire post login functionality	
B B Enforcement	8.		h3c Guest MAC Caching	Post_Authentication	System-defined profile to update the endpoint with Guest user details	
- 🛱 Policies	9.		h3c Guest Session Limit	Post_Authentication	System-defined profile to set concurrent Guest session count	
- Drofiles	10.		h3c Guest Session Timeout	RADIUS		
- + Network	11.		[H3C - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect the user on H3C products (including HPE FlexNetwork / Comware)).
- C Devices	Showing 1	-11 of	11		Copy Export	Delete
C Event Sources						
- D Network Scan						
- Le Policy Simulation						
1						
Administration 0	1					

Profileタブで、TemplateフィールドのRADIUS Based Enforcementを選択し、h3cの名前をACL-VLANに設定します。

図27 プロファイルの構成

aruba		ClearPass Policy Manager					
Dashboard	Configuration > Enforce	configuration » Enforcement » Profiles » Add Enforcement Profile					
Honitoring	 Enforcement Press 	inforcement Profiles					
& Configuration	• Profile Attributes	Summary					
 ¹ Q Service Templates & Wizards 	Template: Name: Description:	RADIUS Based Enforcement KGL-VLAN for h3c					
Q Identity Q Single Sign-On (SSO) Q Local Users Q Endpoints	Type: Action:	RADIUS R Accept O Breject O Drop					
- ∯ Static Host Lists - ∯ Roles ⊉ Rele Mappings ⊒ ∰ Posture = ∰ Enforcement - ∯ Policies	Device Group List.	Amore of the set of th	Add New Device Group				
🚰 Administration	• Back to Enforcement	ant Profiles	Next Save Cancel				

Attributesタブで、IETF Tunnel-Type、Tunnel-Medium-Type、およびTunnel-Private-Group-Idアトリビュートを使用して認可VLAN 1309を追加し、IETF Filter-Idアトリビュートを使 用して認可ACL 3001を追加します。次に、Saveをクリックします。

図28 属性の構成

			ClearPass Policy Manage	er	Menu
Dashboard O	Configura	tion > Enforcement > Profiles > Add Enforce	ment Profile		1
Monitoring O	Enforce	ement Profiles			
Configuration	e m				
- Ö Service Templates & Wizards	Profile	Attributes Summary			
- 🛱 Services	Турс		Name	Value	
🗄 🖶 Authentication	1. Radi	US:IETF	Tunnel-Type	= VLAN (13)	16 T
- 🛱 Methods	2. Radii	us:IETF	Tunnel-Medium-Type	= IEEE-802 (6)	HD 2
- Q Sources	3. Radi	us:IETF	Tunnel-Private-Group-Id	= 1309	1921 日
- Gindle Sign-On (SSO)	4. Radi	us:IETF	Filter-Id (11)	= 3001	B *
- i'i Local Users	5. Click	to add			
- 🛱 Endpoints					
- 🛱 Static Host Lists					
- 🛱 Roles					
- 22 Role Mappings					
- & Enforcement					
2 Policies					
- 🛱 Profiles	1				
- + Network					
- Q Devices					
- g Device Groups					
- 1 Event Sources					
- D Network Scan					
- D Policy Simulation					
	& Back	to Enforcement Profiles			Next -> Save Cancel
Administration 0	Duck	to Enforcement Promes			HEAT
aruba			ClearPass Policy Manage	er	Menu 🗮
Orubo Dashboard	Configurat	tion > Enforcement > Profiles	ClearPass Policy Manage	er	Menu 🗮
aruba 3 pashboard •	Configurat	tion » Enforcement » Profiles	ClearPass Policy Manage	er	Menu 🚞
Dashboard Monitoring	Configurat Enforce	tion > Enforcement > Profiles	ClearPass Policy Manage	er	Menu Add
Dashboard Monitoring Configuration	Configurat Enforce	tion » Enforcement » Profiles ement Profiles	ClearPass Policy Manage	er	Menu → Add ▲ Import & Export All
Carlboard Construction Construc	Configurat Enforce	tion = Enforcement = Profiles ement Profiles	ClearPass Policy Manage	OF rofile "ACL-VLAM for h2c" added	Menu Add Anport Export All
Confloration	Configurat Enforce	tion * Enforcement * Profiles ement Profiles rcement policy contains enforcement profile	ClearPass Policy Manage	CP rofile "ACL-VLAN for h3C" added to actions (enforcement profiles).	Menu Add Aimport Export All
Daskboard Daskboard Daskboard Configuration Oscillates & Wizards Oscillates & Wizards Oscillates & Wizards Oscillates	Configurat Enforce Each enfo	tion » Enforcement » Profiles ement Profiles reement policy contains enforcement profile	ClearPass Policy Manage Enforcement pr as that match conditions (role, posture, and time)	OF rolle "ACL-VLAN for h3c" added to actions (enforcement profiles).	Menu Add A Import Export All
Datableed Monitoring Monitoring Monitoring O Service Emplotes & Wizards O Service Automatics O Service Automatics O Service O Methods O Services	Configurat Enforce Each enfor	tion » Enforcement » Profiles ement Profiles reement policy contains enforcement profile ne v[contains v]h34	ClearPass Policy Manage	CF rofile "ACL-VLAN for h3c" added to actions (enforcement profiles).	Menu Add Show 20 • records
Orubbo Databased Ø Hankorkø Ø Services Ø tentity	Configurat Enforce Each enfo Filter: Nar	tion = Enforcement = Profiles ement Profiles reement policy contains enforcement profile ne v(contains v)h2(ClearPass Policy Manage Enforcement pu as that match conditions (role, posture, and time) a concurrence of the conditions of the conditions a concurrence of the conditions of the condition	Profile "ACL-VLAN for h30" addad to actions (enforcement profiles). Description	Manu Add Show Zo v records
Datableard Datableard Wandbring © Configuration Q Service Emplotes & Witards Q Sarvice Employee (Sign-On (Sign))	Configurat Enforce Each enfor Filter: Nar 1.	tion + Enforcement + Profiles ement Profiles recement policy contains enforcement profile ne v (centains v) hold Act, (r + No:	ClearPass Policy Manage Enforcement pr as that match conditions (role, posture, and time) (2) Co Clear Filter Prep RoDio	Profile "ACL-VLAN for h3c" added to actions (enforcement profiles), Description put	Manu Add Mimport Show 20 V recards
Orubbo Ibashoard ● Manaboring ● Q Service ● Q Methods ● Q Service ● Q Service ● Q Service ● Q Service ● Q Localy ● Q Localy Letters ●	Configurat Enforce Each enfor Filter: Nar 1. 2.	ten + Enforcement + Profiles ement Profiles rcement policy contains enforcement profile ne v(centains v)hdj Name - Act_VLM for hbc	ClearPass Policy Manage Enforcement pu es that match conditions (role, posture, and time) Co Coust Pitter Rocius Rocius Rocius	er roffie "ACL-VLAN for h30" addad to actions (enforcement profiles). Description pull	Manu Add Show Zo v records
Databaerd Databaerd Databaerd Definition Databaerd Definition Databaerd Definition	Configurat Enforce Each enfo Filter: Nar 1. 2. 3.	tion + Enforcement + Profiles ement Profiles rearnent policy contains enforcement profile ne v (contains v)hid Act, for hic Act, for hic discomet for hic	ClearPass Policy Manage	Crofile "ACL-VLAN for h3c" added to actions (enforcement profiles). Description pull	Manu Add Amort Export All Show (20 v) records
Orubbo ■ Menhoring ● Menhoring ● Service Templates & Witzards ● Service Templates & Witzards ● Service Templates & Witzards ● Service Service ● Service Service Service ● Least Unarre ● Service S	Configural Enforce Each enfor Filter: Nar 1. 2. 3. 4.	ten » Enforcement » Profiles ement Profiles resement policy contains enforcement profile ne v) (centains v) hdj Name - ActivuAuf for hbc disconnect for hbc	ClearPass Policy Manage Enforcement pu as that match conditions (role, posture, and time) (2) Col Color State Racius Racius Racius Racius Racius Racius Racius Racius Racius Racius Racius Racius Racius Racius Racius	er roffie "ACL-VLAN for h32" addad to actions (enforcement profiles). Description pull pull pull pull pull pull pull pul	Manu Add Show 20 V records ding HPE Flextetwork / Comware).
Databard Databard Databard Definition Databard Definition	Configurat Enforce Each enfo Filter: Nar 1. 2. 3. 4. 4.	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile mever vicentains vicentains vicentains ACL for h3c ACL for h3c decomet for h3c decomet for h3c (Mucr- Boance Switch Port] (Mucr- Boance Switch Port]	ClearPass Policy Manage Enforcement pu as that match conditions (role, posture, and time) to Constraine Radius Ra	Crofile "ACL-VLAN for h3c" added to actions (enforcement profiles). Description pull pull System-defined profile to disable the switch port on H3C products (inclu System-defined profile to disable the switch port on H3C products (inclu	Manu Add Minort Show 20 v records Show 20 v records ding HPE FlaxNetwork / Comware). ding HPE FlaxNetwork / Comware).
Outbloc ■ Mentering ● Mentering ● Service Traplate & Witzards	Configurat Enforce Each enfo Filter: Nar 1. 2. 3. 4. 5. 6.	ten + Enforcement + Profiles ement Profiles resement policy contains enforcement profile a <u>vocentains vocentains vocentains vocentains</u> Activutual for his disconnect for his (Hor - Cinable Switch hord) (Hor - Cinable Switch hord)	ClearPass Policy Manage	er rollie "ACL-VLAN for h32" addad to actions (enforcement profiles). Description pull pull pull System-defined profile to bounce the anitch port on H3C products (inclu System-defined profile to dauble the anitch port on H3C products (inclu System-defined profile to dauble the anitch port on H3C products (inclu System-defined profile to adubb the anitch port on H3C products (inclu System-defined profile to adubb the anitch port on H3C products (inclu System-defined profile to adubb the anitch port on H3C products (inclu System-defined profile to adubb the anitch port on H3C products (inclu System-defined profile to adubb the anitch port on H3C products (inclu System-defined profile to adubb the anitch port on H3C products (inclu	Menu Add Show 20 V records ding HPE Flashetwork / Comware). ding HPE Flashetwork / Comware).
Dasboard Destouring Des	Configurat Enforce Each enfor Filter: Nar 2. 3. 4. 5. 6. 7.	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile me v (contains v) high Mana v (contains v) high Act-VLAM for his discomet for his discomet for his (HaC - Bounce Switch Port) his Coast Bandwidth Limit his Coast Bandwidth Limit	ClearPass Policy Manage	Confine *ACL-VLAN for h3c* added To actions (enforcement profiles).	Manu Add Import Show 20 v records Show 20 v records ding MPE FlaxNetwork / Comware). Sing MPE FlaxNetwork / Comware).
Outboot Datablead Manaboring Ø Manaboring Ø Service Traplates & Witzards Ø Service Traplates & Witzards Ø Service Traplates & Witzards Ø Methods Ø Service Services Ø Local Users Ø Stadic Host Lists Ø Role Nappings	Configurat Enforce Each enfor Filter: Nar 1. 2. 3. 4. 5. 6. 7. 8.	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile excement policy contains enforcement profile excement policy contains enforcement profile excement for hic disconsector h	ClearPass Policy Manage Enforcement pp as that match conditions (role, posture, and time) (a) Co ClearTime Racitus	Profile "ACL-VLAN for h32" added to actions (enforcement profiles). Description pull pull pull System-defined profile to bounce the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profile to disable the switch port on H3C products (Inclu System-defined profil	Manu Add Show 20 V records Show 20 V records ding HPE FlexNetwork / Comware). ding HPE FlexNetwork / Comware).
Dasbbord Destbord	Configurat Enforce Each enfor 1. 2. 3. 4. 5. 6. 7. 8. 9.	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile ten ten ten ten ten ten ten t	ClearPass Policy Manage Enforcement p to that match conditions (role, posture, and time) to that match conditions (role, posture, and time) to the conditions (role, posture, and time) RADIUS_COA RADIUS R	er roffle "ACL-VLAN for h3c" added to actions (enforcement profiles):	Manu Add Import Show 20 records Show 20 records ding MPE FlexNetwork / Comware). ding MPE FlexNetwork / Comware).
Outboo Interface	Configural Enforce Each enfor Filter: Nar 1. 2. 3. 4. 5. 6. 7. 8. 9. 9. 10.	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile reement policy contains enforcement profile ten contains enforcement profile contains enforc	ClearPass Policy Manage	Pr For ACL-VLAN for h32* added for actions (endorcement profiles).	Manu Add Import Show 20 v records ding MPE FlexNetwork / Comware). ding MPE FlexNetwork / Comware).
Orubbo ■ Mankorids ● Ø Service Templates Witands ● Service Templates Witands ● Ø Service Templates ●	Configurat Enforce Each enfor Filter: Nar 4. 5. 6. 7. 8. 9. 10.	ten + Enforcement + Profiles ement Profiles creament policy contains enforcement profile te texture	ClearPass Policy Manage Enforcement pu as that match conditions (role, posture, and time) as that match conditions (role, posture, and time) as conclusted as the second seco	er rolle "ACL-VLAN for h3C" added to actions (enforcement profiles).	Manu Add Import Show 20 records Show 20 records sing HPE FlexNetwork / Commare). Sing HPE FlexNetwork / Commare).
Outboot Interface	Configurat Enforce Each enfo Filter: Nar 1, 2, 3, 4, 5, 6, 7, 6, 7, 8, 9, 10, 11, 11,		ClearPass Policy Manage	Profile "ACL-VLAN for h3g" added To actions (endorcement profiles). Poscofiption pul pul pul pul pul pul pul pul	Manu Add Import Show 20 v records ding HPE FlexNetwork / Comware). ding HPE FlexNetwork / Comware).
Orubbo ■ Monitoring ● Monitoring ● Service Traplate & Witands ● Prove Traplate & Witands ● Prove Traplate & Witands ● Prove Traplate & Witands	Configural Enforce Filter: Nar 1. 2. 3. 4. 5. 6. 9. 10. 10. 11. 11. 12.	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile ten ten ten ten ten ten ten t	ClearPass Policy Manage	er rolle "ACL-VLAN for h32" addad to actions (enforcement profiles).	Here Add Impot Export All Show 20 • records ding HPE FlexNetwork / Commare), ding HPE FlexNetwork / Commare), HPE FlexNetwork / Commare),
Concision Interface	Configurat Enforce Each enfor Filter: Nar 4 5. 6. 7, 8. 9, 10. 11. 12. Showing 1	ten + Enforcement + Profiles ement Profiles ement Profiles reement policy contains enforcement profil ten Contains enforcement profil ACL Profile ACL Profi	ClearPass Policy Manage	er roller *ACL-VLAN for h3g* added to actions (endorcement profiles). Pusciption pull pull pull pull pull pull pull pul	Manu Add Import Show 20 v records Show 20 v records ding HPE FlexNetwork / Comware). ding HPE FlexNetwork / Comware). g HPE FlexNetwork / Comware). Comy Espott Delate
Image: Stand	Configural Enforce Each enfo Filter: Nar 1, 2, 3, 4, 5, 6, 6, 7, 8, 9, 9, 10, 11, 11, 2, Showing 1	ten + Enforcement + Profiles ement Profiles resenent policy contains enforcement profile ten ten ten ten ten ten ten ten ten t	ClearPass Policy Manage Enforcement per es that match conditions (role, posture, and irme) C C C Cest Filter RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA	Profile "ACL-VILM for h3c" addad to actions (enforcement profiles). Proceepison pull pul pul pul pul system-defined profile to bounce the switch port on H3C products (including system-defined profile to bounce the switch port on H3C products (including system-defined profile to decise to aprile functionality for Enforcement profile for Guarts do expire functionality for Enforcement profile to guarts endpoint with Guart user details system-defined profile to act concurrent Guart seasion count System-defined profile to decisent the user on H3C products (including	Here Add Impot Export All Show 20 • records ding HPE FlexNetwork / Comware). Sng HPE FlexNetwork / Comware). Cony _ Export _ Dates
Imathematic Imathematic Image: Second Sec	Configurat Enforce Each enfo 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. Showing 1	ten + Enforcement + Profiles ement Profiles resement policy contains enforcement profile e v centains enforcement profile ACL for his ACL for h	ClearPass Policy Manage Enforcement p to be that match conditions (role, policitier, and terme) to be that match conditions (role, policitier, and terme) RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA RADIUS_COA	Confine *ACL-VILAN for h3c* added To actions (enforcement profiles):	Add import Show 2 v records ding MPE FlaxNetwork / Comware). g MPE FlaxNetwork / Comware). Copy Espoit Delete
Imatabased Imatabased Imatabased I	Configurat Enforce Each enfor 1. 2. 3. 4. 5. 6. 7. 8. 8. 9. 10. 11. 12. Showing 1	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile Remer Contains	ClearPass Policy Manage Enforcement p as that match conditions (role, posture, and time) as that match conditions (role, posture, and time) a condition of the second	er rolls "ACL-VLAN for h2c" addad to actions (enforcement profiles). Percorption pull pul pul pul pul comparison of the source the switch port on H2C products (includ system-defined profile to bounce the switch port on H2C products (includ system-defined profile to disable the switch port on H2C products (includ system-defined profile to Guest do expire functionality Enforcement profile for Guest do expire functionality Enforcement profile to Guest do expire functionality Enforcement profile to Guest do expire functionality System-defined profile to satisfy the expire functionality System-defined profile to disconnect the user on H3C products (including	Here Add Import Show 20 • records ding HPE FlexNetwork / Comware). ding HPE FlexNetwork / Comware). Coxy Export Dates
Imathematic Imathematic	Configurat Enforce Each enfo 1. 2. 3. 4. 5. 6. 7. 7. 8. 9. 10. 11. 12. Showing 1	ten + Enforcement + Profiles ement Profiles resenent policy contains enforcement profile e v centains enforcement profile ACL for Ibic ACL for Ibic Context Ibic Policy Ibic Const Handwidth Linni Dir Colest Back Policy Dir Colest Policy Dir Colest Back Policy Dir C	ClearPass Policy Manage	er rofile *ACL-VLAN for h3c" added to actions (enforcement profiles):	Add import Show 2 reards Show 2 reards ding MPE FlaxNetwork / Comware). g MPE FlaxNetwork / Comware). Cory Export Dates
Imatabased I	Configurat Enforce Each enfor 1. 2. 3. 4. 4. 5. 6. 7. 8. 9. 9. 10. 11. 12. Showing 1	ten + Enforcement + Profiles ement Profiles ecement policy contains enforcement profile ten + Enforcement profile ten + Contains enforcement profile ten + Contains enforcement profile Act-VuAl for hac disconset for hac (Hor - Ginashe Switch Port] Act - Contains eskitch Port] - Act - Terminate Section Timeut - Act - Contains eskitch Port] - Act	ClearPass Policy Manage Enforcement p a construction of the sector of	er rolls "ACL-VLAN for h32" addad to actions (enforcement profiles). Percorption pull pull pull pull pull pull pull pul	Here Add Import Show 20 • records ding HPE FlexNetwork / Comware). ding HPE FlexNetwork / Comware). Coxy Export Dates
Imatabased Imatabased Imatabased I	Configurate Enforce Filter (Nater 3. 4. 4. 5. 6. 7. 7. 8. 9. 10. 11. 12. Showing 1	ten + Enforcement + Profiles ement Profiles resenent policy contains enforcement profile e v contains enforcement profile ACL for his ACL for hi	ClearPass Policy Manage	er rofile "ACL-VLAN for h3c" added to actions (enforcement profiles).	Add import Show 2 reards Show 2 reards ding IPE FlexNetwork / Comware). g IPE FlexNetwork / Comware). Copy Export Dates
Imatabased Imatabased Imatabased I	Configuration	Iden + Enforcement + Profiles ement Profiles reement policy contains enforcement profile Reement policy contains enforcement profile Reement policy contains enforcement profile Act-VAU for h2c discussed to the policy Act-VAU for h2c discussed to the policy h2c Casta Book Profile h2c Casta Book Profile h2c Casta Book Timed h2c Casta Book T	ClearPass Policy Manage	er rolls "ACL-VLAN for h32" addad to actions (enforcement profiles).	Here Add Import Show 20 V records ding MPE FlexNetwork / Comware). ding MPE FlexNetwork / Comware). (Cory Export Delete)
Dachboard Dachboard Dachboard Defention	Configuration	ten + Enforcement + Profiles ement Profiles resenent policy contains enforcement profile ne vocatains enforcement profile ACL (nr his ACL (nr hi	ClearPass Policy Manage Enforcement p es that match conditions (role, posture, and time) C C Clear Part RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA RADIUS_CA	er rolle *ACL-VLAN for h3C* addad to actions (enforcement profiles).	Here Add Import Show 2 records Show 2 records ding HPE FlexNetwork / Commans). g HPE FlexNetwork / Commans). Coxy Paport Online
Imatabased	Configuration 2015 Each enforce Each enforce 1. 2. 3. 4. 4. 5. 6. 7. 7. 8. 9. 9. 10. 11. 12. 2. 5. 8. 9. 9. 3. 3. 4. 5. 5. 6. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5.	ten + Enforcement + Profiles ement Profiles ecement policy contains enforcement profile ecement policy contains enforcement profile enderse e	ClearPass Policy Manage	er rollie "ACL-VLAN for h2c" addad to actions (enforcement profiles).	Here Add Import Export All Show 20 V records ding HPE FlexNetwork / Comware). ding HPE FlexNetwork / Comware). Cony Export Delay
Dachbord Dachbord Dachbord Decomposition Deco	Configuration of the second se	ten + Enforcement + Profiles ement Profiles reement policy contains enforcement profile Rement Remer + Contains + C	ClearPass Policy Manage	er rolls "ACL-VLAN for h32" addad to actions (enforcement profiles).	Henu Add Import Export All Show 20 records ding HPE FlexNetwork / Commare). Grupy Export Dates

