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

目次

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。

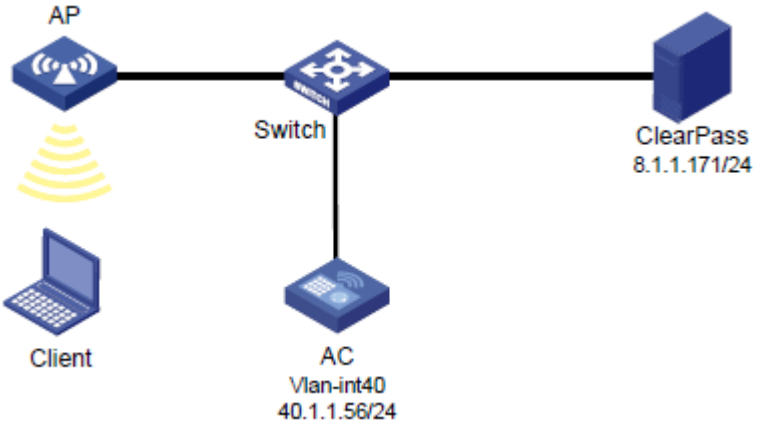
例:ClearPassベースのMAC認証の設定

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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
    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。

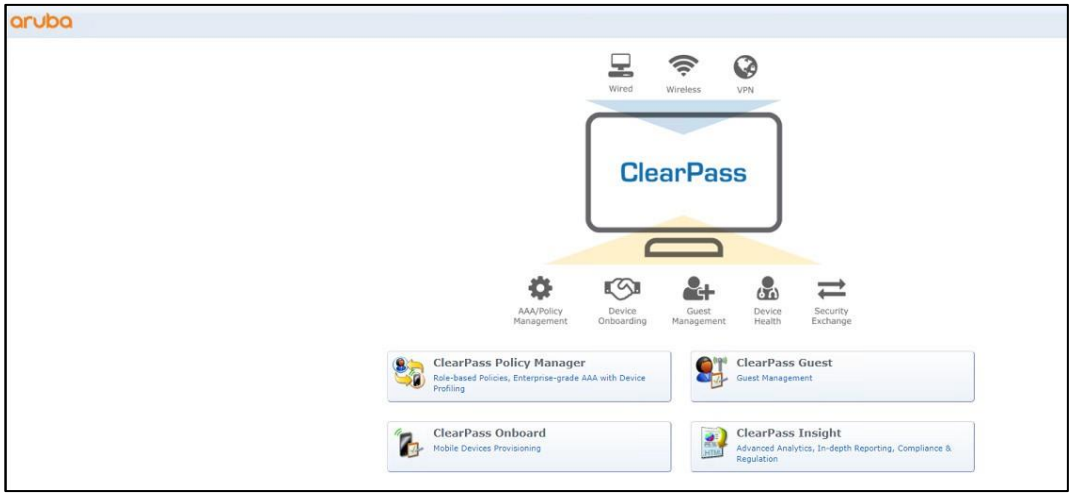
```
#
dhcp server ip-pool vlan1308
   gateway-list 40.8.0.1
   network 40.8.0.0 mask 255.255.0.0
   dns-list 40.8.0.1
#
 return
```

ClearPassサーバーの設定

1. ClearPassサーバーにログインします。

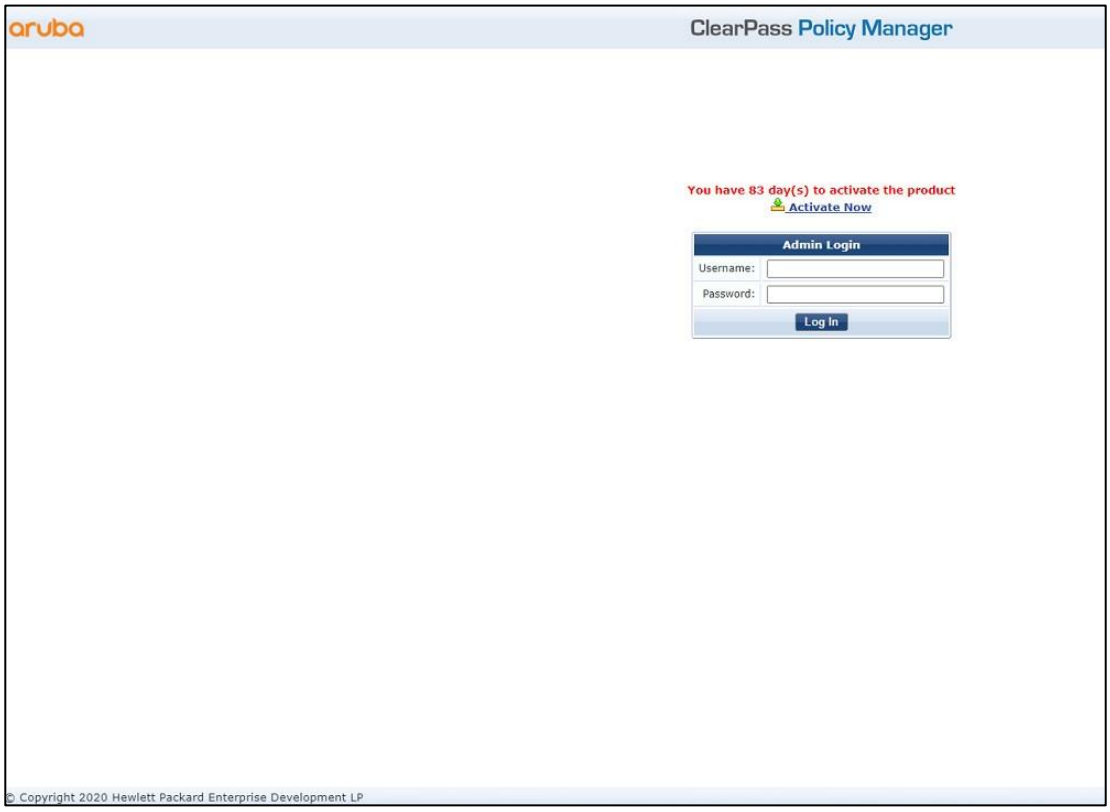
   #サーバーのWebインターフェースにアクセスするには、Webブラウザのアドレスバーに ClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。

   図2 ClearPassへのログイン



   # **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



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。

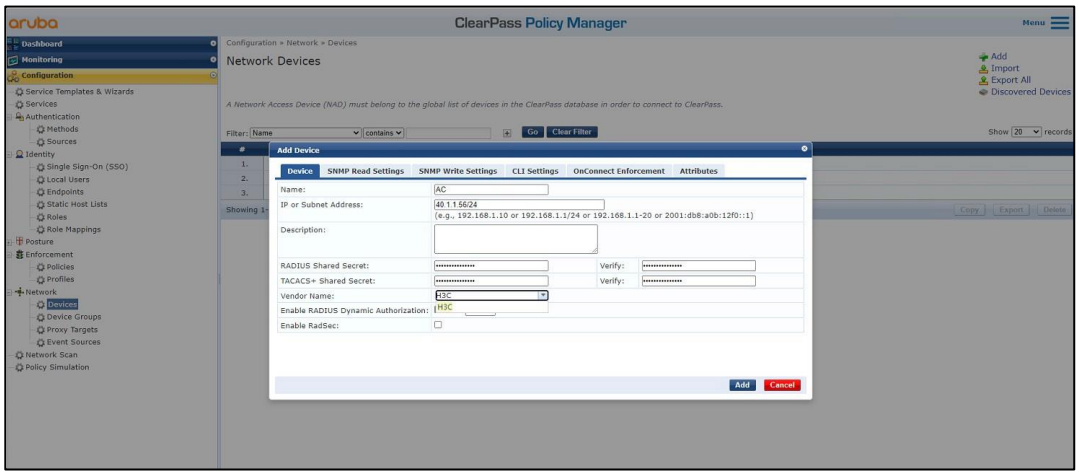
b. RADIUS共有秘密を設定します。

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4 デバイスの追加



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。

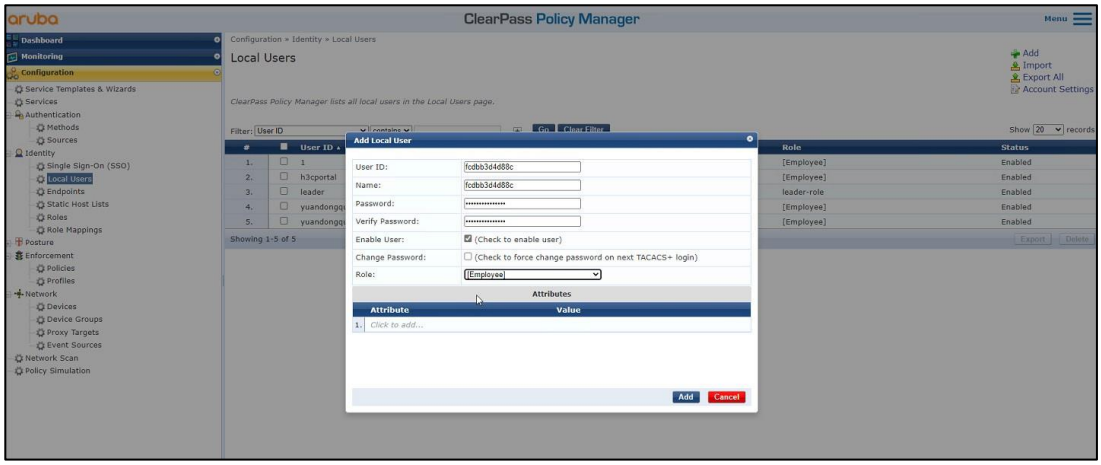
a. ユーザーID、名前、およびパスワードをクライアントのMACアドレスに設定します。MACアドレスの形式がACと同じであることを確認します。