5. 適用ポリシーを追加します。

#左側のナビゲーションペインで、Configuration > Enforcement > Policiesを選択します。表示され たページの右上隅にあるAddをクリックします。

図29 Enforcementポリシーの追加

aruba			ClearPass Policy Manage	er	Menu 🗮
Dashboard	O Configura	ration » Enforcement » Policies			
Monitoring	Enforce	cement Policies			🛶 Add
& Configuration	0				A Import
12 Service Templates & Wizards	ClearDas	es controls national access hu pualuation an enforce	ament noticy accordated with the service		Export All
- Ö Services	Creatives.	so contrast network occess by crossening on emote	inchi ponej associata inti ne scriter		
🗉 🔓 Authentication 👘	Filter: N	ame v contains v	Go Clear Filter		Show 20 v records
ាជ្នុះ Methods	Pilter			- Descalation	
- C Sources		Name x	туре	Description	
🗉 🚨 Identity	1.	ACL for h3c	RADIUS	pui	
- g single sign-on (SSO)	2.	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin	
C Endopints	3.	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices	
	4.	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device	
- Roles	5.	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network	
🗘 Role Mappings	6.	Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application	
🗄 🖶 Posture	7.	□ h3c Guest Access Enforcement Policy	RADIUS		
B Enforcement	8.	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application	
-Q Policies	9.	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access	
- I Profiles	10.	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access	
- Devices	11.	task4-802.1x-enforcement-policy	RADIUS		
- Device Groups	Showing	1-11 of 11			
- 🛱 Proxy Targets					
- 🛱 Event Sources					
- 🛱 Network Scan					
- 🛱 Policy Simulation					
Administration	0				

Enforcementタブで、h3cの名前をACL-VLANに設定し、h3cのACL-VLANを選択します。 をデフォルトプロファイルとして使用します。

図30 ポリシーの構成

		ClearPass Policy Manager	Menu 🔤
Dashboard C	Configuration > Enforcem	ent » Policies » Add	
Monitoring C	Enforcement Poli	ties	
Configuration	Enforcement Rules	Summary	
🖓 Service Templates & Wizards	Name:	ACL-VLAN for h3c	
- i Services	Description:		
- C Methods			
- 🛱 Sources	Enforcement Type:	DADTUE O TACACE+ O WEBAUTH (SIMME/Agent/CL1/CoA) O AppEration O Event	
🗊 🧟 Identity	Default Profile:	KHOLOS O IACKCST O WEDROTH (SWIP)/Agen/CCL/COX) O Approation O Event	Add New Enforcement Profile
C Dool Velles C Endpoints C			
Administration OPUDO ■ Dashboard ●	Back to Enforcemen Configuration > Enforcemen	t Policies ClearPass Policy Manager	Not Save Cancel
Monitoring 0	Enforcement Polici	es	
Configuration	Enforcement Rules	Summary	
A Condex Templetes & Missade			
- A service remplates & wizards	Name:	ACL-VLAN for h3c	
- A service remplates & wizards - 🔆 Services	Name: Description:	ACL-VLAN for h3c	
	Name: Description:	ACL/VLAN for hDc	
↓ Services templates & Wizards ↓ Services ⊕ Authentication ↓ Services ↓ Sources	Name: Description: Enforcement Type:	ACL/VLAN for htsc	
Genvice templates & Wizards Genvice Genvi	Name: Description: Enforcement Type: Default Profile:	AGL/VLAN for his:	Add New Enforcement Profile
Quervice templates & witards Quervices Querv	Name: Description: Enforcement Type: Default Profile:	ACL/VLAN for Noc RADIUS O TACACS+ O WEBAUTH (SNMP/Agent/CLUCoA) O Application O Event ACL/VLAN for INC V Web Details Koolly	Add New Enforcement Profile
Convex reinplates & witards Convextore	Name: Description: Enforcement Type: Default Profile:	ACL-VLAN for Noc ACLACLEN O NUEBAUTH (SMMP/Agent/CLUCOA) O Application O Event ACLAULAN for Ib: View Distails Modify	Add New Enforcement Profile
Lorenvice templates a writares Janices Autoritation Arethonication Orethones Detactions Outors Out	Name: Description: Enforcement Type: Default Profile:	ACL/KAN for Not RADIUS O TACACS+ O WEBAUTH (SINNP/Agent/CLI/CoA) O Application O Event RCL/KAN for Not Vow DitBlin ModBy	Add New Enforcement Profile
Orenvices	Name: Description: Enforcement Type: Default Profile:	ACL/VLAN for Ibc	Add New Enforcement Profile
John (Brighted & Withold S Service John (Brighted & Withold S John (Brighted S Service John (Brighted S Jo	Name: Description: Enforcement Type: Default Profile:	Image: Activitian Ser Disc. Image: Second Ser Disc. Image: Second Secon	Add New Enforcement Profile
Jorn vice Impletes a vitares Jorn vice Jorn	Name: Description: Enforcement Type: Default Profile:	ACL/KAN for Not RADIUS O TACACS+ O WEBAUTH (SINNP/Agen/CLUCOA) O Application O Event (ACL/KAN for Not) Vow Dictality ModBy	Add New Enforcement Profile
Convices	Name: Description: Enforcement Type: Default Profile:	ACL-VLAN for Noc # RADIUS O TACACS* O WEBAUTH (SMMP/Agen/ICLUCAS) O Application O Event ACL-VLAN for Noc V Wood Dealshs Modify	Add New Enforcement Profile
Januaria (ampiada a vitanda Januaria) Januaria Januariaria Januariariaria Januaria Januariariaria Januariaria Januaria J	Name: Description: Enforcement Type: Default Profile:	AGLIVLAN for hitz RADIUS O TACACS+ O WEBAUTHI (UNHPH/Agent/CLUCAS) O Application O Event AGLIVLAN for hit: V Web Hitshin Modify:	Add New Enforcement Profile
U per vice i demplatés a vitatrás je per vices a justification O retentos O per des D anoles O per des O per des	Name: Description: Enforcement Type: Default Profile:	ACL/KAN for Not RADIUS O TACACS+ O WEBAUTH (SINNP/Agent/CLI/CoA) O Application O Event CACL/KAN for Not Vow Dutable ModBy	Add New Enforcement Profile
Jornes Jorden Status	Name: Description: Enforcement Type: Default Profile:	# RADIUS O TACACS* O WEBAUTH (SMM9/Agen/ICLI/CAS) O Application O Event # RADIUS O TACACS* O WEBAUTH (SMM9/Agen/ICLI/CAS) O Application O Event # RADIUS O TACACS* O WEBAUTH (SMM9/Agen/ICLI/CAS) O Application O Event # RADIUS O TACACS* O WEBAUTH (SMM9/Agen/ICLI/CAS) O Application O Event # RADIUS O TACACS* O WEBAUTH (SMM9/Agen/ICLI/CAS) O Application O Event # RADIUS O TACACS* O WEBAUTH (SMM9/Agen/ICLI/CAS) O Application O Event # RADIUS O TACACS* O WEBAUTH (SMM9/Agen/ICLI/CAS) O Application O Event	Add New Enforcement Profile
Jan vice Implets a vitates Jan vice	Name: Description: Enforcement Type: Default Profile:	ACLIVLAN for hits RELIVLAN for hits RELIVLAN for hits Konty Konty Konty Konty Konty Konty Konty K	Add New Enforcement Profile
Jervices Jervices Jervices Justices	Name: Description: Enforcement Type: Default Profile:	ACL/KAN for h0x RADIUS O TACACS+ O WEBAUTH (SINNP/Agen/CLUCAA) O Application O Event (ACL/KLNN for h0x) Yow Distable Roothy	Add New Enforcement Profile
Jan Kangel (angledes a Witholds Jan Kangel	Name: Description: Enforcement Type: Default Profile:	RACL/RAN for Ibx Image: Contracts - O WEBAUTH (SMMP/Agent/CLUCAS) O Application O Event RACL/RLAN for Ibc View Details Modify	Add New Enforcement Profile
Jervice Jervices	Name: Description: Enforcement Type: Default Profile:	ACLIVEAN for hitz RELIVEAN for hitz RELIVEAN for hitz	Add New Enforcement Profile
Jervices Jervices Justices	Name: Description: Enforcement Type: Default Profile:	ACL/KAN for h0x RADIUS O TACACS+ O WEBAUTH (SINHP/Agen/CLUCAA) O Application O Event (ACL/KLNN for h0x) Yow Distable Roothy	Add New Enforcement Profile
Jan vice Implates wittans Jan vice	Name: Description: Enforcement Type: Default Profile:	AGLIVLAN for hitz RADULS O TACACS+ O WEBAUTHI (UNHPH/Agent/CLUCA) O Application O Event AGLIVLAN for hit XGLIVLAN for hit Modify	Add New Enforcement Profile
Janvices	Name: Description: Enforcement Type: Default Profile:	ACL/VLAN for h0z REUVLAN for h0z REUVLAN for h0z	Add New Enforcement Profile
Jernice (amplates vitants Jernice) Janice	Name: Description: Enforcement Type: Default Profile:	ACL/RAN for IOX RADIUS O TACACS+ O WEBAUTH (SIMMI/Agen/CLU/CAA) O Application O Event	Add New Enforcement Profile