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。

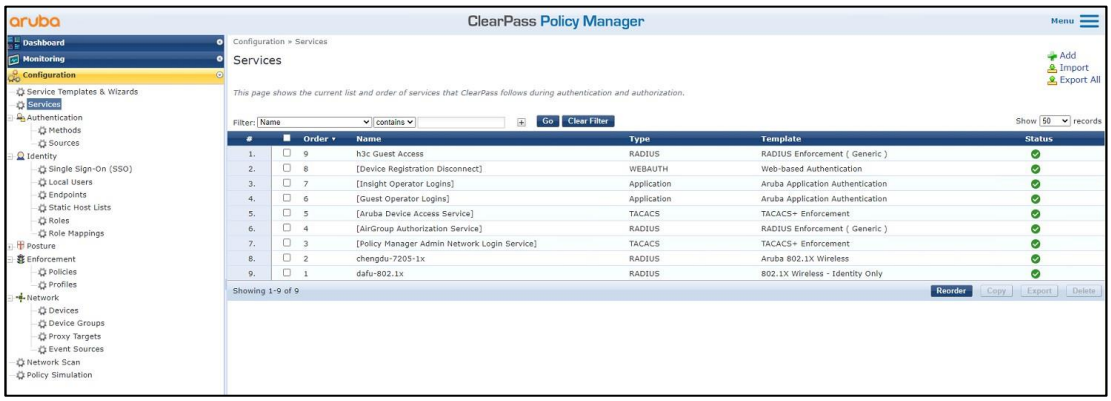
図5 ユーザーの追加



4. サービスを追加します。

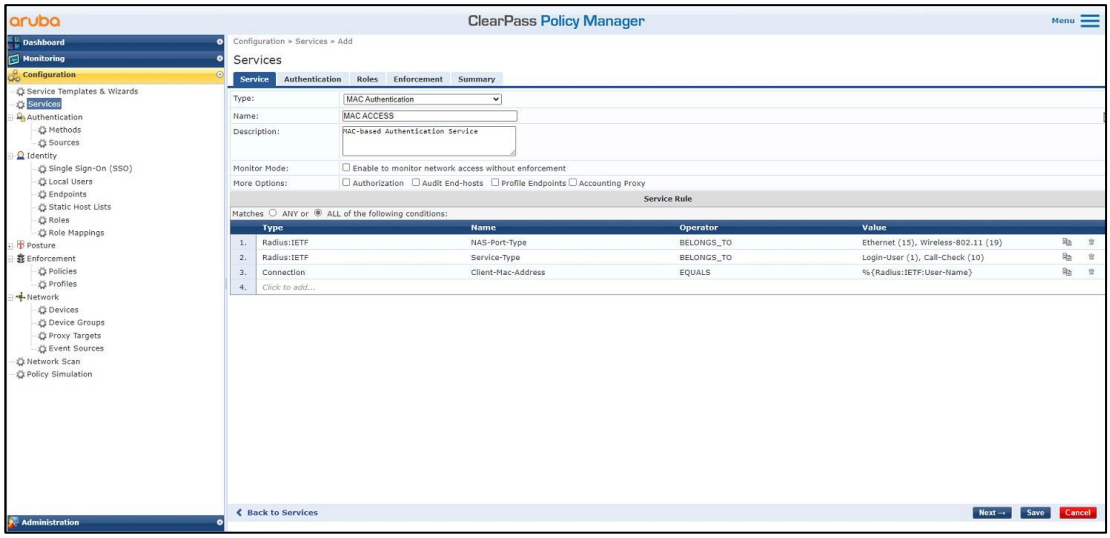
#左側のナビゲーションペインで、**Configuration > Services**を選択します。表示されたページで、右上隅の**Add**をクリックします。

図6 Serviceページ



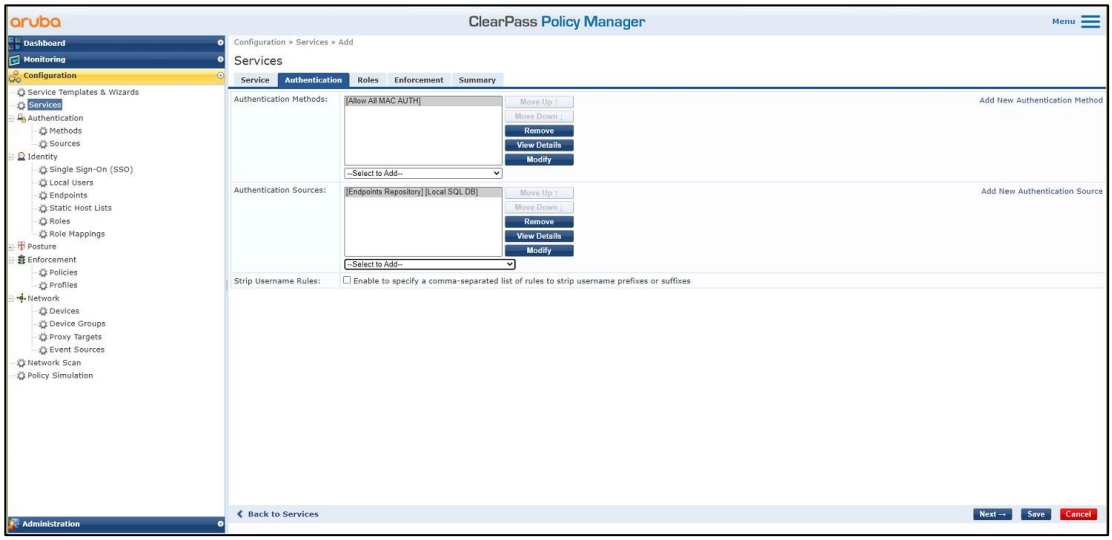
Serviceタブで、Typeフィールドから**MAC Authentication**を選択し、名前を**MAC ACCESS**とします。

図7 Serviceの追加



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。

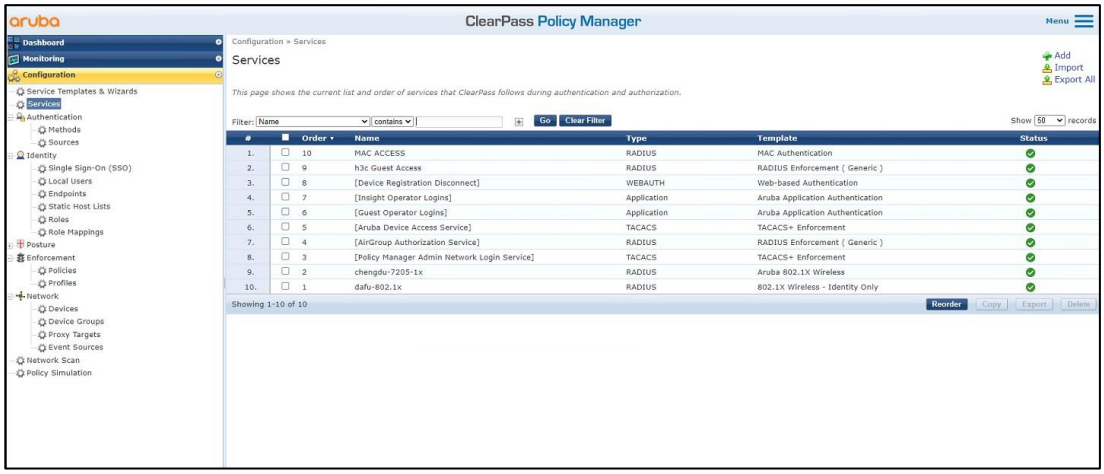
図8 認証の構成



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



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
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 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/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 : 0days 0hours 0minutes 15seconds
FT status : Inactive

[AC] display mac-authentication connection
Total connections: 1
User MAC address : fcdb-b3d4-d88c
AP name : ap1
Radio ID : 2
SSID : h3c-macauth
BSSID : ac74-0906-e872
Username : fcdbb3d4d88c
Authentication domain : clearpass
Initial VLAN : 1308
Authorization VLAN : 1308
Authorization ACL number : N/A
Authorization user profile : N/A
Authorization CAR : N/A
Authorization URL : N/A
Termination action : N/A
Session timeout last from : N/A
Session timeout period : N/A
Online from : 2019/03/16 10:37:14