Rulesタブで、フィルタ条件を設定し、適用プロファイルを選択します。 RADIUS:ACL-VLAN for h3cを選択し、Saveをクリックします。

図31 一致条件の設定

Dashboard		CI	earPass Policy Mana	ger	Menu
	O Configura	ation = Enforcement = Policies = Add			
Monitoring	Enford	ement Policies			
Configuration	Enforce	ment Rules Summary			
Service Templates & Wizards	Rules Eva	aluation Algorithm:	I matches		
- O Services	Enforcem	ent Policy Rules:			
- C Methods	Con	ditions		Actions	
C Sources	Duday Californi			Add Bule Conv Bule Move Un :	
Single Sign On (SSO)	Rules Editor				
Local Users			Conditions		
- 🎝 Endpoints	Match ALL of	the following conditions:			
C Static Host Lists	Type	Name	Operator	Value	
Role Mappings	1. Authen	add	Deconds_10	incom Ca o	
- 🕀 Posture	Li Garde Lo				
Enforcement					
ti Profiles					
⊒- Network			Enforcement Profiles		
Devices	Profile Name	s: [RADIUS] ACL-VLAN for h3c			
- D Proxy Targets			Move Up t		
- C Event Sources			Remove		
- Q Network Scan		Select to Add	~		
- Q Policy Simulation					
				Save Cancel	
	K Back	to Enforcement Policies			Next Save Cancel
Administration	0				
aruba		Clea	Pass Policy Manage	ir i	Menu
Dashboard	O Configuratio	n » Enforcement » Policies			
Monitoring	0 5 6				
	- Entorcer	nent Policies			🚽 Add
Configuration	 Enforcer 	nent Policies			Add
Configuration	 Enforcer 	nent Policies	Enforcement policy	"ACI -VI AN for h3c" has been added	♣ Add ♣ Import ♣ Export All
Configuration	• Enforcer	nent Policies	Enforcement policy '	'ACL-VLAN for h3c" has been added	🚽 Add 🐣 Import ዿ Export All
Configuration Q Service Templates & Wizards Q Services Authentication	ClearPass co	nent Policies	Enforcement policy '	'ACL-VLAN for h3c" has been added	교 Add 오 Import 오 Export All
Configuration C Service Templates & Wizards Services Authentication Methods	ClearPass co	nent Policies ntrols network access by evaluating an enforcement po	Enforcement policy '	'ACL-VLAH for h3C" has been added	⊯ Add ▲ Import ▲ Export All Show (20 v) records
Computation	ClearPass co	nent Policies ntrols network access by evaluating an enforcement po v[contains v] Name •	Enforcement policy ' licy associated with the service.	*ACL-VLAH for h3C* has been added	⊯ Add ≗ Import ▲ Export All Show 20 ♥ records
Configuration ↓ Service Templates & Wizards ↓ Services ↓ Surtends ↓ Surces ↓ Surces ↓ Identity ↓ J Single Sign-On (SSO)	ClearPass co	nent Policies ntrols network access by evaluating an enforcement po v contains v None • Act, for No	Enforcement policy ' licy associated with the service.	'ACL-VLAN for h3c" has been added Description puli	⊯ Add ≗ Import ≗ Export All Show 20 ▼ records
Confuguration Q Service Templates & Wizards Q Services B Juthentication ↓ Sources Q Identity ↓ Single Sign-On (SSO) ↓ Local Users	ClearPass co	nent Policies netroit access by evaluating an enforcement po contains v Netroit for take Accivitation for take	Enforcement policy ' licy associated with the service. Go Clear Filter Yype RADIUS RADIUS	'ACL-VLAN for h3C" has been added Description puli	∳ Add ≜, Ingort ≗ Export All Show 28 – ♥ records
Contrugration Oservice templates & Wizards Oservice templates & Wizards Oservice templates & Wizards Oservice Ose	ClearPass co	nent Policies ntrols network access by evaluating an enforcement po v[centains v] Kanne ACL for h3c ACL for h3c (contract work login Policy]	Enforcement policy's licy associated with the service.	ACL-VLAN for h3C* has been added Description pull Enforcement policy controlling access to Policy Manager Admin	v Add A, Import & Export All Show (29 v) records
Comparison Service Templates & Witards Services Authentication Careful Services Elemity Canal Users Canal Users	ClearPass co Filter: Name	nent Policies trols network access by evaluating an enforcement po v contains v Act, for Noc ACt, for Noc ACt, VirkAN for Noc [Admin Network Legin Policy]	Enforcement policy ' dicy associated with the service.	*ACL-VLAN for Ix3C" has been added	w Add & Import & Export All Show 22 ❤ records
© comparison © construction © Services ■ Authentication © Services ■ Construction © Services ■ Construction © Single Sign-Cin (SSO) ■ Conspirate © Conspirate © Static Host Litits © Roles ■ Construction © Ro	ClearPass co Filter: Name	nent Policies ntrols network access by evaluating an enforcement po v contains v Accuration v contains v contains v contains testwork Legin Policy] [Admin Network Legin Policy] [Admin Network Legin Policy] [Admin Network Legin Policy]	Enforcement policy * licy associated with the service. Go Clear Filer Yupe RADIUS RADIUS RADIUS TACACS TACACS	ACL-VLAN for h3c* has been added Description pul Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access for Alforcep devices Enforcement policy controlling access for Alforcep devices	⊶ Add 2, Import 2, Export All Show (20 - v) records
© comparison © service templates & Witards © Services ■ Authentication — Q services ■ Litentity ■ Concell Users — Q Single Sign-On (SSO) — Q Local Users — Q Single Sign-On (SSO) — Q Single	ClearPass co Filter: Name	nent Policies	Enforcement policy ticy associated with the service. Go Clear Filter	*ACL-VLAN for h3C* has been added Peccription pull Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Aruba device Enforcement policy controlling access to Aruba device Enforcement policy controlling access to Aruba device	w Add & Import & Export All Show 20 m records
S comparison S concernation of the second	ClearPass co Filter: Name 3. 4. 5. 6. 7.	nent Policies ntrols network access by evaluating an enforcement po contains v contains v contains v Activitation for bits Activitation bitsconnect [Andio rouse Registration Disconnect] [Andio Revise Registration Disconnect] [Coset Operatic Loging]	Enforcement policy * fility associated with the service. Clear Filter * RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS TACACS * KADIUS * RADIUS * * RADIUS * RADIUS * RADIUS * RADIUS * * RADIUS * * * * * * * * * * * * *	ACL-VLAH for h3c* has been added	w Add & Ingort & Export All Show 23 ▼ records
Comparison Constraints Constra	ClearPass co Filter: (Name 1. 2. 3. 4. 5. 6. 7. 8.	nent Policies ntrols network access by evaluating an enforcement po	Enforcement policy / licy associated with the service.	ACL-VLAN for h3c* has been added Description pul Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Anab device Enforcement policy controlling access to Guest application	w Add A, Import & Export All Show 29 v records
Comparison Conservation Conserv	ClearPass co Filter: Name 2. 3. 4. 5. 6. 7. 8. 9.	nent Policies ntrols network access by evaluating an enforcement policies Network access by evaluating an enforcement policy Accurate for has Cater access for forcement Policy Decises Access Enforcement Policy Decises Access Access Enforcement Policy Decises Access Access Enforcement Policy Decises Access Access Policy Decises Access Decises Access Decises Access Decises Access Decises Access Decises Access Decises Decises Access Decises Decises Decises Decises Decises Decises Decises Decises Decises Decises Decises Decises Decises Decises Decises Dec	Enforcement policy ' ticy associated with the service. C G Clear Harrier RaDius Ra	*ACL-VLAN for Ib3C* has been added Conscription puti Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Anba device Enforcement policy controlling access to Anba device Enforcement policy controlling access to Anba device Enforcement policy controlling access to Gest application Enforcement policy controlling access to Gest application Enforcement policy controlling access to Stable Advice Enfo	w Add & Import & Export All Show 23 ♥ records
© comparison © service Implates & Witards ○ services ■ Authentitation ■ Graindes ■ Isenity ■ Comparison ■	ClearPass co Filter: Name 3. 2. 3. 4. 5. 6. 7. 8. 9. 9.	nent Policies ntrols network access by evaluating an enforcement po	Enforcement policy / licy associated with the service. Constraints of the service of the serv	ACL-VLAN for h3c* has been added Description pul Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Anab device Enforcement policy controlling access to Guest application Enforcement policy controlling access to Susplication Enforcement policy controlling access to Insight application Enforcement policy controlling access to Insight application Enforcement policy controlling access	₩ Add ♣, Import ♣ Export All Show 20 v reords
Comparison Construction Services Impattes & Witards Construction Q Services Q Servic	ClearPass co Filter: Name	nent Policies	Enforcement policy * ticy associated with the service.	*ACL-VILAN for h3C* has been added Perception pull Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Anba device Enforcement policy controlling access to Insight application Enforcement policy to deny network access Enforcement policy to deny network access	w Add & Import & Export All Show 20 ★ records
25 Comparison 2	ClearPass co Filter Name	nent Policies ntrols network access by evaluating an enforcement po contains v ntrols network access by evaluating an enforcement policy Act, Vitab for bits Act, Act, Act, Act, Act, Act, Act, Act,	Enforcement policy * Ity associated with the service. C C Clear Plane RADIUS RADIUS TACACS KOLUS TACACS WEBAUTM RADIUS RADIUS RADIUS RADIUS	*ACL-VLAN for h3c* has been added	₩ Add ▲, Import ▲ Export All Show (20 - v) records
Comparison Service Implates & Witards O Service Authentication Q Service Services Q Service Control Q Service Control Q Services Control Q Single Sign=On (SSO) Concol Users Q Single Sign=On (SSO) Q Single Sign=On (SSO) Q Static Host Lists Q Another Sign=Service Q Mark Hospings Q Mark Hospings If For Control Q Devices Q Devices Q Devices Q Devices Q Devices Q Devices Trapes Q Portuges Trapes Q Network Start Q Devices Trapes Q Network Start Q Network Start	ClearPass co Filter; Name 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. Showing 1-1	nent Policies ntrols network access by evaluating an enforcement po V contains V Acc. for h3c Cubic for	Enforcement policy / licy associated with the service. Constraints of the service of the serv	ACL-VLAN for h3c* has been added	Add Add Armont Copy Expert Dedex
Comparison Conservation Conserv	ClearPass co Filter: Name 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 10. 11. 12. Showing 1-1	nent Policies ntrols network access by evaluating an enforcement policy Network AcctVata for ble A	Enforcement policy ' lity associated with the service. Constraints of the service of the servi	*ACL-VLAR for his" has been added	Add ▲ Import. ▲ Export All Show 20 ● records Cony Export Debre
© comparison © service Implates & Witards © services ■ Authentitation ■ Grandos ■	ClearPass co ClearPass co Piter Name 2. 3. 4. 5. 6. 7. 7. 8. 9. 9. 9. 9. 10. 11. 12. 2. 2. 3. 4. 5. 6. 7. 7. 8. 9. 9. 9. 9. 9. 9. 11. 12. 12. 12. 12. 12. 12. 12. 12. 12	ment Policies ntrols network access by evaluating an enforcement po v contains v ACLVLAR for h3c ACLVLAR for h3c (Admin Network Legin Policy] (Admin Network Legin Policy] (Admin Network Legin Policy] (Gaust Access Policy] (Gaust Access Enforcement Policy (Sample Damy Access Policy] (Sample	Enforcement publy 4 lity associated with the service. Constraints of the service RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	ACL-VLAR for h3c* has been added Description pul Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Anab device Enforcement policy controlling access to Guest application Enforcement policy controlling access to Insigh application Enforcement policy controlling access Sample policy to deny network access	Add Minport Export All Show 20 ♥ records Cony Export Desire
Gongaristica Gong	ClearRas co Piter Viene 1, 2, 3, 4, 5, 6, 6, 9, 10, 11, 12, Showing 1-1	nent Policies network access by evaluating an enforcement policy	Enforcement policy 4 licy associated with the service.	*ACL-VILAN for h3c* has been added Perceiption pull Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Aruba device Enforcement policy controlling access to Aruba device Enforcement policy controlling access to Lingib Application Enforcement policy controlling access Sample policy to devine thevir access	€ Add Export All Show 20 v records Copy Export Delete
Comparison Service Transplates & Witards Services Authentication Comparison C	ClearPas co ClearPas (Name 7 1. 2. 3. 4. 5. 6. 7. 8. 9. 9. 10. 11. 12. Showing 1-1	nent Policies ntrols network access by evaluating an enforcement po control of the second s	Enforcement publicy Ity associated with the service. C C Clear Plane RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	*ACL-VLAN for hJc" has been added	€ Add © Inport © Export All Show 20 ♥ records Copy Export Delate
Generation Service Translates & Witards Services Authentication Generation Ge	ClearRas of ClearR	ment Policies ntrols network access by evaluating an enforcement policy ACL for h3c ACL for h3c Cannot be access policy (Anno Policy (Bange Registration Disconnect) (Bange Registration Disconnect) (Bange Demy Access Policy (Sample Demy Access Policy (Sample Demy Access Policy 2 of 12	Enforcement policy / Iticy associated with the service. Image: Constraint of the service. Image: Conservice. Image: Conservice.<	ACL-VLAN for hJQ ^c has been added Puri Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Arbab device Enforcement policy controlling access to Arbab device Enforcement policy controlling access to Arbab device Enforcement policy controlling access to Insight application Sample policy to deny network access	 Add Import Export All Show 29 v records Cary Export Dates
Comparison Construction Con	ClearRas co Filer Name - - - - - - - - - - - - -	ment Policies ntrols network access by evaluating an enforcement policy Name ACL for bla ACLYLak for bla ACLYLak for bla ACLYLak for bla ACLYLak conset: ACLYLak conset: ACLYLak conset: ACLYLak conset: C	Enforcement policy ' lity associated with the service. Constraints of the service of the servi	*ACL-VLAR for hJc" has been added	€ Add Export All Show 20 ♥ records
© comparison © service Implates & Witards © Services ■ Authentication ■ Cathodication ■ Cathodication	ClearPas co ClearPas co Filer [Name	nent Policies ntrols network access by evaluating an enforcement po Venters V ACLV124 for h3c [Admin Testwork Legin Policy] [Admin Testwork Legin Policy] [Admin Testwork Legin Policy] [Admin Testwork Legin Policy] [Aruba Device Registration Disconnect] [Guest Operator Legins] [Guest Access Enforcement Policy] [Sample Damy Access Policy] [Sample Damy Access Policy] [Sample Damy Access Policy] 2 of 12	Enforcement publicy 4 lity associated with the service. C C Clear Plane RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	ACL-VLAR for hJc,* has been added Description pul Enforcement policy controlling access to Folicy Manager Admin Enforcement policy controlling access to Anab device Enforcement policy controlling access to Anab device Enforcement policy controlling access to Anab device Enforcement policy controlling access to Guest application Enforcement policy controlling access to Insigh application Enforcement policy controlling access to Insigh application Enforcement policy controlling access Sample policy to deny network access	Add Import Export All Show 20 → records Cony Export Desire
S comparison S convext implates & Witards Services Authentication Q services Q servi	ClearRas co 7 ClearRas co 7 Rer 1400 1. 2. 3. 4. 4. 5. 6. 6. 9. 10. 11. 12. Showing 1-1	nent Policies network access by evaluating an enforcement policy Name Accuration v Accuration in termork (adjo Policy) Accuration termork (adjo Policy) Accuration termork (adjo Policy) Accuration policy Accuration (adjo Policy) (anab policy Access Policy) (bardies Registration Disconnect) (bardies Registration Disconnect Policy) (bardies Access Informent Policy) (bardies Access Informent Policy) (bardies Access Informent Policy) (bardies Access Informent Policy) (bardies Access Policy) (bardies Access Informent Policy) (bardies Access Informent Policy) (bardies Access Pol	Enforcement policy ' Ity associated with the service Constraints' Constraints' RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	*ACL-VA.RI for his" has been added	€ Add © Import © Export All Show 20 ♥ records Coyy Export Delve
Scalarity Constraints Services Implates & Witards Services Authentication Grandward Constraints Services Ser	ClearPas co ClearPas (Name 7 7 8 7 8 9 10 11 12 5 8 8 9 10 11 12 5 8 8 9 10 11 12 12 12 12 12 12 12 12 12	nent Policies ntrols network access by evaluating an enforcement policy Activitation (for hite) Activitation (for hite	Enforcement publicy Ity associated with the service. C Clear Plane RADIUS RADIUS TACACS WEBAUTH RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	ACL-VLAR for hJc" has been added	 Add Import Export All Show 20 → records Cony Export Delite
Service Translates & Witards Services Authentication Carlos Services Se	Clearflass (Clearflass (Clearflast (Clearf	nent Policies network access by evaluating an enforcement policy Accurates v Accurates v Accurates by evaluating an enforcement policy Accurate brack Accurate Acc	Enforcement publy 4 licy associated with the service.	CACL-VLAR for hJ2 ^{ch} has been added pull Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Policy Manager Admin Enforcement policy controlling access to Anab device Enforcement policy controlling access to Insight application Sample policy to demy network access	Add ▲ Import ▲ Export All Show 20 v records Carry Export Delate.