1. 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

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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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
```

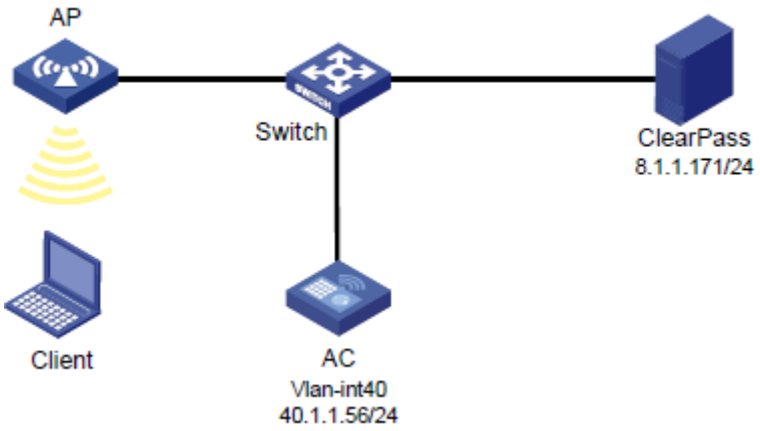
例:ClearPassベースの802.1X EAP-PEAP認証の設定

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。

図11 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

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 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h3c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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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。

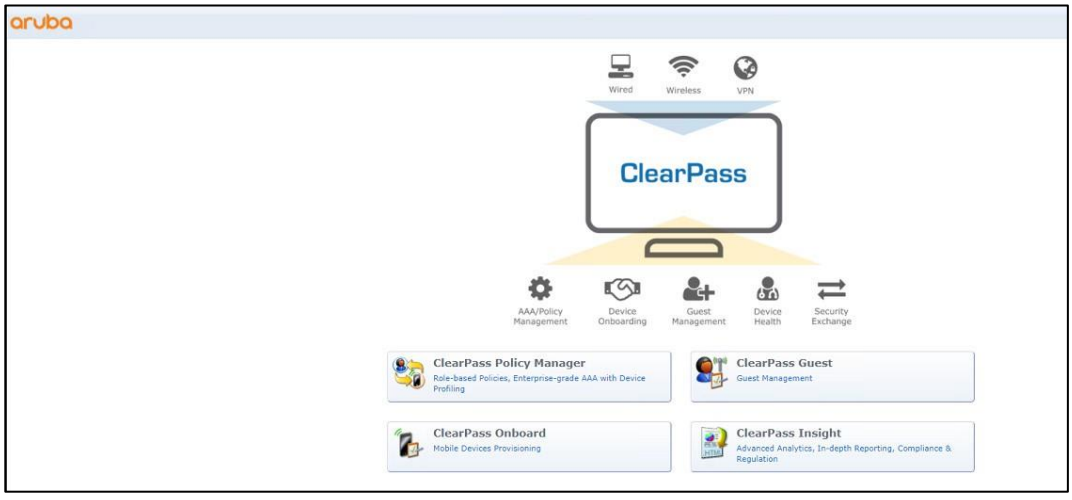
```
#
dhcp server ip-pool vlan1308
  gateway-list 40.8.0.1
  network 40.8.0.0 mask 255.255.0.0
  dns-list 40.8.0.1
#
return
#
```

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。

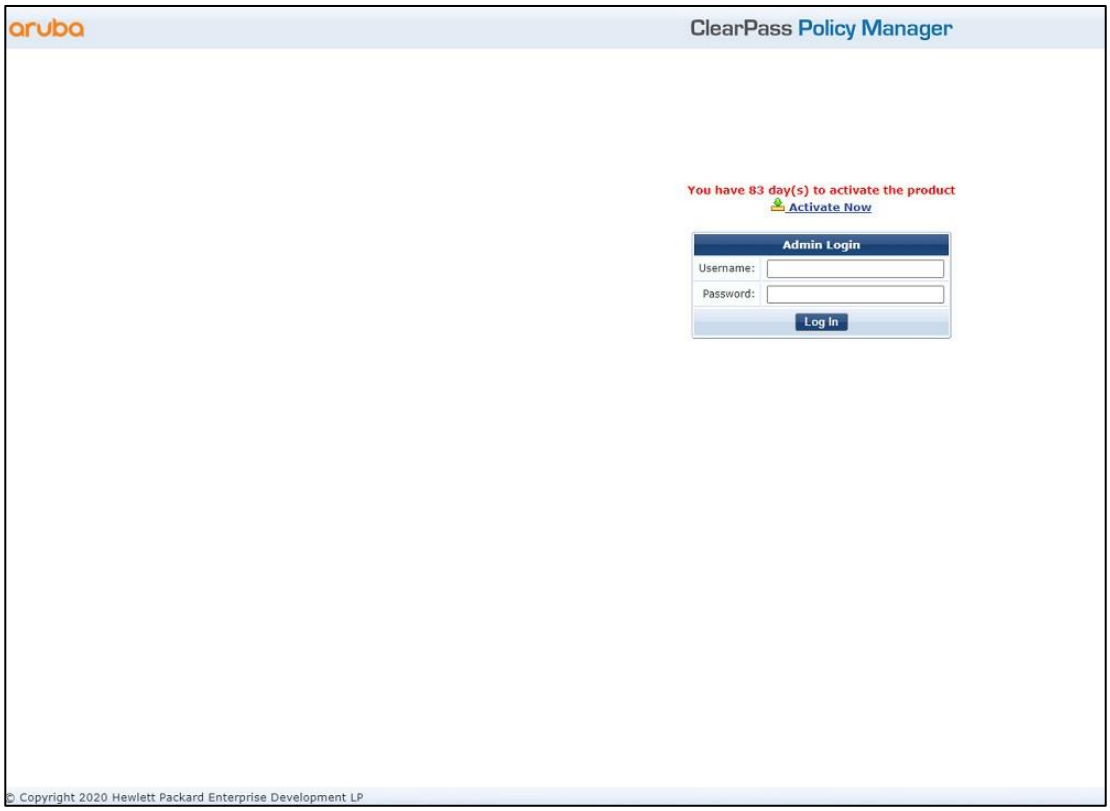
図12 ClearPassへのログイン



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。

図13 ClearPass Policy Managerへのログイン



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。

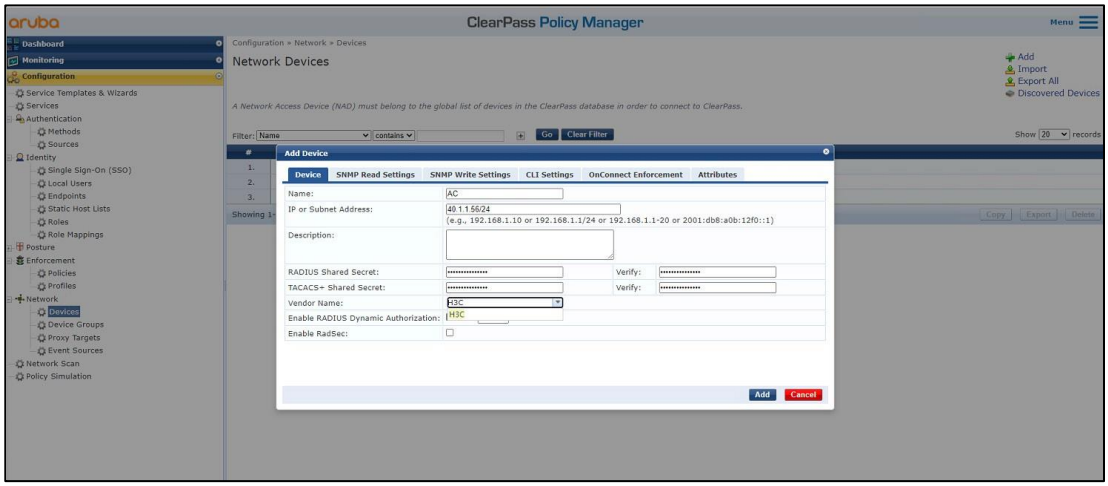
b. RADIUS共有秘密を設定します。

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14 デバイスの追加



3. ユーザーの追加:

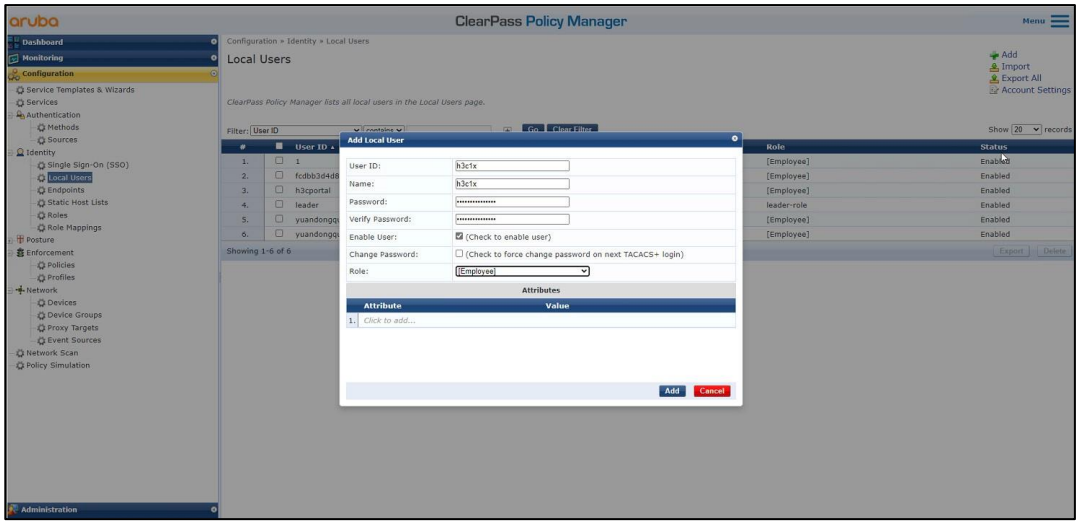
#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたページで、右上隅にあるAddをクリックします。

a. ユーザーID、名前、およびパスワードをh3c1xl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。

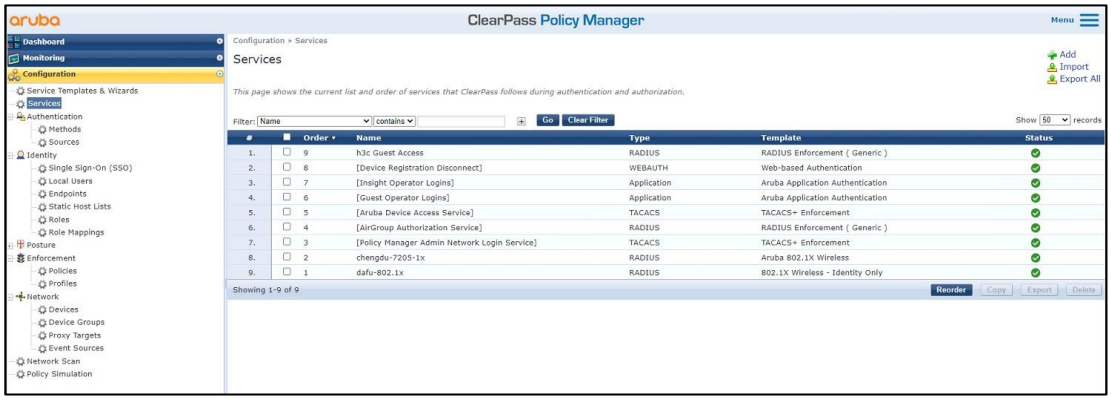
図15 ユーザーの追加



4. サービスを追加します。

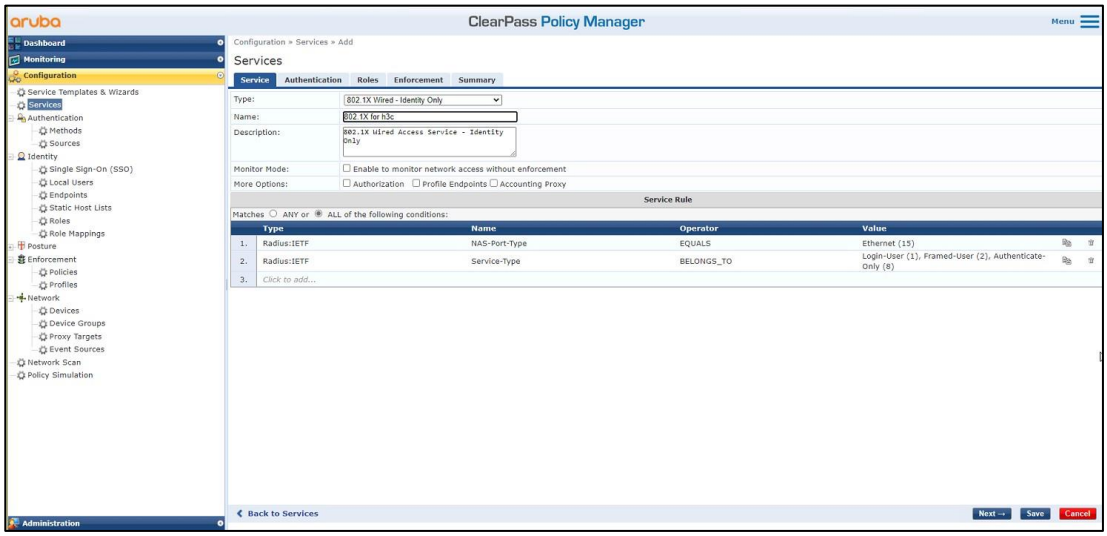
#左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、右上隅の**Add**をクリックします。

図16 サービスページ



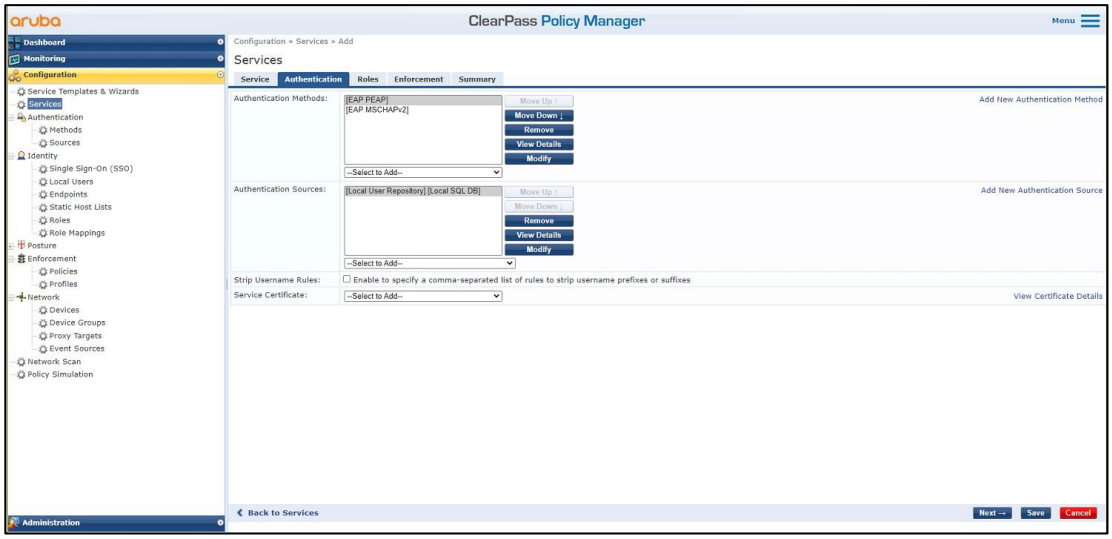
Serviceタブで、**Type**フィールドから**802.1X Wireless-Identity Only**を選択し、h3cの名前を802.1Xに設定します。

図17 サービスの追加



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。

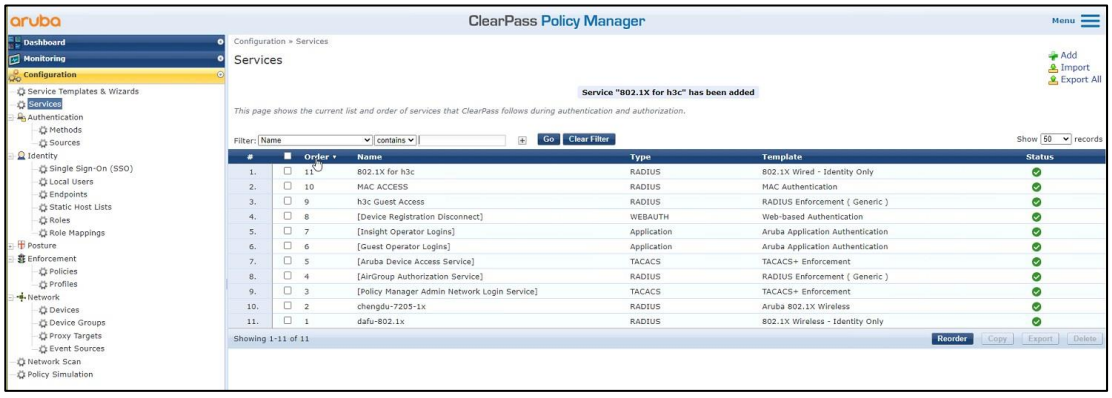
図18 認証の構成



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



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。