6. サービスを追加します。

左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、 右上隅のAddをクリックします。

図32 Serviceページ

aruba			ClearPass	Policy Manager		Menu	
Dashboard	O Configur	onfiguration > Services					
Monitoring	Servie	ces				🚽 Add	
Configuration	0					Export All	
- 🛱 Service Templates & Wizards - 🏟 Services	This pag	e shows the curr	ent list and order of services that ClearPass follows do	iring authentication and authorization.			
E Authentication	Filter: N	lame	✓ contains ✓ +	Go Clear Filter		Show 50 v records	
- C Methods		Order	• Name	Туре	Template	Status	
- Q Identity	1.	0 9	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	0	
G Single Sign-On (SSO)	2.	0 8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	
- 🛱 Local Users	3.	0 7	[Insight Operator Logins]	Application	Aruba Application Authentication	0	
- 🛱 Endpoints	4.	6	[Guest Operator Logins]	Application	Aruba Application Authentication	0	
- Carlo Host Lists	5.	0 s	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0	
- CR Role Mannings	6.	0 4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	ø	
Posture	7.	3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	۲	
B B Enforcement	8.	0 2	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	0	
- 🛱 Policies	9.	0 1	dafu-802.1x	RADIUS	802.1X Wireless - Identity Only	0	
— 段 Profiles	Showing	1-9 of 9				Reorder Copy Export Delete	
- · Network							
- A Device Groups							
- D Proxy Targets							
Event Sources							
- 🛱 Network Scan							
- 🛱 Policy Simulation							

Serviceタブで、Typeフィールドから802.1X Wireless-Identity Onlyを選択し、h3cの名前を802.1Xに設定します。

図33 サービスの追加

aruba			ClearPass Policy M	anager		Men	
Dashboard C	Confi	iguration » Service	» Add				
Monitoring 0	Ser	vices					
Configuration C	Ser	vice Authentic	tion Roles Enforcement Summary				
Service Templates & Wizards Services Authentication Q Methods	Type Name Desc	: e: ription:	802.1X Wired - Identity Only 802.1X for h3c 802.1X Wired Access Service - Identity halv				
Q Sources ⊇ Q Identity - Q Single Sign-On (SSO) - Q Local Users	Monit	tor Mode: Options:	Enable to monitor network access without enforcement Authorization Profile Endpoints Accounting Proxy				
- di Static Host Lists				Service Rule			
- CR Roles	Match	hes O ANY or ®	ALL of the following conditions:	Omentee	Malua	_	
다. Cole Mappings	1	Radius:IETE	NAS-Port-Type	EQUALS	Ethernet (15)	9	a 17
Brindrammet Orelides Orelides	2.	Radius:IETF Click to add	Service-Type	BELONGS_TO	Login-Uter (1), Framed-Uter (2), Authenticat Only (8)		5 97
🕵 Administration 🛛 🖉	< B	ack to Services			Next → Sav	•	Cancel

Authenticationタブで、Authentication Methodsフィールドで[EAP MSCHAPv2]および [EAP PEAP]を選択し、Authentication Sourcesフィールドで[Local User Repository][Local SQL DB]を選択します。

図34 認証の設定

aruba	ClearPass Policy Manager	Menu
Dashboard O	Configuration > Services > Add	
Monitoring O	Services	
Configuration	Service Authentication Roles Enforcement Summary	
Q Service Templates & Wizards Q Services Q Lettroids Q Methods Q Sources Q Identity Q Single Sign-On (SSO) Q Incy I laters	Authentication Methods: [EAP (FAP)] Know Up : [EAP IASCHAPH2] Rove Down] Renove View Details -Select to Add-	Add New Authentication Method
Count of the second seco	Authentication Sources: [[Local User Repository][Local SQL DB] Money Up : Morey Up : Morey Up : Money U	Add New Authentication Source
- 🛱 Profiles	Strip Username Rules: Danble to specify a comma-separated list of rules to strip username prefixes or suffixes	
Arteroxic Covices Covices	Service Lettinicate: [-Seekit biodos-	View Certificato Defaito
Administration O	K Back to Services	Next → Save Cancel

#Enforcementタブで、h3cの強制ポリシーACL-VLANを選択し、Saveをクリックします。

図35 h3c用の実施ポリシーACL-VLANの選択

aruba			ClearPass Polic	y Manager		Menu
Dashboard O	Configuration » Services	s » Add				
Monitoring 0	Services					
Configuration O	Service Authentica	tion Roles Enforcement	Summary			
Corrice Templotes & Wtards Corrice Corri	Service Authentics Benforcement Policy: Description: Default Profile: Rules Evaluation Majoriti Conditions 1. (Authentication	Iteles Teles Teles Use cache Reles and P Reles and P ACL-VLAN for h3c ACL-VLAN for h3c Imm: ftrst-applicable	Summary Porture attributes from provious as Modely (214)	Enforcement Policy Details	s Enforcement Profiles ACL-VLAH for h3c	Add Hear Enforcement Policy
Administration 0	K Back to Services					Next → Save Cancel

Configuration > Servicesページで、サービスを変更して、h3cのサービス802.1Xを最初に移動します。

図36 サービスの順序変更

aruba			ClearPass Policy	/ Manager		Menu
Dashboard	O Configura	ation » Services				
Monitoring	 Service 	es				🚽 Add
Configuration	0					A Import
	This page	e shows the curre	nt list and order of services that ClearPass follows during auth	Service "802.1X for h3c" has be entication and authorization.	en added	
-	Filter: N	anne	✓ contains ✓	ear Filter		Show 50 v records
E Q Identity		Order •	Name	Туре	Template	Status
- 🛱 Single Sign-On (SSO)	1.	0 11	802.1X for h3c	RADIUS	802.1X Wired - Identity Only	0
Local Users	2.	10	MAC ACCESS	RADIUS	MAC Authentication	0
- Gradio Visat Lista	3.	9	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	۲
- in Boles	4.	8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0
A Role Mappings	5.	0 7	[Insight Operator Logins]	Application	Aruba Application Authentication	0
B Posture	6.	6	[Guest Operator Logins]	Application	Aruba Application Authentication	0
- B Enforcement	7.	□ s	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0
- 🛱 Policies	. 8.	0 4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0
- 🗘 Profiles	9.	0 3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
- ••• Network	10.	2	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	0
- Z Device Groups	11.		dafu-802.1x	RADIUS	802.1X Wireless - Identity Only	0
Proxy Targets	Showing	1-11 of 11				Reorder Copy Export Delete
↓ Network Scan ↓ Policy Simulation						

設定の確認

- 1. クライアントで、サービスh3c-dot1xに関連付けられ、802.1X認証を通過し、VLAN 1309のゲートウェイにpingできることを確認します(詳細は省略)。
- ACで、WLANクライアント情報を表示して、クライアントが802.1X認証に合格したことを確認します。 詳細なWLANクライアント情報と802.1Xオンラインユーザー情報を表示して、VLAN 1309とACL 3001がクライアントに割り当てられていることを確認します。
 [AC] display wlan client Total number of clients: 1 MAC address User name AP name R IP address VLAN fcdb-b3d4-d88c h3c1x ap1 2 40.9.0.13 1309

[AC] display wlan client verbose Total number of clients: 1 MAC address : fcdb-b3d4-d88c IPv4 address : 40.9.0.13 IPv6 address : N/A Username : h3c1x AID :1 AP ID :26 AP name : ap1 Radio ID :2 SSID : h3c-dot1x BSSID : ac74-0906-e874 : 1309 VLAN ID Sleep count :0 Wireless mode : 802.11gn Channel bandwidth : 20MHz 20/40 BSS Coexistence Management : Not supported SM power save : Disabled Short GI for 20MHz : Supported Short GI for 40MHz : Not supported STBC RX capability : Supported STBC TX capability : Supported : Supported LDPC RX capability Block Ack : N/A : 0, 1, 2, 3, 4, 5, 6, 7, Supported HT MCS set 8, 9, 10, 11, 12, 13, 14, 15 Supported rates : 11, 12, 18, 24, 36, 48, 54 Mbps QoS mode : WMM Listen interval : 10 RSSI:0 Rx/Tx rate : 0/0 Mbps Authentication method : Open system Security mode : RSN AKM mode : 802.1X Cipher suite : CCMP User authentication mode : 802.1X WPA3 status : Disabled Authorization ACL ID : 3001 Authorization user profile : N/A Authorization CAR : N/A Roam status : N/A Key derivation : SHA1 PMF status : N/A Forwarding policy name : Not configured Online time : Odays Ohours Ominutes 20seconds FT status : Inactive

[AC] display dot1x connection Total connections: 1 User MAC address : fcdb-b3d4-d88c AP name : ap1 Radio ID : 2 SSID : h3c-dot1x BSSID : ac74-0906-e874 Username : h3c1x

Authentication domain	: clearpass
IPv4 address	: 40.9.0.13
Authentication method	: EAP
Initial VLAN	: 1308
Authorization VLAN	: 1309
Authorization ACL number	: 3001
Authorization user profile	: N/A
Authorization CAR	: N/A
Termination action	: N/A
Session timeout last from	: N/A
Session timeout period	: N/A
Online from	: 2019/03/16 15:35:40
Online duration	: 0h 0m 26s

3. ClearPassサーバーで、オンラインユーザー情報を表示します。

左側のナビゲーションペインで、Monitoring > Live Monitoring > Access Trackerを選択します。 #表示されたページで、クライアントが802.1X EAP-PEAP認証を通過したことを確認します。

図37 オンラインユーザーの表示

aruba		Clear	Pass Policy Manager			Menu 🗮	
Dashboard	Monitoring > Live Monitoring > Acc	nitoring » Live Monitoring » Access Tracker					
Uve Monitoring	Access Tracker oct 27, 202 The Access Tracker page provides	1 16:39:52 CST a real-time display of per-session a	iccess activity on the selected server c	ir domain.			
P Accounting OnGuard Activity Analysis & Trending	T [All Requests]	CPPM (6.6.	1.201)	Last 1 day before To	day	Edit	
System Monitor	Filter: Usemame	contains 🖌	Go Clear Filter			Show 50 v records	
Indpoint Profiler Indpoint Profiler Indpoint Scan Results Indpoint Scan Results Indpoint Scan Results Indpoint Scan Indpoint Indpoint Scan	Ø Server	Source	Username	Service	Login Status	Request Timestamp •	

構成ファイル

AC:

```
#
radius scheme clearpass
  primary authentication 8.1.1.171
  primary accounting 8.1.1.171
  key authentication cipher $c$3$y9gLDgP10B8T9ry5u3AHTHOadEYI7g==
  key accounting cipher $c$3$bNuYW3C3Tf2AlrFwSRSRjUdZMn1uoQ==
  user-name-format without-domain
#
domain clearpass
  authentication default radius-scheme clearpass
  authorization default radius-scheme clearpass
  accounting default radius-scheme clearpass
#
dot1x authentication-method eap
#
wlan service-template h3c-dot1x
  ssid h3c-dot1x
  akm mode dot1x
  cipher-suite ccmp
  security-ie rsn
  client-security authentication-mode dot1x
  dot1x domain clearpass
  service-template enable
#
```

```
wlan ap ap1 model WA5320
    serial-id 219801A0YD8171E04018
    radio 1
      radio enable
      service-template h3c-dot1x vlan 1308
    radio 2
      radio enable
      service-template h3c-dot1x vlan 1308
 #
 vlan 1308 to 1309
 #
 interface Ten-GigabitEthernet1/0/26
    port link-type trunk
    port trunk permit vlan all
 #
 acl advanced 3001
    rule 0 deny ip destination 40.8.0.119 0
    rule 5 permit ip
 #
    スイッチ:
#
vlan 1308 to 1309
#
interface Ten-GigabitEthernet0/0/35
  port link-type trunk
  port trunk permit vlan all
#i
nterface Vlan-interface1308
  ip address 40.8.0.1 255.255.0.0
#i
nterface Vlan-interface1309
  ip address 40.9.0.1 255.255.0.0
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
dhcp server ip-pool vlan1309
  gateway-list 40.9.0.1
  network 40.9.0.0 mask 255.255.0.0
  dns-list 40.9.0.1
```