```
[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
Total 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/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 : RSN
AKM mode : 802.1X
Cipher suite : CCMP
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
Key derivation : SHA1
PMF status : N/A
Forwarding policy name : Not configured
Online time : 0days 0hours 0minutes 13seconds
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 : 40.8.0.129

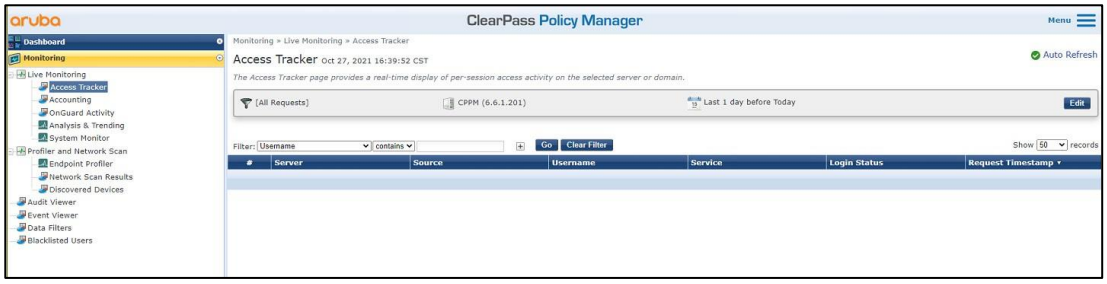
Authentication method : EAP
Initial VLAN : 1308
Authorization VLAN : 1308
Authorization ACL number : N/A
Authorization user profile : N/A
Authorization CAR : N/A
Termination action : N/A
Session timeout last from : N/A
Session timeout period : N/A
Online from : 2019/03/16 11:14:25
Online duration : 0h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



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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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

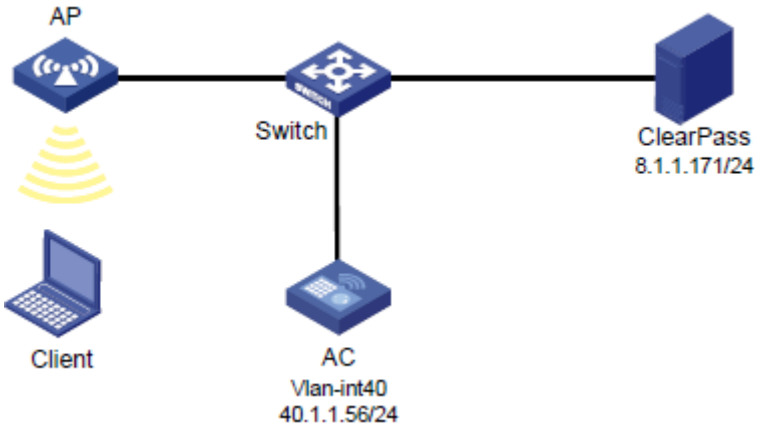
ネットワーク構成

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。

図21 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

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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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。

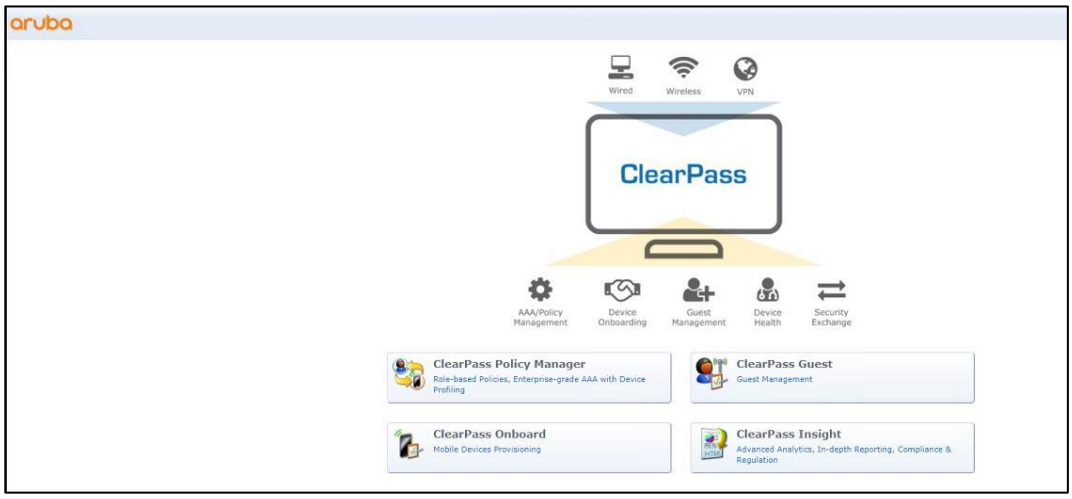
```
#
dhcp server ip-pool vlan1308
   gateway-list 40.8.0.1
   network 40.8.0.0 mask 255.255.0.0
   dns-list 40.8.0.1
#
dhcp server ip-pool vlan1309
   gateway-list 40.9.0.1
   network 40.9.0.0 mask 255.255.0.0
   dns-list 40.9.0.1
#
```