#

例:ClearPassベースのポータル認証の設定

ネットワーク構成

図38に示すように、ACはスイッチを介してClearPassサーバーに到達できます。次の要件を満たすよう にデバイスを設定します。

• ACは、ClearPassサーバーをRADIUSサーバーおよびポータル認証サーバーとして使用して クライアントのポータル認証を実行します。 • 認証方式は、直接ポータル認証です。



使用されているソフトウェアバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成および確認されています。

ハードウェア	ソフトウェアのバージョン
WX5540Hアクセスコントローラ	R5444P03
WA5320アクセスポイント	R5444P03
Aruba ClearPassサーバー	CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf

制約事項とガイドライン

APの背面パネルに表示されているシリアルIDを使用して、APを指定します。

手順

()重要:

この設定例では、ClearPassサーバーでのポータル認証によるクライアントの認証に関連する主な設定 だけを説明します。基本的なネットワーク設定および基本的なWLAN設定については、デバイスおよび サーバーのマニュアルを参照してください。

ACの 設定

ClearPassという名前のRADIUSスキームを作成し、ユーザー認証とアカウンティング用に 8.1.1.171のClearPassサーバーを指定します。そして、暗号化文字列h3cを共有キーとして設定します。

radius scheme clearpass

primary authentication 8.1.1.171 primary accounting 8.1.1.171 key authentication cipher \$c\$3\$y9gLDgP10B8T9ry5u3AHTHOadEYI7g== key accounting cipher \$c\$3\$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ== user-name-format without-domain

#

#ユーザー認証、認可、アカウンティングにRADIUSスキームのclearpassを使用するように、ISPドメイン

```
のclearpassを設定します。
#
domain clearpass
  authentication default radius-scheme clearpass
  authorization default radius-scheme clearpass
  accounting default radius-scheme clearpass
#
#HTTPおよびHTTPSサービスを有効にし、ポータルWebサーバーを構成し、HTTPおよびHTTPSベー
スのローカルポータルWebサービスを構成します。
ip http enable
ip https enable
#
portal web-server clearpass
  url https://8.1.1.171/guest/h3c.php?_browser=1
#
portal local-web-server http
  default-logon-page defaultfile.zip
#
portal local-web-server https
  default-logon-page defaultfile.zip
#
# ワイヤレスポータルクライアントの有効性チェックを有効にし、40.1.1.56宛てのトラフィックを許可するよ
うにIPベースのポータルフリー規則を設定します。
#
portal host-check enable
portal free-rule 200 destination ip 40.1.1.56 255.255.255.255
#サービステンプレートh3c-portalを構成します。SSIDをh3c-portalに設定し、直接ポータル認証を有効に
して、認証ドメインclearpassを指定します。
#
wlan service-template h3c-portal
  ssid h3c-portal
  portal enable method direct
  portal domain clearpass
  portal apply web-server clearpass
  service-template enable
#
#手動APを設定し、サービステンプレートh3c-portalをAPの無線にバインドします。
#
wlan ap ap1 model WA5320
  serial-id 219801A0YD8171E04018
  radio 1
    radio enable
    service-template h3c-portal vlan 1308
  radio 2
    radio enable
    service-template h3c-portal vlan 1308
#
#スイッチに接続されているポートのリンクタイプをトランクに設定し、クライアントのVLAN内のトラフィック
がポートを通過できるようにします。
#
interface Ten-GigabitEthernet1/0/26
```

```
port link-type trunk
```

port trunk permit vlan all

#

スイッチの設定

```
#VLAN 1308とVLAN-interface 1308を作成し、VLANインターフェースにIPアドレスを割り当てます。ス
イッチはこのVLANを使用してクライアントへのパケットを転送します。ACIに接続されているポートのリン
クタイプをトランクに設定し、クライアントのVLAN内のトラフィックがポートを通過できるようにします。
[Switch] vlan 1308
#
interface Ten-GigabitEthernet0/0/35
port link-type trunk
port trunk permit vlan all
#
interface Vlan-interface1308
ip address 40.8.0.1 255.255.0.0
#vlan1308という名前のDHCPアドレスプールを作成し、DHCPアドレスプールにサブネット40.8.0.0/16と
ゲートウェイIPアドレス40.8.0.1を指定します。この例では、DNSサーバーのアドレスは次のとおりです。
40.8.0.1(ゲートウェイアドレス)。ネットワーク上のDNSサーバーの実際のアドレスに置き換える必要があ
```

ります。 #

```
dhcp server ip-pool vlan1308
gateway-list 40.8.0.1
network 40.8.0.0 mask 255.255.0.0
dns-list 40.8.0.1
```

return

ClearPassサーバーの設定

1. ポータル認証を設定します。

#サーバーのWebインターフェースにアクセスするには、WebブラウザのアドレスバーにClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。

#ClearPass Guestをクリックします。

図39 ClearPassゲストへのログイン



#左側のナビゲーションペインで、Configuration > Pages > Web Loginsを選択します。表示されたページで、新しいWebログインページを作成します。

図40 Webログインページ

aruba		Clear	Pass Guest
Guest	• Home > Configuration > Pages > Web Logins	15	
Devices	Web Logins		
Onboard	0		
Configuration	Many NAS devices support Web-based auth	nentication for visitors.	
- SAuthentication	By defining a web login page on the ClearPa	ass Guest you are able to provide a	customized graphical login page
🥶 Content Manager	Use this list view to define new web login pa	ages, and to make changes to exis	ing web login pages.
Suest Manager		a now managed from the Web Login	tab within provisioning settings
By Hotspot Manager	A Maria	Dage Title	thes Name - Dage Chie
Pages	rane 48 h3c	h3c	Galleria Skin
Tields	A h3c-local	h3c-l	cal Galleria Skin
- Di Forms	2 web looins (Reload		Show all rows
Sal-Fagination Sal-Fagination	 Back to pages Back to configuration Back to main 		

#ポータルログインページを次のようにカスタマイズします。

- a. 名前をh3clこ設定します。
- b. ページ名をh3clc設定します。
- c. Vendor SettingsリストからCustom Settingsを選択します。
- **d.** Submit URLフィールドにhttp://40.1.1.56/portal/logon.cgiと入力します。IPアドレス40.1.1.56 はACのIPアドレスです。
- e. Username FieldフィールドにPtUser、Password FieldフィールドにPtPwdと入力しExtra Fields フィールドにPtButton=Logonと入力します。 Username Field、Password Field、およびExtra Fieldsフィールドの設定は変更しないことをお

Username Field、Password Field、およひExtra Fieldsフィールドの設定は変更しないことをお 勧めします。

- f. 他のパラメータにはデフォルト値を使用します。
- g. Save Changesをクリックします。

図41 ポータルログインページのカスタマイズ



		ClearPass Guest
Guest 0	Login Page	It selected, the client's default destination will be overridden regardless of its value.
E Onboard	Options for controlling the	look and feel of the login page.
Configuration	* Skin:	Choes the skin to use when this web login page is displayed.
- 🥵 Authentication E- 🍲 Content Manager	Title:	The title to display on the web login page. Leave blank to use the default (Login).
Guest Manager Hotspot Manager Transaction Processors Pages - Fields - Forms - List Views - Self-Rejistrations - Web Pages	Header HTML:	<pre>[mus_cooltecheck] {fif Sernsgi/mus_context type=erron}{serrmsglescape} {/mus_text id=7980{cp> Please login to the network using your username and password. {/p}{/mus_text}</pre>
Constraints Const	Footer HTML:	<pre>{ma_text id=7979}cp> Contact a staff member if you are experiencing difficulty loggin in. //mus_text}</pre>
Administration O	Login Message:	HTML template code displayed after the login form. [nwm_text id=7978;cp> Logging in, plases wait
on the		Clean Dage Guest
droba		Clear Pass Guest
Cuest O Devices O Conboard O Configuration O	Login Message:	
- S Authentication		
🗄 🕼 Content Manager		Insert HTML template code displayed while the login attempt is in progress.
Gest Manager Guest Manager	* Login Delay:	Insert
. € Content Manager - St. Guest Manager - St. Hotspot Manager - St. Transaction Processors	* Login Delay: Advertising Services	Insert HTML template code displayed while the login attempt is in progress. 0 The time in seconds to delay while displaying the login message.
B C Content Manager - S Cuest Manager - S Hotspot Manager - S Transaction Processors - S Pages	* Login Delay: Advertising Services Enable advertising content	Insert
Guest Manager Guest Manager Guest Manager Guest Manager Guest Manager Government Manager	* Login Delay: Advertising Services Enable advertising content Advertising:	Insert
	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests of	Insert ITAL template code displayed while the login attempt is in progress. The time in seconds to delay while displaying the login message. on the login page. Enable Advertising Services content with various cloud identity / social login options.
Gontent Manager Guest	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests of Enabled:	Insert HTML template code displayed while the login attempt is in progress. The time in seconds to delay while displaying the login message. on the login page. Enable Advertising Services content with various cloud identity / social login options. Enable logins with cloud identity / social network credentials
	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally preset guests v Enabled: Multi-Factor Authentio	
	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests u Enabled: Multi-Factor Authentit Require a secondary factor	Insert
Guest Manager Guest Manager Guest Manager Stransaction Processors Pages Fields Transactions Guest Registrations Self-Registrations Web Pages Receipts Receipts	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionaly present guests Brabled: Multi-Factor Authentit Require a secondary factor Provider: Network I conta Access	Insert HTML template code displayed while the login attempt is in progress. The time in seconds to delay while displaying the login message. on the login page. Enable Advertising Services content with various cloud identity / social login options. Enable logins with cloud identity / social network credentials attion when authenticating. No multi-factor authentication
Content Manager Conte	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests Enabled: Multi-Factor Authentit Require a secondary factor Provide: Network Login Access Controls access to the Logi	Insert
Content Manager Content Manager Content Manager Fields Fields Self-Registrations Web Pages Receipts Digital Pass Templates Fields Self-Services	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests Enabled: Multi-Factor Authentit Regure a secondary factor Provider: Network Login Access Controls access to the login Allowed Access:	Insert HTML template code displayed while the login attempt is in progress. 0 The time in seconds to delay while displaying the login message. on the login page. Enable Advertising Services content with various doud identity / social login options. Enable Indentity / social network credentials station when suthenticating. No multi-factor authentication page. Enter the IP addresses and networks from which logins are permitted.
Content Manager Conte	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests Enabled: Multi-Factor Authentit Require a secondary factor Provider: Network Login Access: Controls access to the login Allowed Access: Denied Access:	Insert
Content Manager Conte	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests Enabled: Multi-Factor Authentit Require a secondary factor Provider: Network Login Access: Controls access to the login Allowed Access: Denied Access: * Deny Behavior:	Insert
Guest Manager Guest Manager Guest Manager Hotspot Manager Fields Transaction Processors Fages Fields Forms Till List Views Self-Registrations Web Pages Recoipts Fields Fields Guest Receipt Fields Translations	* Login Delay: Advertising Services Enable advertising content Advertising: Cloud Identity Optionally present guests Enabled: Multi-Factor Authentit Require a secondary factor Provide: Network Login Access: Controls access to the login Allowed Access: Denied Access: * Deny Behavior: Post-Authentication	Insert. HTML template code displayed while the login attempt is in progress. HTML template code displayed while the login attempt is in progress. The time in seconds to delay while displaying the login message. on the login page. Enable Advertising Services content with various cloud identity / social login options. Enable logins with cloud identity / social network credentials attion when authentication Page. Enter the IP addresses and networks from which logins are permitted. Enter the IP addresses and networks from which logins are permitted. Enter the IP addresses and networks from which logins access. Send HTTP 404 Not Found status v Select the response of the system to a reguest that is not permitted. Enterected une-authentication
Content Manager Conte	togin Delay: Advertising Services Enable advertising Services Enable advertising Could dentity Optionally present guests vi Enabled: Multi-Factor Authentic Regure a secondary factor Provider: Network Login Access: Controls access to the login Allowed Access: Denied Access: Denied Access: * Deny Behavior: Post-Authentication Actions to perform after a Health Check:	Insert HTML template code displayed while the login attempt is in progress. Image: Image
Content Manager Content Manager Content Manager Factor of the second	* Login Delay: Advertising Services Enable advertising Cloud Identity Optionally presert guests Enabled: Multi-Factor Authentit Require a secondary factor Provider: Network Login Access: Controls access to the login Allowed Access: * Denied Access: *	Insert. HTML template code displayed while the login attempt is in progress. Image: Ima

2. ClearPass Policy Managerにログインします。

#サーバーのWebインターフェースにアクセスするには、WebブラウザのアドレスバーにClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。





ClearPass Policy Managerをクリックします。表示されたページで、ログインユーザー名とパスワードを入力し、Log Inをクリックします。

aruba	ClearPass Policy Manager
	You have 83 day(s) to activate the product <u>Activate Now</u>
	Admin Login Usemame:
	Password: Log In
Copyright 2020 Hewlett Packard Enterprise Development LP	

図43 ClearPass Policy Managerへのログイン

3. ClearPass Policy ManagerにACを追加します。

#左側のナビゲーションペインで、Configuration > Network > Devicesを選択します。開いたページ で、右上隅にあるAddをクリックします。

- a. ACでIPアドレス40.1.1.56/24を指定します。 ClearPassサーバーがこのIPアドレスに到達できることを確認します。
- b. RADIUS共有秘密を設定します。 ここで指定した共有シークレットが、AC上のRADIUSサーバーに指定した共有キーと同じである

ことを確認します。この例では、共有シークレットはh3cです。

- c. ベンダー名H3Cを選択します。
- d. Addをクリックします。

図44 デバイスの追加

aruba		ClearPass Policy	Manager			Menu 🗮
Dashboard C	Configuration > Network > Devices					
Monitoring C	Network Devices					🕂 Add
Configuration						A Import
Service Templates & Wizards Services Services Authentication	A Network Access Device (NAD) must belong to the	global list of devices in the ClearPass	latabase in order t	o connect to ClearPass.		 Discovered Devices
- Q Methods	Filter: Name V contains V	🕀 Go Cle	ar Filter			Show 20 v records
- Q Identity	# Add Device				•	
- C Single Sign-On (SSO)	1. Device SNMP Read Settings	SNMP Write Settings CLI Settings	OnConnect Enfor	rcement Attributes		
- 💭 Local Users	2. Name:	AC.			and the second s	
- 12 Endpoints - 12 Static Host Lists	3. IP or Subnet Address:	40.1.1.56/24				1.
- CR Roles	Showing 1-	(e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)				CopyExportOelete
- 🛱 Role Mappings	Description:					
Posture						
-Ö Policies	RADIUS Shared Secret:	[······	Verify:			
Profiles	TACACS+ Shared Secret:	[]	Verify:			
Network	Vendor Name:	НЗС				
- Q Devices	Enable RADIUS Dynamic Authorizatio	n: LH3C				
- Di Proxy Targets	Enable RadSec:					
O Event Sources O Event Sources O Event Sources Proley Simulation		_		Add	Casca	

4. ユーザーの追加:

#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたペ ージで、右上隅にあるAddをクリックします。

- a. ユーザーID、名前、およびパスワードをh3cportalに設定します。
- b. 事前定義済ロールEmployeeまたはユーザー定義済ロールを選択します。この例では、事前定 義済ロールEmployeeが選択されています。
- c. Addをクリックします。

45 ユーザーの追加

aruba	ClearPass Policy Manager					Menu	
Dashboard	O Configura	Configuration » Identity » Local Users					
Monitoring	• Local	Users					🗣 Add
Configuration	ChenPase Roky Manager lists all local laters in the Local Laters page.						Export All
- Authentication							()
r'i Sources	Filter: U	ser ID		Add Local User		•	Show (20 V records
Identity	"		User ID 🔺			Role	Status
_ the Single Sign-On (SSO)	1.		1	User ID:	h3cportal	[Employee]	Enabled
🗘 Local Users	2.		fcdbb3d4d8	Manager	P2erceted	[Employee]	Enabled
- 🗱 Endpoints	з.		h3c1x	name:	nscportar	[Employee]	Enabled
- 🛱 Static Host Lists	4.		h3cportal	Password:		[Employee]	Enabled
- 🗘 Roles	5.		leader	Verify Password:		leader-role	Enabled
- Q Role Mappings	6.		yuandongqu	Enable User:	Check to enable user)	[Employee]	Enabled
Enforcement	7.		yuandongqu			[Employee]	Enabled
- D Policies	Showing	1-7 of 7		Change Password:	Check to force change password on next IACACS+ login)		Export Delete
- 🛱 Profiles		tona. (frembolaal					
🗄 🕂 Network					Attributes		
- 🛱 Devices				Attribute	Value		
- Q Device Groups				1. Click to add			
Proxy Targets Q Event Sources Network Scan Q Policy Simulation							
					Add C	ancel	

5. ゲストアクセスの設定:

#左側のナビゲーションペインで、Configuration > Service Templates & Wizardsの順に選択します。表示されたページで、Guest Accessを選択します。

図46 ゲストアクセス

aruba	ClearPass Policy Manager	Menu
Dashboard O Monitoring O	ClearPass Admin Access (Active Directory) Service templete for Access to Grantess Policy Humager administration consule (Active Directory users).	
Configuration	ClearPass Admin SSO Login (SAML SP Service) SH/L based Single Sgn-On (SSO) access to ClearMass Policy Hanager, Rolph, Queet and Operator sorvers via entermal Identity Provider	
⇒ Authentication → Methods	Service template to provide SAHL based single sign-or service that can be used by other applications.	
⊇ Identity →⊉ Single Sign-On (SSO) →☐ local Users	Cloud Identity / Social Media Authentication To sufferitore user logging in via captive portal with their cloud identity or social media accounts. Guests must in-sufferitorate after their session ends.]
- California - Cal	Device MAC Authentication To suffericate guest devices based on their MAC address.	
- ☆ Role Mappings	EDUROAM service EDUROAM service to connect to compute the connect to compute retworks that are part of the eduration federation.	
Policies Profiles	Encrypted Wireless Access via 802.1X Public PEAP method Server Template for providing etcrypted wreters access to (guest) users via field 80.1X PEAP credentals.	
Devices Device Groups Device Transfer	Guest Access To sutheritate guest sams logging in via captive portal. Guests must re-sutheritate after their session ends.	
- Č Event Sources	Seusst Access - Web Login To subtericate parts users logang in via guest portal.	
- servicy amonaton	Guest Authentication with MAC Caching To authenticate users once using cachine portal and later to allow logins using cachied MAC Address of the device.	
	OAuth2 API User Access Servet template for API clerts subtracticating with username and password (OAuth2 grant type "password").	
	Onboard Service template for authorizing device predential provisioning and probarding.	

Generalタブで、Select Prefixフィールドのh3cを選択します。

図47 Generalタブ

aruba	ClearPass Policy Manager Menu 🚍
a 🖥 Dashboard	Configuration > Service Templates 8. Wizards
Honitoring	Service Templates - Guest Access
Configuration	
— Service Templates & Wizards	General Wireless Network Settings Posture Settings Guest Access Restrictions
- 🛱 Services	Select Prefix: h3c V
- Authentication	Name Tardina Line
- 💭 Methods	Name Preix, 105
- D Sources	Description
🗉 🧕 Identity	
- ☆ Single Sign-On (SSO)	For authenticating guest users who login via captive portal. Guests must re-authenticate after their session ends. Network access can be restricted based on day of the week or bandwidth limit used by the guest user.
🛱 Local Users	Posture checks can be enabled, optionally, to validate the client device for antivirus, anti-spyware, and firewall status. These results will determine the enforcement for the device.
- Q Endpoints	
- Q Static Host Lists	Kack to Service Templates & Wizards Delete Next→ Update Service Cancel
- Q Roles	
- La Role Happings	
* Coferement	
P Policier	
- Profiles	
Network	
- L' Devices	
- I'l Device Groups	
- C Proxy Targets	
- C Event Sources	
- D Network Scan	
- D Policy Simulation	

Wireless Network Settingsタブで、SSIDをh3c-portalに設定し、ワイヤレスコントローラとして ACを選択します。他のタブでは、パラメータのデフォルト値を使用して、設定を保存します。

図48 ワイヤレスネットワーク設定の構成

aruba		C	earPass Policy Manager	Menu
Dashboard	 Configuration > Service Templates & 	Wizards		
Monitoring	· Service Templates - Gue	ct Accors		
Configuration	o olivice templates oue	St Access		
- 🛱 Service Templates & Wizards	General Wireless Network Setti	ngs Posture Settings	Guest Access Restrictions	
🗸 🛱 Services	Select a wireless controller from	the list, or create a new	ne	
E Authentication	Wireless SSID for Guest access ::	h3c-portal		
- C Methods	Select Wireless Controller:	AC	~	
= Q Identity	Wireless Controller Name:	AC		
	Controller IP Address:	40.1.1.56/24		
- 🛱 Local Users	Vendor Name:	H3C	*	
- 🛱 Endpoints	RADIUS Shared Secret:			
- Q Static Host Lists	Enable RADIUS Dynamic Authorizatio	on: 🖾		
- Ca Role Mappings	Dynamic Authorization Port:	3799		
E Posture	Enable RadSec:			
⊖ S Enforcement - ⇔ Policies				
- D Profiles				
- Devices				
Device Groups				
— 谟 Proxy Targets				
- 🛱 Event Sources	K Back to Service Templates & Wi	izards		Delete Next → Add Service Cancel
- i Network Scan				
- 44 Policy Simulation				

6. サービスを追加します。

#左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、 サービスh3c Guest Accessを追加し、サービスの順序を変更して、サービスh3c Guest Accessを 最初のサービスに移動します。

図49 サービスh3c Guest Accessの追加

nfiguratio ervices is page si cer: Name	on > Services S hows the current	I list and order of services that ClearPass follows during auther	ntication and authorization.		🚽 Add 🔔 Import 🙎 Export A
ervices is page si ter: Name	5 hows the current	t list and order of services that ClearPass follows during auther	ntication and authorization.		⇒ Add ≜ Import ≗ Export A
is page si cer: Nami	hows the current	t list and order of services that ClearPass follows during author	ntication and authorization.		🛓 Import 🧟 Export A
is page si ter: Name	hows the current	t list and order of services that ClearPass follows during auther	ntication and authorization.		
er: Name	•	v contains v Go Cle			
			ar Filter		Show 50 v recor
Parent I	Order 🔺	Name	Туре	Template	Status
1.	1	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	0
2.	2	dafu-802.1x	RADIUS	802.1X Wireless - Identity Only	0
3.	3	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	0
4.	0 4	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
5.	5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0
6.	6	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0
7.	7	[Guest Operator Logins]	Application	Aruba Application Authentication	0
8.	8	[Insight Operator Logins]	Application	Aruba Application Authentication	0
9.	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	۲
10.	10	MAC ACCESS	RADIUS	MAC Authentication	0
11.	11	802.1X for h3c	RADIUS	802.1X Wired - Identity Only	0
owing 1-:	11 of 11				Reorder Copy Export Delet
	4. 5. 6. 7. 8. 9. 10. 11. owing 1-	4. 4 5. 5 6. 6 7. 7 8. 8 9. 9 10. 10 11. 11 cwing 1-11 of 11	4 [Priory Planager Admin Network Login Service] 5 5 [AliGroup Authonitation Service] 6 [AliGroup Authonitation Service] 7 [Const Operator Legina] 8 7 [Const Operator Legina] 9 [Doing For Operator Legina] 9 [Doing For Operator Legina] 10 11 Mac Access 11 11 802.1X for h3c	4 Pellon Manager Admin Internotic Login Service] TACACS 5 C Mich Group Authorization Service] RADUS 6 C Ando Borieck Access Service] TACACS 7 C Group Authorization Service] TACACS 8 8 6 Analo Service Access Service] TACACS 8 0 7 Construct Operator Loging Application 9 0 Device Registration Eleconnect] WEBAUTH 10 1 MAZ SES RADIUS 11 11 802.1X for hbc RADIUS	4 Piking Managar Admin Nethernik Ligh Service] TACACS TACACS TACACS TACACS TACACS Nathernamet 5 C A C Maria Versional Administration Service] TACACS TACACS RADUIS Enforcement (Generic) 7 C C Marka Device Access Service] TACACS TACACS Enforcement 7 C C vect Operator Loging] Application Annala Application Automatication 8 0 C Enforth Conservert Light Application Annala Application Automatication 9 C Device Registration Disconnect] WEBAUTH WeBAUTH WeBAUTH 10 0 NACACSES RADUIS RACAUNATICATION 11 0 11 002.1X for hbc RADUIS 802.1X Wird - Identity Only

#service h3c Guest Accessを編集します。Authenticationタブで、認証ソースとして Authenticationおよび[Local User Repository][Local SQL DB],を選択し、構成を保存します。

aruba		ClearPass Policy Manager	Menu 📕
Dashboard	Configuration > Services >	Edit - h3c Guest Access	
Monitoring	 Services - h3c Gu 	est Access	
& Configuration	Summary Service	Authentication Boles Enforcement	
	Authentication Methods:	[CHAP] [PAP] Micros Up ; [MICRAP] More Down ;	Add New Authentication Method
- ☆ Sources ⇒ © Identity - ☆ Single Sign-On (SSO) - ☆ Local Users - ☆ Endenint		Remove Vere DataBe ModifySelect to Add- v	
→ C Static Host Lists → C Static Host Lists → C Roles → C Role Mappings T III Posture	Authentication Sources:	(Closes User Repository) [Local SQL DB] [Local User Repository] [Local SQL DB] Home Domain 3 Sentone	Add New Authentication Source
을 활 Enforcement - 次 Policies - 次 Profiles - 아 Network		Vew Datab Modily	
- C Devices - C Device Groups	Strip Username Rules: Service Certificate:	Enable to specify a comma-separated list of rules to strip username prefixes or suffixes	View Certificate Details
-☆ Proxy Targets -☆ Event Sources -☆ Network Scan -☆ Policy Simulation			
aruba	Configuration = Services =	ClearPass Policy Manager	Menu
Nonitoring	Complete h2e Cu		
Configuration	Services - risc Gu	est Access	
- Z Service Templates & Wizards	Summary Service	Authentication Roles Enforcement	
- 🛱 Services	Service:		
- Authentication	Name:	h3c Guest Access	
- Q Methods - C Sources	Description:	RADULE Palacement (Canada)	
🗃 🧕 Identity	Ctatue:	Enabled	
្ស៊ី Single Sign-On (SSO)	Monitor Mode:	Disabled	
🛱 Local Users	More Ontions:	5. State 1	
- I Endpoints			
- O Roles		Service Rule	
🛱 Role Mappings	match ANY of the following	conditions:	Value
) 🕆 Posture	170-s		
	Authentication Methods:	1. [CHAP] 2. [PAP]	
∋ I Network - Devices	Authentication Sources:	3. [MSCHAP] 1. [Guest User Repository] [Local SQL DB] 2. [Card Use Repository] [Local SQL DB]	
Device Groups	Strip Username Pulae	an (cooler ower responsion) (cooler SQL DB)	
- 2's Event Sources	Service Certificate:		
Q Network Scan	Dervice Continueder		
- © Policy Simulation	Roles:		
	Role Mapping Policy:	*	
	Enforcement:		
	Use Cached Results:	Disabled	
	Enforcement Policy:	[Sample Allow Access Policy]	
	Back to Services		Disable Copy Save Cancel
Administration	•		

図50 認証の設定

設定の確認

- 1. クライアント上で、サービスh3c-portalに関連付けられた後にポータル認証ページにリダイレクト され、ポータル認証を通過できることを確認します(詳細は省略)。
- ACで、WLANクライアント情報とオンラインポータルユーザー情報を表示して、クライアントがオン ラインになったことを確認します。 [AC] display wlan client

Total number of MAC address fcdb-b3d4-d88c	clients: 1 User name N/A	AP name ap1	R IP address VLAN 1 40.8.0.129 1308
[AC] display wla	n client verbos	е	
Total number of	clients: 1		
MAC address		: fo	cdb-b3d4-d88c
IPv4 address		: 4	0.8.0.129
IPv6 address		: N	J/A
Username		: N	/A
AID		: 1	
AP ID		: 2	.6
AP name		: a	p1
Radio ID		:1	
SSID		: h:	3c-portal
BSSID		: a	1074-0906-0860
VLAN ID		: 1.	308
		. / (
Channel bandwi	dth	. 0	
SM power save	am	. 2 	
Short GL for 20M	1117	. D . c	Supported
Short GI for 40M	1112 1Hz		Supported
Short GI for 80M	1Hz		Supported
Short GI for 160	/80+80MHz	· N	lot supported
STBC RX capab	oility	· N	ot supported
STBC TX capab	ility	: S	upported
LDPC RX capab	oility	: 5	Supported
Beamformee ST	S capability	: 1	
Number of Soun	ding Dimensio	ons :1	
SU beamformee	capability	: 5	Supported
MU beamformee	e capability	: 5	Supported
Block Ack		: T	ID 0 Both
		TI	D 1 Out
		TI	D 6 In
Supported VHT-	MCS set	: N	NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
_		1	NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT M	ICS set	: 0	, 1, 2, 3, 4, 5, 6, 7,
		8	3, 9, 10, 11, 12, 13, 14,15
Supported rates		: 6,	, 9, 12, 18, 24, 36,
		48	
QoS mode		: /\	
		: 10	
RUU Dy/Ty rata		. 0.	73.3/173.3 Mbps
Authentication m	nethod	 . O	non system
Security mode	lethou	. U	PRF-RSNA
AKM mode		· N	ot configured
Cipher suite		· N	/A
User authenticat	tion mode	: E	Bypass
WPA3 status		: N	J/A
Authorization AC	CL ID	: N	/A
Authorization us	er profile	: N	/A
Authorization CA	٨R	: N	J/A
Roam status		: N	/A
Key derivation		: N	/A
PMF status		: N	/A