ClearPassサーバーの設定

1. ClearPassサーバーにログインします。

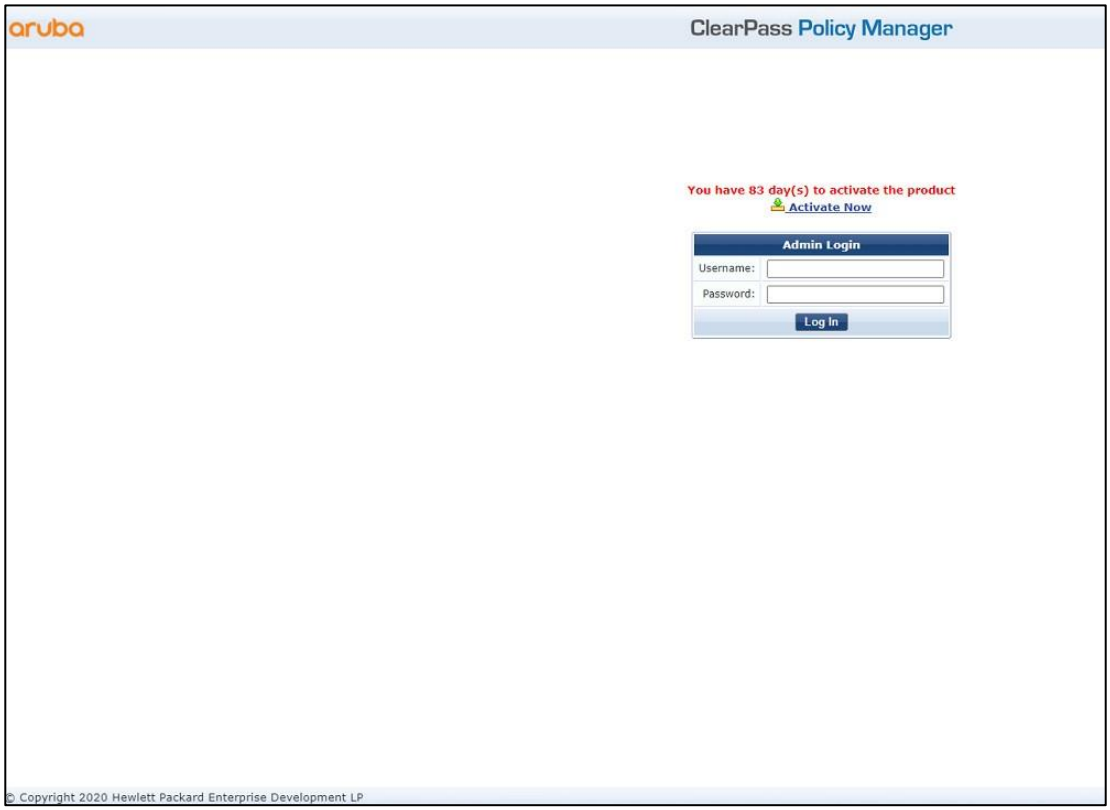
   #サーバーのWebインターフェースにアクセスするには、Webブラウザのアドレスバーに ClearPassサーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。

   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。

図23 ClearPass Policy Managerへのログイン



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。

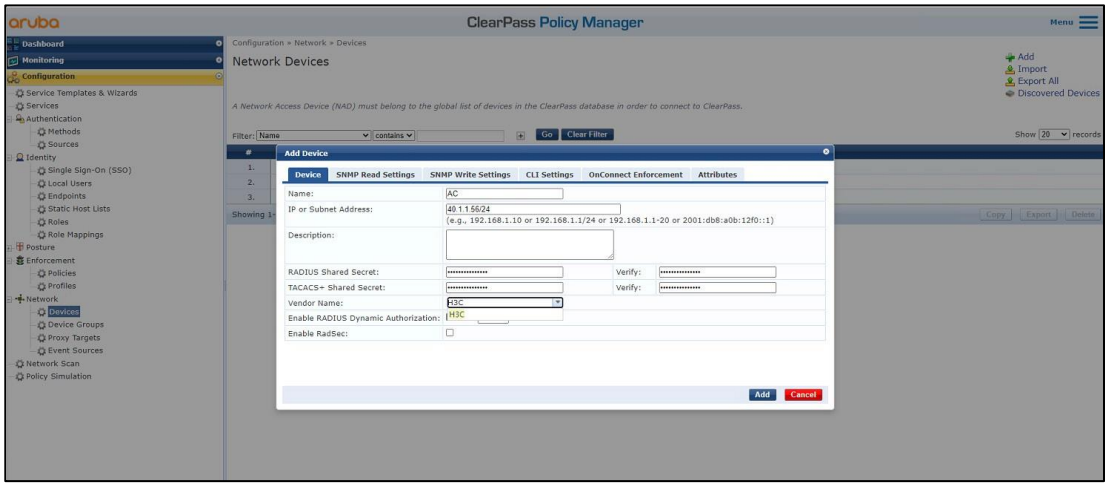
b. RADIUS共有秘密を設定します。

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24 デバイスの追加



3. ユーザーの追加:

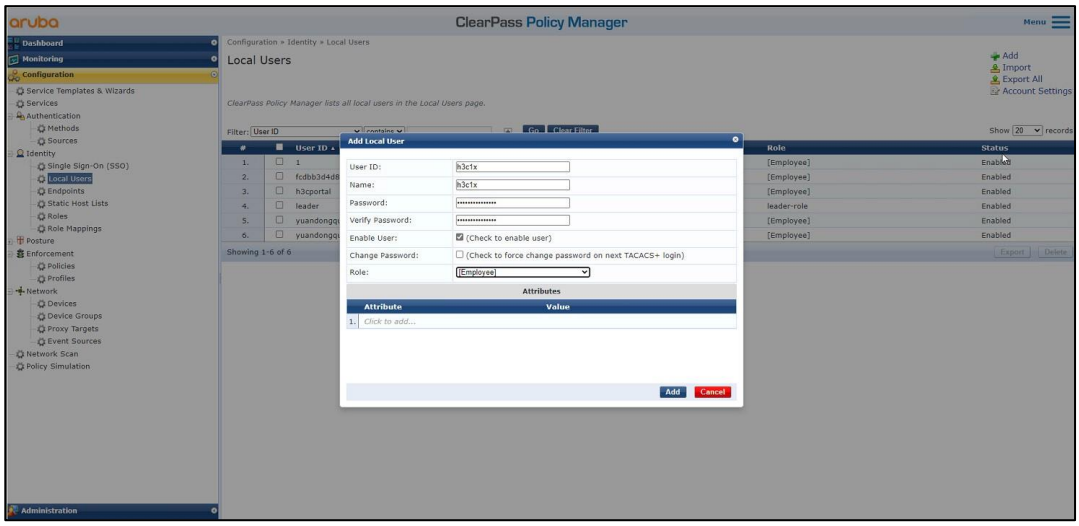
   #左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたページで、右上隅にある**Add**をクリックします。

   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。

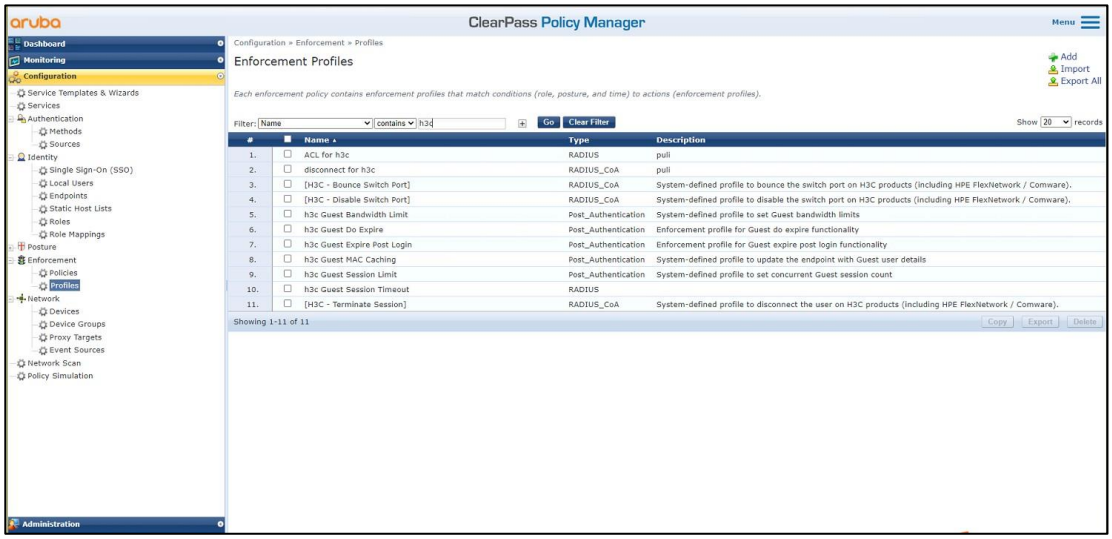
図25 ユーザーの追加



4. enforcementプロファイルを追加します。

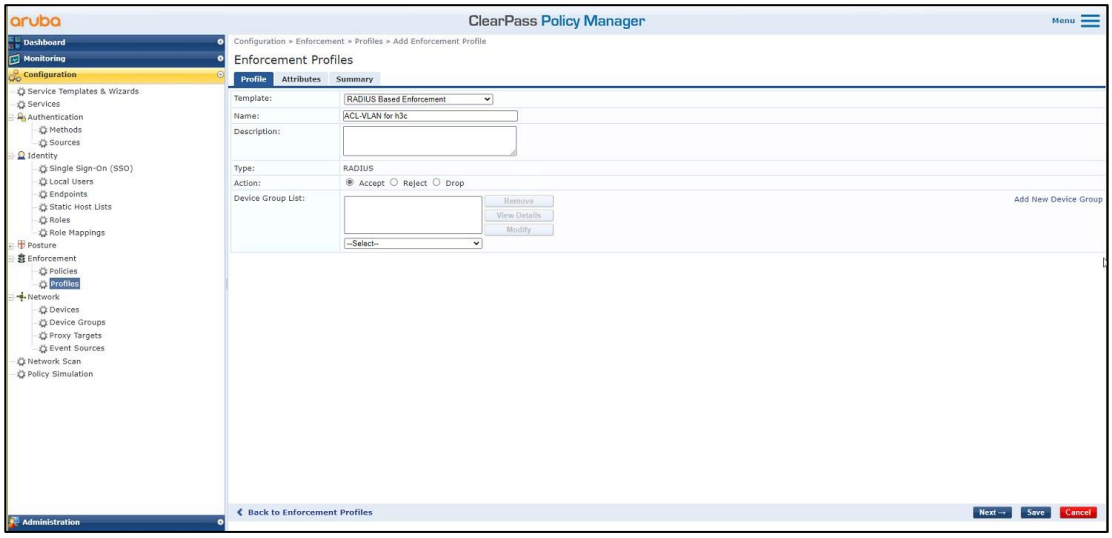
   #左側のナビゲーションペインで、Configuration > Enforcement > Profilesを選択します。開いたページで、右上隅にあるAddをクリックします。

図26 Enforcementプロファイルの追加



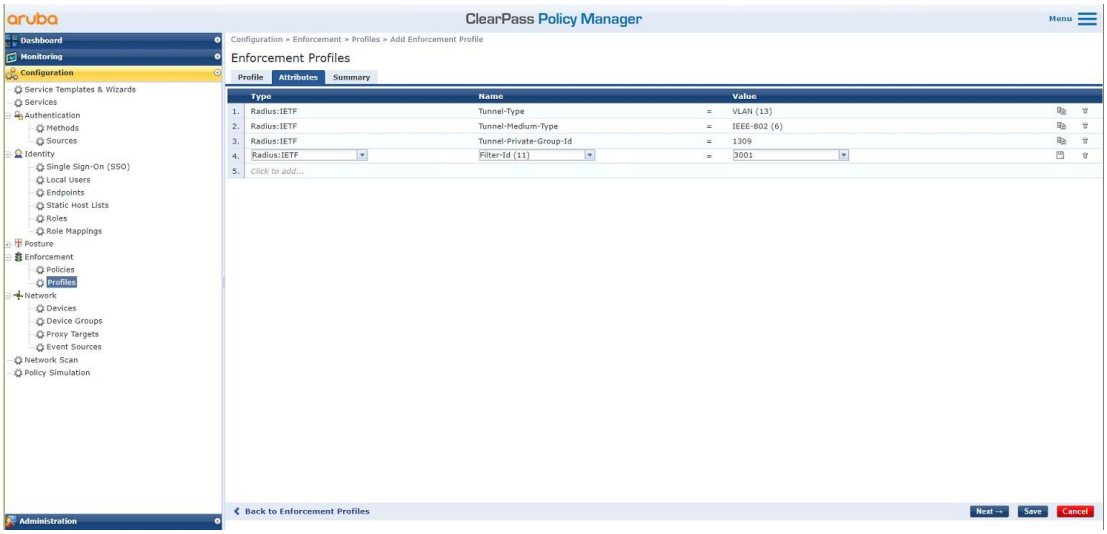
Profileタブで、TemplateフィールドのRADIUS Based Enforcementを選択し、h3cの名前をACL-VLANに設定します。

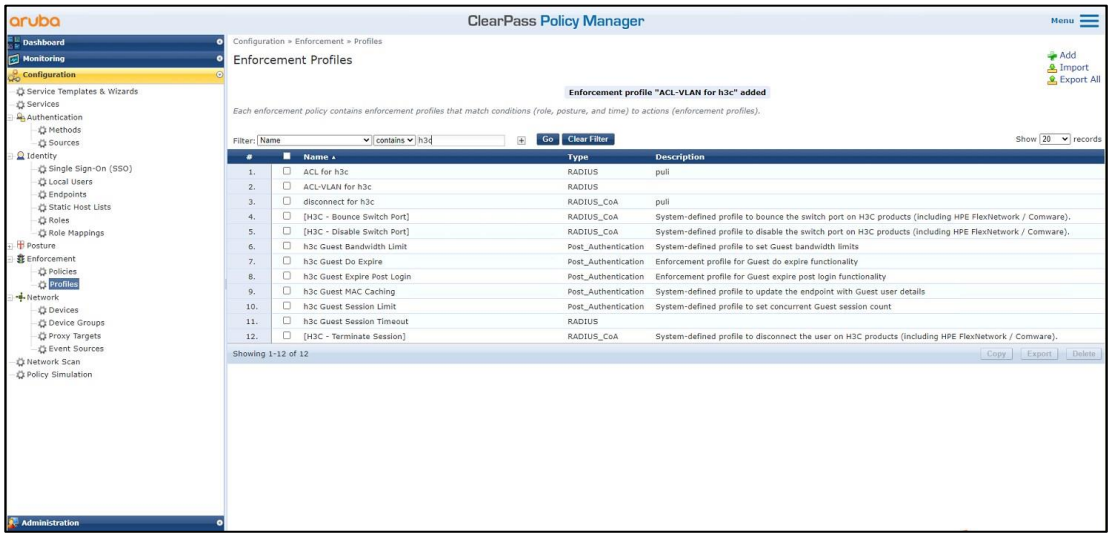
図27 プロファイルの構成



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

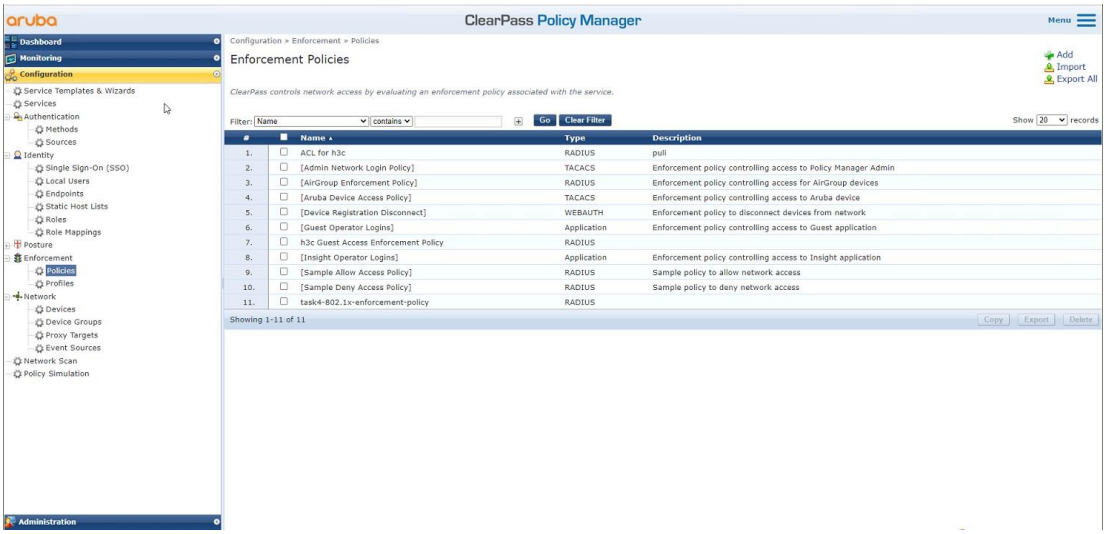




5. 適用ポリシーを追加します。

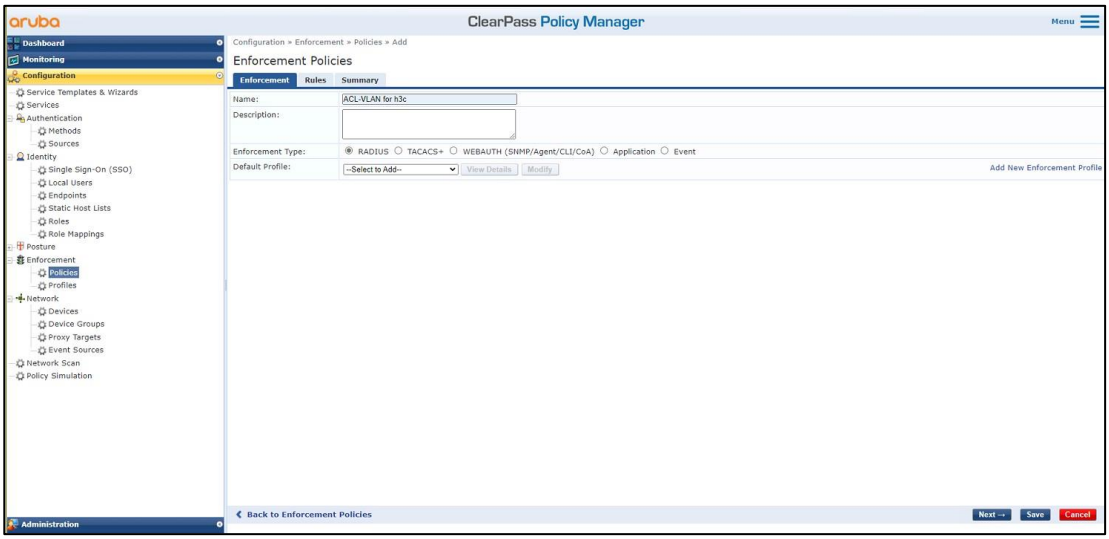
#左側のナビゲーションペインで、Configuration > Enforcement > Policiesを選択します。表示されたページの右上隅にあるAddをクリックします。