Forwarding policy name Online time FT status : Inactive [AC] display portal user all Total portal users: 1 Username: h3cportal AP name: ap1 Radio ID: 1 SSID: h3c-portal Portal server: N/A State: Online VPN instance: N/A IP MAC fcdb-b3d4-d88c 40.8.0.129 Authorization information: DHCP IP pool: N/A User profile: N/A Session group profile: N/A ACL number: N/A Inbound CAR: N/A Outbound CAR: N/A [AC] display portal user all verbose Total portal users: 1 Basic: AP name: ap1 Radio ID: 1 SSID: h3c-portal Current IP address: 40.8.0.129 Original IP address: 40.8.0.129 Username: h3cportal User ID: 0x1000009 Access interface: WLAN-BSS1/0/614 Service-VLAN/Customer-VLAN: 1308/-MAC address: fcdb-b3d4-d88c Authentication type: Local Domain name: clearpass VPN instance: N/A Status: Online Portal server: N/A Vendor: N/A Portal authentication method: Direct AAA: Realtime accounting interval: 720s, retry times: 5 Idle cut: N/A Session duration: 0 sec, remaining: 0 sec Remaining traffic: N/A Login time: 2019-03-16 14:46:17 UTC Online time(hh:mm:ss): 00:00:41 DHCP IP pool: N/A ACL&QoS&Multicast: Inbound CAR: N/A Outbound CAR: N/A ACL number: N/A User profile: N/A Session group profile: N/A

: Not configured

: 0days 0hours 11minutes 54seconds

VLAN Interface 1308 WLAN-BSS1/0/614 Max multicast addresses: 4 Flow statistic: Uplink packets/bytes: 56/5061 Downlink packets/bytes: 0/0

3. ClearPassサーバーで、オンラインユーザー情報を表示します。

#左側のナビゲーションペインで、Monitoring > Live Monitoring > Access Trackerを選択します。

#開いたページで、クライアントがポータル認証を通過したことを確認します。

図51 オンラインユーザーの表示

aruba		ClearPass Policy Manager						
Dashboard	Monitoring > Live Monitoring > Ac	cess Tracker						
Monitoring	Access Tracker oct 27, 20	Access Tracker oct 27, 2021 16:39:52 CST Ø Auto Refresh						
Live Monitoring	The Access Tracker page provides	a real-time display of per-session access ad	tivity on the selected server	or domain.				
Accounting	T [All Requests]	CPPM (6.6.1.201)		Last 1 day before 1	oday	Edit		
Analysis & Trending System Monitor	Filter: Usemame	▼] contains ▼] +	Go Clear Filter			Show 50 v records		
Endpoint Profiler	# Server	Source	Username	Service	Login Status	Request Timestamp 🔹		
Endpoint Profile Results Discovered Devices Audit Viewer Event Viewer Data Filters Blacklisted Users								

構成ファイル

```
AC:
radius scheme clearpass
  primary authentication 8.1.1.171
  primary accounting 8.1.1.171
  key authentication cipher $c$3$y9gLDgP10B8T9ry5u3AHTHOadEYI7g==
  key accounting cipher $c$3$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ==
  user-name-format without-domain
#
domain clearpass
  authentication default radius-scheme clearpass
  authorization default radius-scheme clearpass
  accounting default radius-scheme clearpass
#
ip http enable
ip https enable
#
portal web-server clearpass
  url https://8.1.1.171/guest/h3c.php?_browser=1
#
portal local-web-server http
  default-logon-page defaultfile.zip
#
portal local-web-server https
  default-logon-page defaultfile.zip
#
portal host-check enable
  portal free-rule 200 destination ip 40.1.1.56 255.255.255.255
#
wlan service-template h3c-portal
  ssid h3c-portal
  portal enable method direct
  portal domain clearpass
```

```
portal apply web-server clearpass
  service-template enable
#
wlan ap ap1 model WA5320
  serial-id 219801A0YD8171E04018
  radio 1
    radio enable
    service-template h3c-portal vlan 1308
  radio 2
    radio enable
    service-template h3c-portal vlan 1308
  #
  interface Ten-GigabitEthernet1/0/26
  port link-type trunk
  port trunk permit vlan all
 スイッチ:
#
vlan 1308
#
interface Ten-GigabitEthernet0/0/35
  port link-type trunk
  port trunk permit vlan all
#i
nterface Vlan-interface1308
  ip address 40.8.0.1 255.255.0.0
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
return
```

例:ClearPassサーバーからユーザーを強制的 にログオフする

ネットワーク構成

•

図52に示すように、ACはスイッチを介してClearPassサーバーに到達できます。次の要件を 満たすようにデバイスを構成します:

- ACはClearPassサーバーをRADIUSサーバーとして使用して、次の802.1X認証を実行します。 クライアント。
- 認証方式はEAP-PEAPです。
- ClearPassサーバーは、クライアントを強制的にログオフできます。



使用されているソフトウェアバージョン

この設定例は、次のハードウェアおよびソフトウェアバージョンで作成および確認されています。

ハードウェア	ソフトウェアのバージョン
WX5540Hアクセスコントローラ	R5444P03
WA5320アクセスポイント	R5444P03
Aruba ClearPassサーバー	CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf

制約事項とガイドライン

APの背面パネルに表示されているシリアルIDを使用して、APを指定します。

手順

()重要:

この設定例では、ClearPassサーバーからクライアントを強制的にログオフすることに関連する主な設定についてのみ説明します。基本的なネットワーク設定および基本的なWLAN設定については、デバイスおよびサーバーのマニュアルを参照してください。

ACの 設定

#ClearPassという名前のRADIUSスキームを作成し、ユーザー認証とアカウンティング用に8.1.1.171の ClearPassサーバーを指定し、共有キーをh3cの暗号化されたプレーンテキスト文字列に設定します。 # radius scheme clearpass primary authentication 8.1.1.171 primary accounting 8.1.1.171 key authentication cipher \$c\$3\$y9gLDgP10B8T9ry5u3AHTHOadEYI7g== key accounting cipher \$c\$3\$bNuYW3C3Tf2AlrFwSRSRjUdZMn1uoQ== user-name-format without-domain #

#ユーザー認証、認可、アカウンティングにRADIUSスキームのclearpassを使用するように、ISPドメイン のclearpassを設定します。 # domain clearpass authentication default radius-scheme clearpass authorization default radius-scheme clearpass accounting default radius-scheme clearpass # #EAPリレーを使用して802.1Xクライアントを認証するようにACを設定します。 [AC] dot1x authentication-method eap #サービステンプレートh3c-dot1xを作成し、そのSSIDをh3c-dot1xに設定し、認証モードを802.1X認証に 設定して、認証ドメインclearpassを指定します。 # wlan service-template h3c-dot1x ssid h3c-dot1x akm mode dot1x cipher-suite ccmp security-ie rsn client-security authentication-mode dot1x dot1x domain clearpass service-template enable # #手動APを設定し、サービステンプレートh3c-dot1xをAPの無線にバインドします。 # wlan ap ap1 model WA5320 serial-id 219801A0YD8171E04018 radio 1 radio enable service-template h3c-dot1x vlan 1308 radio 2 radio enable service-template h3c-dot1x vlan 1308 # #スイッチに接続されているポートのリンクタイプをトランクに設定し、クライアントのVLAN内のトラフィック がポートを通過できるようにします。 # interface Ten-GigabitEthernet1/0/26 port link-type trunk port trunk permit vlan all # #RADIUS DAEサーバー(DAS)を有効にし、ClearPassサーバーをDAEクライアント(DAC)として指定し、 暗号化された形式の共有キーh3cを設定します。RADIUSセッション制御を有効にします。 # radius dynamic-author server client ip 8.1.1.171 key cipher \$c\$3\$LkLgZHMHKYai/BgJw8LF98DwtLq6RQ== # radius session-control enable # スイッチの設定

#VLAN 1308とVLAN-interface 1308を作成し、VLANインターフェースにIPアドレスを割り当てます。ス イッチはこのVLANを使用してクライアントへのパケットを転送します。ACに接続されているポートのリン

```
クタイプをトランクに設定し、クライアントのVLAN内のトラフィックがポートを通過できるようにします。
[Switch] vlan 1308
#
interface Ten-GigabitEthernet0/0/35
  port link-type trunk
  port trunk permit vlan all
#
interface Vlan-interface1308
  ip address 40.8.0.1 255.255.0.0
#vlan1308という名前のDHCPアドレスプールを作成し、DHCPアドレスプールにサブネット40.8.0.0/16と
ゲートウェイIPアドレス40.8.0.1を指定します。この例では、DNSサーバーのアドレスは次のとおりです。
40.8.0.1(ゲートウェイアドレス)。ネットワーク上のDNSサーバーの実際のアドレスに置き換える必要があ
ります。
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
```

```
return
```

ClearPassサーバーの設定

1. ClearPassサーバーにログインします。

#サーバーのWebインターフェースにアクセスするには、WebブラウザのアドレスバーにClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。





#[ClearPass Policy Manager]をクリックします。表示されたページで、ログインユーザー名とパスワードを入力し、Log Inをクリックします。

図54 ClearPass Policy Managerへのログイン

aruba	ClearPass Policy Manager
	You have 83 day(s) to activate the product
	Admin Login
	Password:
	Log In
E copyright 2020 newlett Packard Enterprise Development LP	

2. ClearPass Policy ManagerにACを追加します。

#左側のナビゲーションペインで、Configuration > Network > Devicesを選択します。開いたページ で、右上隅にあるAddをクリックします。

- a. ACでIPアドレス40.1.1.56/24を指定します。 ClearPassサーバーがこのIPアドレスに到達できることを確認します。
- b. RADIUS共有秘密を設定します。 ここで指定した共有シークレットが、AC上のRADIUSサーバーに指定した共有キーと同じである ことを確認します。この例では、共有シークレットはh3cです。
- **c.** ベンダー名H3Cを選択します。
- d. Addをクリックします。

図55 デバイスの追加

aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	O Configuration * Network * Devices	
Monitoring	Network Devices	🕂 Add
S Configuration		Import Export All
- 🛱 Service Templates & Wizards		Discovered Devices
- 🛱 Services	A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.	
🗄 🚘 Authentication		
- 💭 Methods	Filter: Name Contains V 🕒 Go Clear Filter	Show 20 v records
Sources	Add Device O	
- I Single Sign-On (SSO)	1. In the second se	
- Q Local Users	2. Device SMMP Keda Settings SMMP Write Settings CLI Settings Unconnect Enforcement Attributes	
- 🛱 Endpoints	3. Name: AC	
- C Static Host Lists	Showing 1- IP or Subnet Address: 40.1156/24	
D Roles	(w.g., 192.106.1.10 of 192.106.1.1/24 of 192.106.1.1/20 of 2001:005:005:1210:11)	
Posture	Description:	
S Enforcement		
- 🛱 Policies	RADIUS Shared Secret: Verify:	
- C Profiles	TACACS+ shared Secret: Verify:	
Network	Vendor Name: H3C	
- A Device Groups	Enable RADIUS Dynamic Authorization: (H3C	
- C Proxy Targets	Enable RadSec:	
- O Event Sources		
- 🛱 Network Scan		
- 🎝 Policy Simulation		
	Add Cancel	

3. ユーザーの追加:

#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたペ ージで、右上隅にあるAddをクリックします。

- a. ユーザーID、名前、およびパスワードをh3c1xに設定します。
- b. 事前定義済ロールEmployeeまたはユーザー定義済ロールを選択します。この例では、事前定 義済ロールEmployeeが選択されています。
- c. Addをクリックします。

図56 ユーザーの追加

aruba			ClearPass Policy Manager		Menu 🗮
Dashboard	Configuration > Identity > Lo	ocal Users			
Monitoring	Local Users				🛖 Add
S Configuration					A Import
C Service Templates & Wizards					Account Settings
- 🛱 Services	ClearPass Policy Manager lis	ts all local users in the Loc	al Users page.		La recont octaine
Authentication					
- 🗘 Methods	Filter: User ID	v Containe v	Go Clear Filter		Show 20 v records
- 🛱 Sources	a 📕 liser ID a	Add Local User		• Role	Status
E Q Identity				[Employee]	Enabled
- C Single Sign-On (SSO)		User ID:	h3c1x	(Employee)	Enabled
C Local Users	2. 0 10003040	Name:	h3c1x	[employee]	Enabled
- 4 Endpoints	3. 🗆 n3cportai	Dassword-		[Employee]	Enabled
A Boles	4. Lader			leader-role	Enabled
- C Role Mappings	5. U yuandong	qu Verify Password:		[Employee]	Enabled
E Posture	6. 🗌 yuandong	Enable User:	(Check to enable user)	[Employee]	Enabled
🗄 🕏 Enforcement	Showing 1-6 of 6	Change Password:	(Check to force change password on next TACACS+ login)		Export Delete
- C Policies		Role:	[Employee]		
- Antwork			Attributes		
Devices		Attribute	Value		
- Device Groups		1 Click to add		_	
- 🛱 Proxy Targets		in the to out in			
- 🛱 Event Sources					
Network Scan					
- I Policy Simulation					
			Add		
			Add		
Administration	0				

4. enforcementプロファイルを追加します。

左側のナビゲーションペインで、Configuration > Enforcement > Profilesを選択します。開いたページで、右上隅にあるAddをクリックします。

図57 enforcementプロファイルの追加

aruba			C	earPass Pol	icy Manager		Menu 📕
Dashboard O	Configurati	ion » E	nforcement » Profiles				
Monitoring 0	Enforce	mer	t Profiles				🐥 Add
& Configuration	Linoree	inci	it fromes				A Import
D Service Templates & Wizards	Fach enfon	remer	t policy contains enforcement profiles that mat	ch conditions (mla m	osture and time) to ar	tions (enforcement profiles)	Export All
- 🛱 Services	Local canon	center	e poney contains entereenten promes that may	en conditions (role) p	une, une une, to be	terroreanent promesti	
E Authentication	Tithe av Man		http://www.sectores.com		Clear Filter	Shaw	20 × recorde
🖧 Methods	Filter: [Nali		• Contains • Insq				Tecords
- 🛱 Sources			Name 🔺		Туре	Description	
🖹 🧕 Identity	1.	0	ACL for h3c		RADIUS	puli	
–	2.	0	disconnect for h3c		RADIUS_COA	puli	
Local Users	3.		[H3C - Bounce Switch Port]		RADIUS_COA	System-defined profile to bounce the switch port on H3C products (including HPE FlexNetwork / C	omware).
- 🛱 Endpoints	4.		[H3C - Disable Switch Port]		RADIUS_CoA	System-defined profile to disable the switch port on H3C products (including HPE FlexNetwork / C	omware).
- Q Static Host Lists	5.		h3c Guest Bandwidth Limit		Post_Authentication	System-defined profile to set Guest bandwidth limits	
- Li Roles	6.		h3c Guest Do Expire		Post_Authentication	Enforcement profile for Guest do expire functionality	
The Posture	7.	0	h3c Guest Expire Post Login		Post_Authentication	Enforcement profile for Guest expire post login functionality	
# Enforcement	8.		h3c Guest MAC Caching		Post Authentication	System-defined profile to update the endpoint with Guest user details	
- O Policies	9.		h3c Guest Session Limit		Post Authentication	System-defined profile to set concurrent Guest session count	
- 🛱 Profiles	10		h3c Guest Session Timeout		RADIUS	and the second	
Network		-	[UDC - Terminate Consider]		DADIUG CHA	Custom defined applies to discover the uses on USC appliests (includes USC FlagMatural) (Com	
- 🛱 Devices -	11.		(MSC - Terminate Session)		KADIOS_COA	System-denned prome to disconnect the user on HSC products (including HVE Rexidential)	wate).
- 🛱 Device Groups	Showing 1-	-11 of	11				xport Delete
- 🛱 Proxy Targets							
- 🛱 Event Sources							
- Q Network Scan							
- Q Policy Simulation							
R Administration 0							

#H3Cのプロファイル名をDisconnectに設定し、RADIUS_CoAと入力して、属性を追加します。 [Radius:IETF Acct-Session-Id]を選択し、[Save]をクリックします。

図58 プロファイルの構成

aruba		ClearPass Poli	cy Manager		Menu
ashboard	O Configuration > Enforcement	nt = Profiles = Edit Enforcement Profile - Disconnect for H3C			
Honitoring	 Enforcement Profi 	les - Disconnect for H3C			
Configuration	0		Enforcement profile has not been sav	ed	
 — Ö Service Templates & Wizards – Ö Services 	Summary Profile A	ttributes			
Authentication	Profile:				
C Methods	Name:	Disconnect for H3C			
⇒ Ω Identity	Description:				
	Type:	RADIUS_CoA			
🛱 Local Users	Action:	Disconnect			
Endpoints Or Otatio Next Lists	Device Group List:	•			
- La Roles	Attributes:				
C Role Mappings	Туре	Name		Value	
A Bernormant A Denicles A Denicles A Denicles A Denicles A Denicle A De			-		
Administration	Back to Enforcement	Profiles			Copy Save Cancel

- 5. 強制ポリシーを追加します。詳細については、「例:VLANおよびACL割り当てを使用した ClearPassベースの802.1X認証の設定」を参照してください。
- 6. サービスを追加します。

#左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、 右上隅のAddをクリックします。 図59 サービスページ

図60 サービスの追加

aruba				ClearPass Policy	Manager		Menu
Dashboard	O Configur	ration »	Services				
Monitoring	 Servie 	ces					🚽 Add
8 Configuration	0						A Import
Ö Service Templates & Wizards Services	This pag	je show	s the current	list and order of services that ClearPass follows during auth	entication and authorization.		Export
Authentication	Filter: N	lame		✓ contains ✓ + Go Cl	ear Filter		Show 50 v reco
- C Methods			Order •	Name	Туре	Template	Status
2 Identity	1.	0	9	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	0
- C Single Sign-On (SSO)	2.	0	8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0
- 🛱 Local Users	3.	0	7	[Insight Operator Logins]	Application	Aruba Application Authentication	۲
- 🗘 Endpoints	4.		6	[Guest Operator Logins]	Application	Aruba Application Authentication	0
- i Static Host Lists	5.		5	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0
- 11 Roles	6.	0	4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0
Posture	7.	0	3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	٢
& Enforcement	8.	0	2	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	0
- 🗘 Policies	9.		1	dafu-802.1x	RADIUS	802.1X Wireless - Identity Only	0
Profiles	Showing	1-9 of	9			Re	order Copy Export Delet
La Devices							
Device Groups							
- D Proxy Targets							
🛱 Event Sources							
🛱 Network Scan							
Policy Simulation							

Serviceタブで、Typeフィールドから802.1X Wireless-Identity Onlyを選択し、h3cの名前を802.1Xに設定します。

aruba			ClearPass Policy Ma	anager		Menu 🗮
Dashboard	Onfiguration > Services > Add					
Monitoring 0	Services					
Configuration 📀	Service Au	uthentication Roles Enforcement	Summary			
Image/regime Image/regime Operation Operation Operation Operation	Services Au Type: Name: Description: Monte Option: Matches O Att Matches O Att Click to /	uthentification Roles Enforcement 002 XX Wared - learning Only 002 XX Wared - learning Only 002 XX Wared - learning Only 002 XX Wared - learning Only 002 XX Wared - learning Only 001 XX Wared - learning Only 01 Authorization > nonitor - networe - authorization > nonitor - networe 01 Authorization > nonitor - networe - authorization > nonitor - networe 12 FT	Summary	Service Rule Operation EQUALS BELONGS_TO	Volter Etheret (15) Login Use (1), Framed-User (2), Authenticat Only (8)	9 <u>6</u> 9 9 <u>6</u> 9
_	Back to Ser	ervices			Next Sa	re Cancel

Authenticationタブで、Authentication Methodsフィールドで[EAP MSCHAPv2]と[EAP PEAP]を選択し、Authentication Sourcesフィールドで[Local User Repository]を選択します。 Enforcementタブで、Disconnect for H3Cを選択し、設定を保存します。

```
図61 サービスの構成
```

aruba	ClearPass Policy Manager	Menu
Dashboard	Configuration > Services > Add	
Monitoring	Services	
Configuration	Service Authentication Roles Enforcement Summary	
Q Service Templates & Wizards Q Services Q Authentication Q Methods Q Sources Q Identity Q Single Sign-On (SSO)	Authentication Methods: [EAP IECHAPY2] More Up 1 [EAP ISCHAPY2] R More Down j R Wow Dy 1 Wore Down j Wow Dy 10 Wore Down j Wow Dy 10 Wore Down j Wow Dy 10 Wore Down j R Wore Down j Wore Down j R Wore Down j R Wore Down j Wore Down j R Wore Down j Wore Down j R Wore Down j R Wore Down j Wore Down j R Wore Down j Wore Down j	Add New Authentication Method
-Q.Local Users -Q.Endpoints -Q.Static Host Lits -Q.Role Mappings - Proture # Enforcement	Authentication Sources: [Local User Repository] (Local SQL DB) Move Up : Move Up : Move Down ; Comove View Details ModBy -Select to Add-	Add New Authentication Source
- in Profiles	Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes	
⊴ firstensk ⊖ Device Groups ⊖ Device Groups ⊖ Provy Trapets ⊖ Revent Sources ⊖ Revent Sources ⊖ Revent Sources ⊖ Revent Sources → O Herbork Scan	Service Certificate: Selectib Add-	View Certificate Details
Administration	Back to Services	Next → Save Cancel

Configuration > **Services**ページで、サービスの順序を変更してh3cのサービス802.1Xを最初 へ移動します。

図62 サービスの順序変更

aruba			ClearPass Policy	Manager		Menu
Dashboard	O Configur	ration » Services				
Honitoring	 Service 	ces				🚽 Add
S Configuration	0					A Import
Service Templates & Wizards Services Authentication	This pag	ge shows the curre	nt list and order of services that ClearPass follows during authe	Service "802.1X for h3c" has be ntication and authorization.	en added	
- C Methods	Filter: N	lame	✓ contains ✓ Go Cte	ar Filter		Show 50 v records
□ _ Q Identity		Order	Name	Туре	Template	Status
- 🛱 Single Sign-On (SSO)	1.	0 11	802.1X for h3c	RADIUS	802.1X Wired - Identity Only	0
- 🛱 Local Users	2.	0 10	MAC ACCESS	RADIUS	MAC Authentication	0
- Q Endpoints	3.	9	h3c Guest Access	RADIUS	RADIUS Enforcement (Generic)	0
- I't Roles	4.	8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0
Role Mappings	5.	0 7	[Insight Operator Logins]	Application	Aruba Application Authentication	0
🗊 🖶 Posture	6.	6	[Guest Operator Logins]	Application	Aruba Application Authentication	٢
🗄 🔹 Enforcement	7.	□ s	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0
- 🖧 Policies	. 8.	0 4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	۲
- Q: Profiles	9.	3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	۲
- The Network	10.	2	chengdu-7205-1x	RADIUS	Aruba 802.1X Wireless	۲
- Ž Device Groups	11.	□ 1	dafu-802.1x	RADIUS	802.1X Wireless - Identity Only	0
Proxy Targets	Showing	1-11 of 11				Reorder Copy Export Delete
— ♀ Network Scan → ♀ Policy Simulation						

設定の確認

- 1. クライアントで、サービスh3c-dot1xに関連付けられ、802.1X認証を通過してIPアドレスを取得できることを確認します(詳細は省略)。
- **2.** ACで、WLANクライアント情報とオンライン802.1Xユーザー情報を表示して、クライアントがオン ラインになったことを確認します。

AP name	R	IP address VLAN
ap1	2	40.8.0.129 1308
: 1		
: fcdb-	b3d4-d8	38c
: 40.8	.0.129	
: N/A		
: h3c1	х	
: 1		
	AP name ap1 : 1 : fcdb- : 40.8 : N/A : h3c1 : 1	AP name R ap1 2 : 1 : fcdb-b3d4-d8 : 40.8.0.129 : N/A : h3c1x : 1

AP ID AP name Radio ID SSID BSSID VLAN ID Sleep count Wireless mode Channel bandwidth 20/40 BSS Coexistence Management SM power save Short GI for 20MHz Short GI for 40MHz STBC RX capability STBC TX capability LDPC RX capability Block Ack Supported HT MCS set Supported rates QoS mode Listen interval RSSI Rx/Tx rate Authentication method Security mode AKM mode Cipher suite User authentication mode WPA3 status Authorization ACL ID Authorization user profile Authorization CAR Roam status Key derivation PMF status Forwarding policy name Online time FT status [AC] display dot1x connection Total connections: 1 User MAC address : fcdb-b3d4-d88c AP name Radio SSID BSSID Username Authentication domain IPv4 address Authentication method Initial VLAN Authorization VLAN Authorization ACL number Authorization user profile Authorization CAR : N/A Termination action : N/A

:26 : ap1 :2 : h3c-dot1x :ac74-0906-e874 : 1308 :0 : 802.11gn : 20MHz : Not supported : Disabled : Supported : Not supported : Supported : Supported : Supported : N/A : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 : 11, 12, 18, 24, 36, 48, 54 Mbps : WMM :10 :0 : 0/0 Mbps : Open system : RSN :802.1X : CCMP :802.1X : Disabled : N/A : N/A : N/A : N/A : SHA1 : N/A : Not configured : Odays Ohours Ominutes 13seconds : Inactive : ap1 ID:2 : h3c-dot1x : ac74-0906-e874 : h3c1x : clearpass : 40.8.0.129 : EAP : 1308 : 1308 : N/A : N/A

Session timeout last from	: N/A
Session timeout period	: N/A
Online from	: 2019/03/16 11:14:25
Online duration	: 0h 0m 19s
	· · · · · · · · · ·

3. ClearPassサーバーで、オンラインユーザー情報を表示します。

#左側のナビゲーションペインで、Monitoring > Live Monitoring > Access Trackerを選択します。 #表示されたページで、クライアントが802.1X EAP-PEAP認証を通過したことを確認します。

図63 オンラインユーザーの表示

aruba		ClearPa	ss Policy Manager			Menu 📃
Monitoring	Monitoring > Live Monitoring > Av Access Tracker oct 27, 20	ccess Tracker 321 16:39:52 CST				🖉 Auto Refresh
Access Tracker Access Tracker OnGuard Activity	The Access Tracker page provide	s a real-time display of per-session access	activity on the selected server	or domain.	day	Edit
Analysis & trending System Monitor Monitor Profiler and Network Scan Metwork Scan Results	Filter: Usemame Server	Contains Source	Go Clear Filter Username	Service	Login Status	Show 50 v records Request Timestamp v
Audit Viewer Event Viewer Data Filters Blacklisted Users						

#802.1Xユーザーの詳細な要求情報を表示し、要求ステータスを変更します。アクセスコントロー ルタイプとして[RADIUS CoA]を選択し、[RADIUS CoA type]を[Disconnect for H3C]に設定して、 設定を送信します。

4. パケットをキャプチャして、ClearPassサーバーが接続解除要求メッセージを送信してオンラインユ ーザーをログオフし、ACからACKメッセージを受信できることを確認します。

```
図64 切断メッセージ
```

No. Source Destination Protocol Length Info 629 8.1.1.171 40.1.1.56 RADIUS 110 Disconnect-Request(40) (id=108, 1=60)
No. Source Destination Protocol Length Info 629 8.1.1.171 40.1.1.56 RADIUS 110 Disconnect-Request(40) (id=108, 1=60)
629 8.1.1.171 40.1.1.56 RADIUS 110 Disconnect-Request(40) (id=108, 1=60)
634 40.1.1.56 8.1.1.1/1 RADIUS 110 Disconnect-ACK(41) (1d=108, 1=60)
635 40.1.1.56 8.1.1.171 RADIUS 460 Accounting-Request(4) (id=7, 1=410)
636 8.1.1.171 40.1.1.56 RADIUS 70 Accounting-Response(5) (id=7, l=20)
Frame 629: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II (VLAN tagged), SrC: 50:08:00:84:00:71 (50:08:00:84:00:71), Dst: 48:78:08:68:68:68:68:68:68:68:68:68:68:68:68:68
HINTERNET PROTOCOL VERSION 4, SPC: 8.1.1.1/1 (8.1.1.1/1), DST: 40.1.1.56 (40.1.1.56)
B oser Datagram Protocol, Src Port: 5/461 (5/461), Dst Port: radius-dynauth (3/99)
Code: Disconnect Request (40)
Parket identifier: Nofc (108)
Length: 60
Authenticator: d93cc147d6152a8708672d1593577290
The response to this request is in frame 6341
Attribute value Pairs

構成ファイル

AC: • # radius scheme clearpass primary authentication 8.1.1.171 primary accounting 8.1.1.171 key authentication cipher \$c\$3\$y9gLDgP10B8T9ry5u3AHTHOadEYI7g== key accounting cipher \$c\$3\$bNuYW3C3Tf2AIrFwSRSRjUdZMn1uoQ== user-name-format without-domain # domain clearpass authentication default radius-scheme clearpass authorization default radius-scheme clearpass accounting default radius-scheme clearpass # dot1x authentication-method eap # wlan service-template h3c-dot1x ssid h3c-dot1x akm mode dot1x cipher-suite ccmp security-ie rsn client-security authentication-mode dot1x dot1x domain clearpass service-template enable # wlan ap ap1 model WA5320 serial-id 219801A0YD8171E04018 radio 1 radio enable service-template h3c-dot1x vlan 1308 radio 2 radio enable service-template h3c-dot1x vlan 1308 # interface Ten-GigabitEthernet1/0/26 port link-type trunk port trunk permit vlan all # radius dynamic-author server client ip 8.1.1.171 key cipher \$c\$3\$LkLgZHMHKYai/BgJw8LF98DwtLq6RQ== # radius session-control enable # スイッチ: . # vlan 1308 # interface Ten-GigabitEthernet0/0/35 port link-type trunk port trunk permit vlan all # interface Vlan-interface1308

```
ip address 40.8.0.1 255.255.0.0
#
dhcp server ip-pool vlan1308
gateway-list 40.8.0.1
network 40.8.0.0 mask 255.255.0.0
dns-list 40.8.0.1
#
return
```