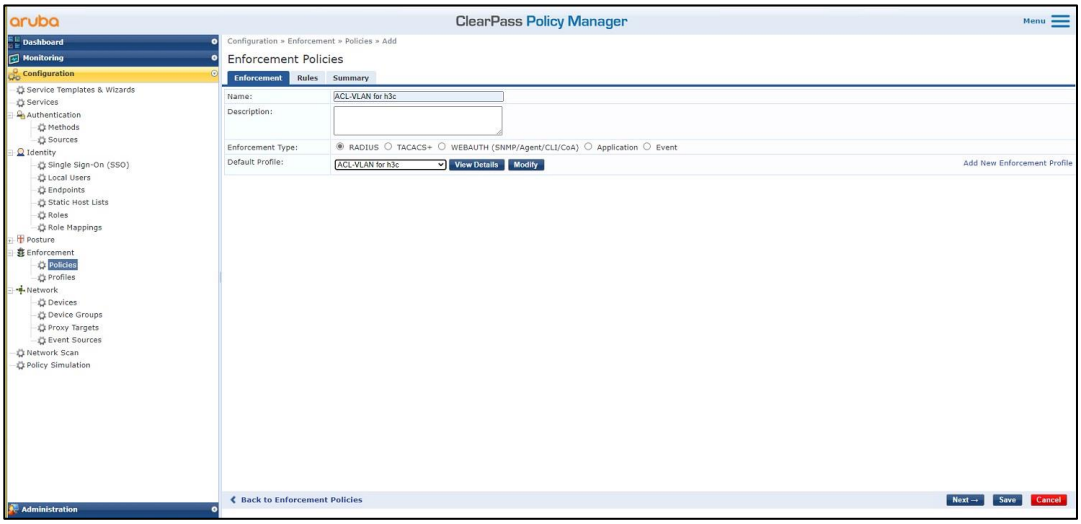
図29 Enforcementポリシーの追加



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。

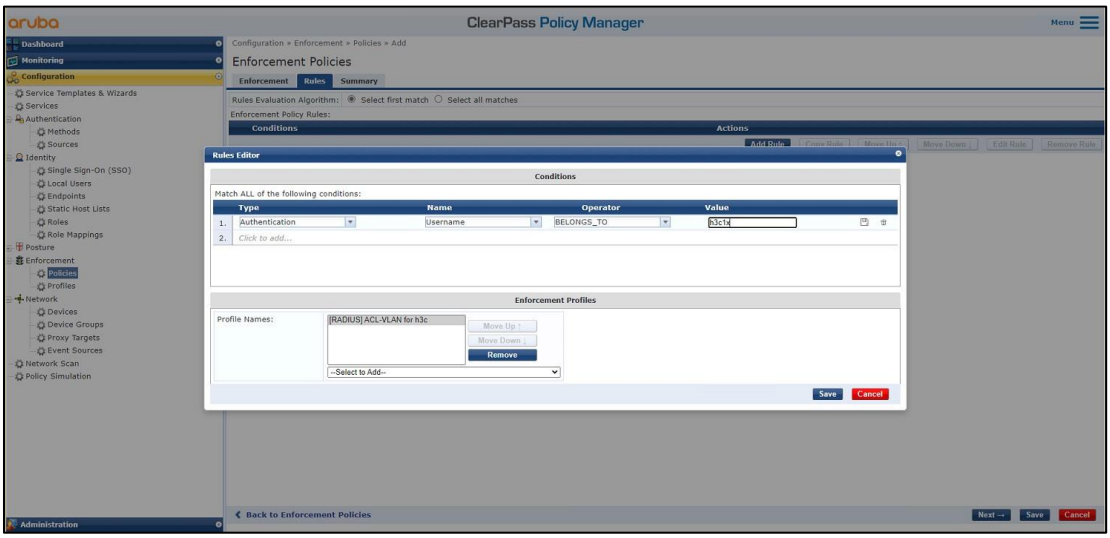
図30 ポリシーの構成

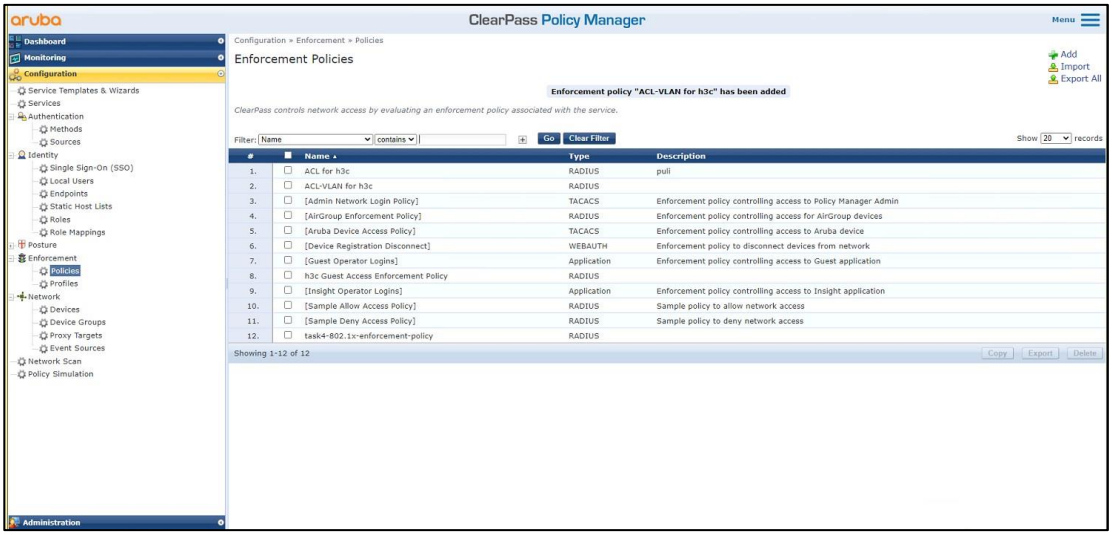




Rulesタブで、フィルタ条件を設定し、適用プロファイルを選択します。
RADIUS:ACL-VLAN for h3cを選択し、Saveをクリックします。

図31 一致条件の設定

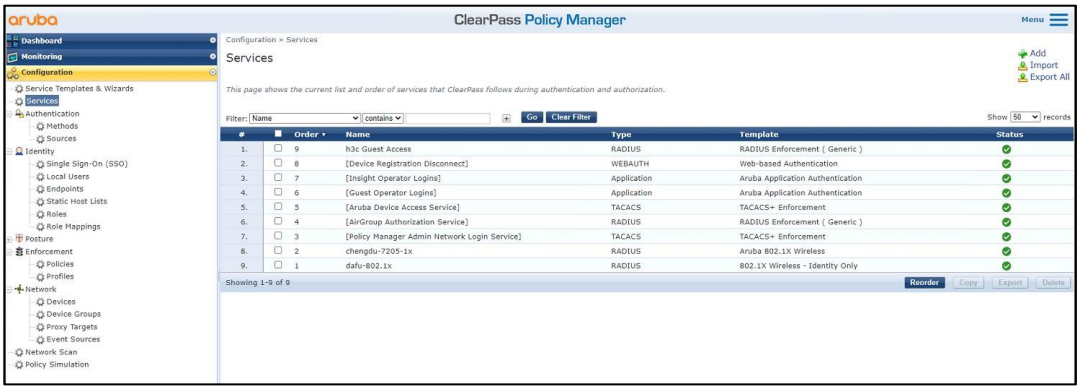




6. サービスを追加します。

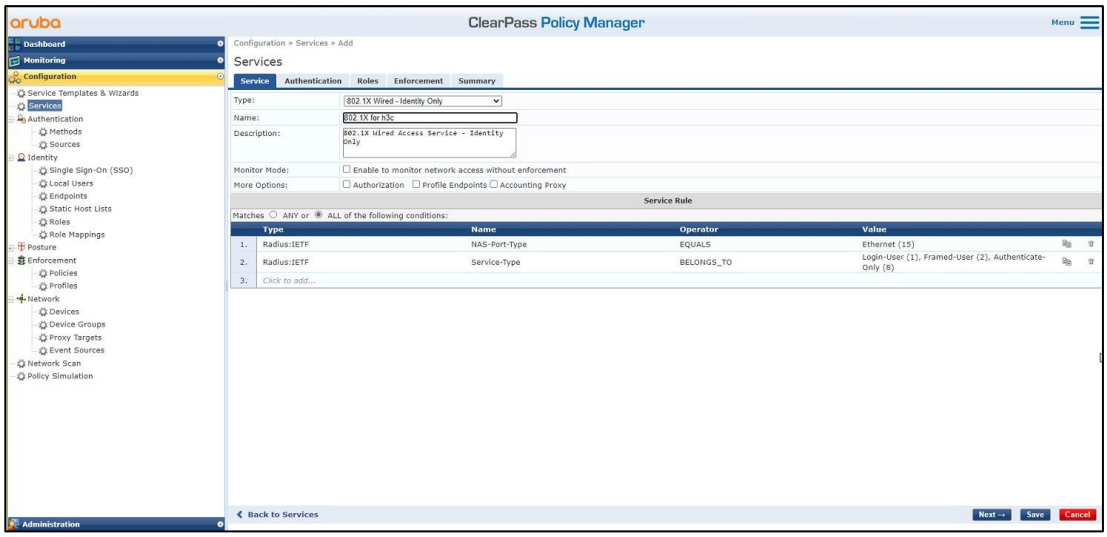
左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、右上隅のAddをクリックします。

図32 Serviceページ



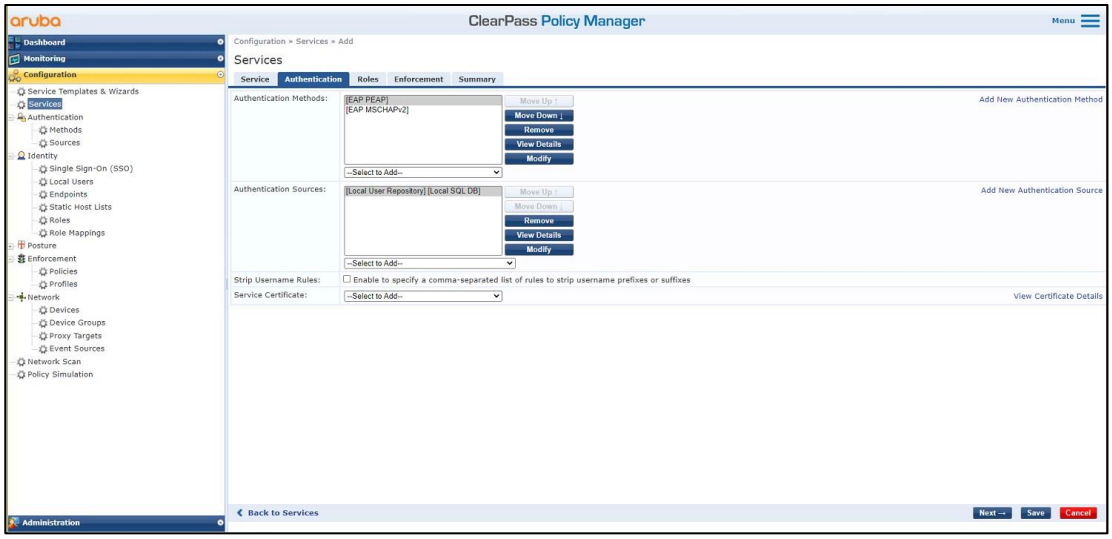
Serviceタブで、Typeフィールドから802.1X Wireless-Identity Onlyを選択し、h3cの名前を802.1Xに設定します。

図33 サービスの追加



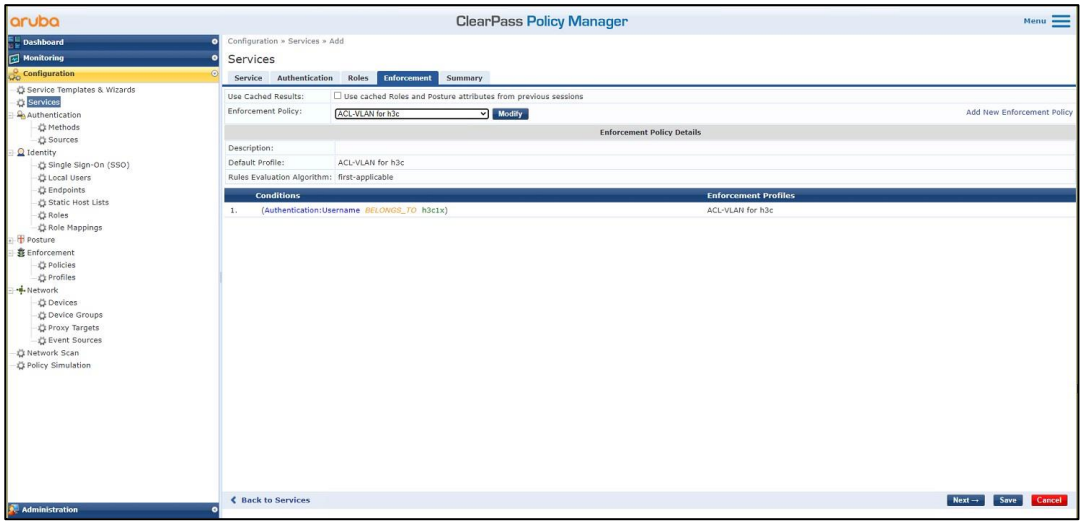
Authenticationタブで、**Authentication Methods**フィールドで**[EAP MSCHAPv2]**および**[EAP PEAP]**を選択し、**Authentication Sources**フィールドで**[Local User Repository][Local SQL DB]**を選択します。

図34 認証の設定



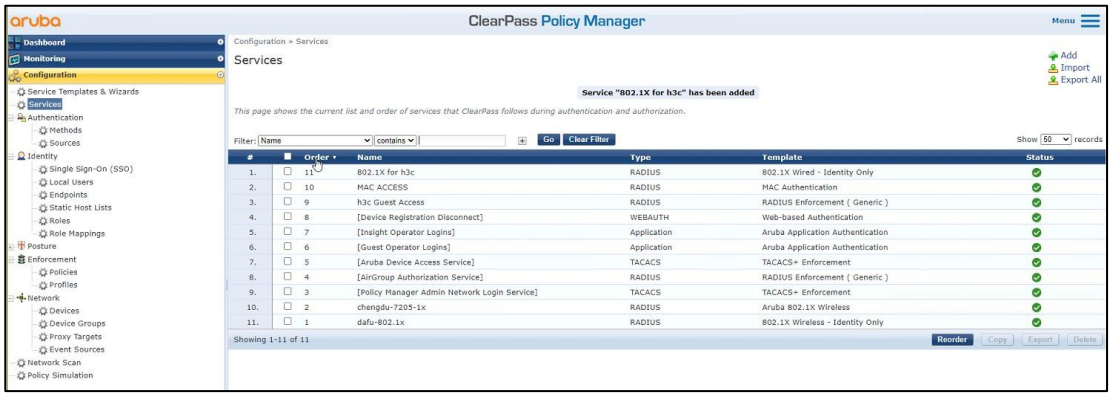
#**Enforcement**タブで、h3cの強制ポリシーACL-VLANを選択し、**Save**をクリックします。

図35 h3c用の実施ポリシーACL-VLANの選択



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



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)。
2. 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
VLAN ID : 1309
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/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 : 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 : 0days 0hours 0minutes 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

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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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

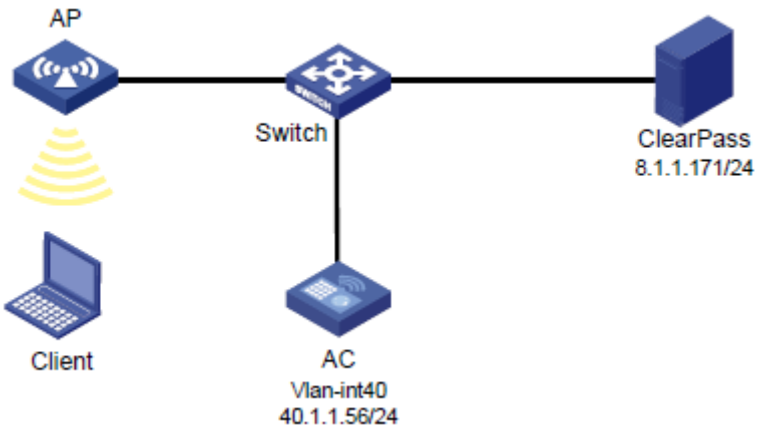
ネットワーク構成

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。

図38 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

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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
   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。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
```

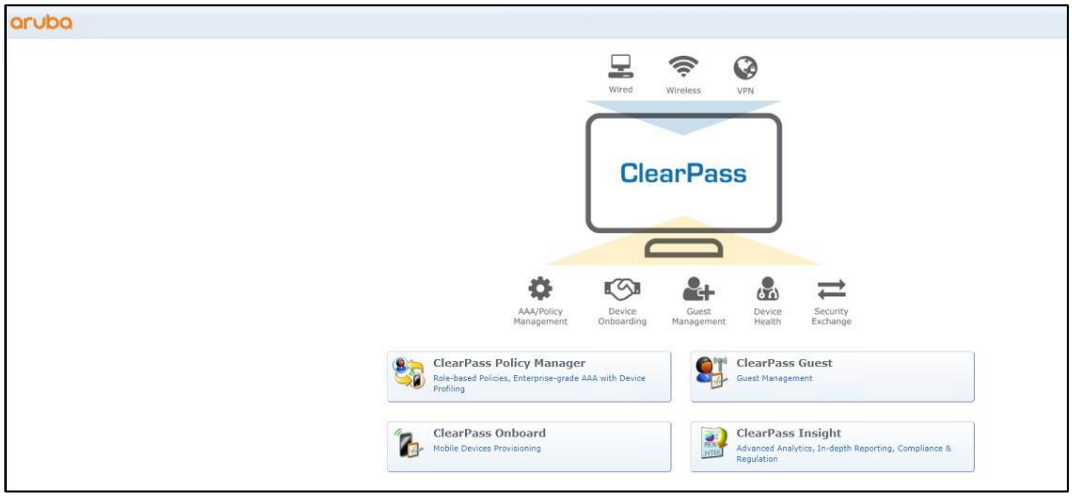
ClearPassサーバーの設定

1. 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。

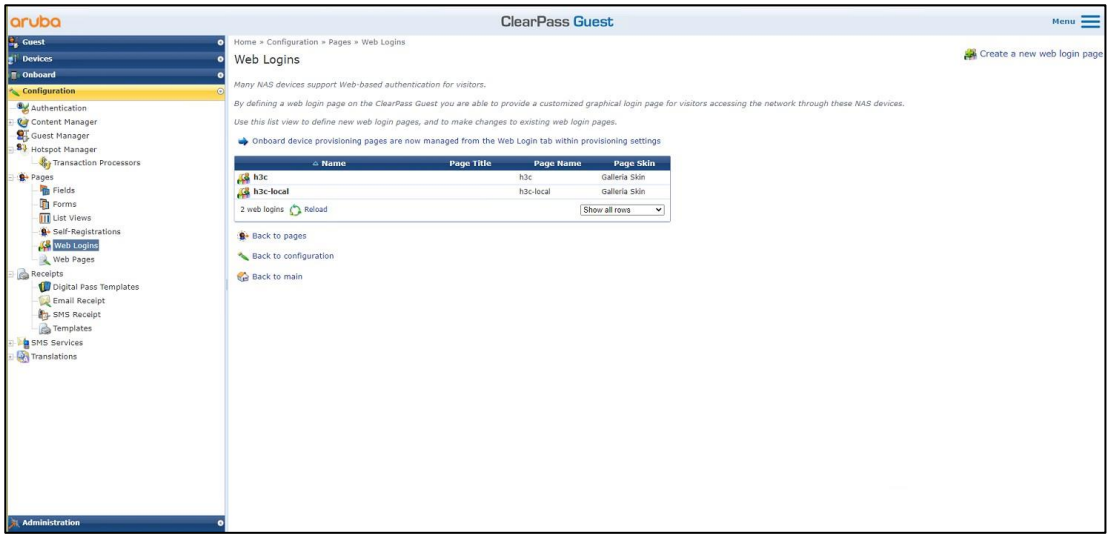
   #ClearPass Guestをクリックします。

   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



#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h3cに設定します。

b. ページ名をh3cに設定します。

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。

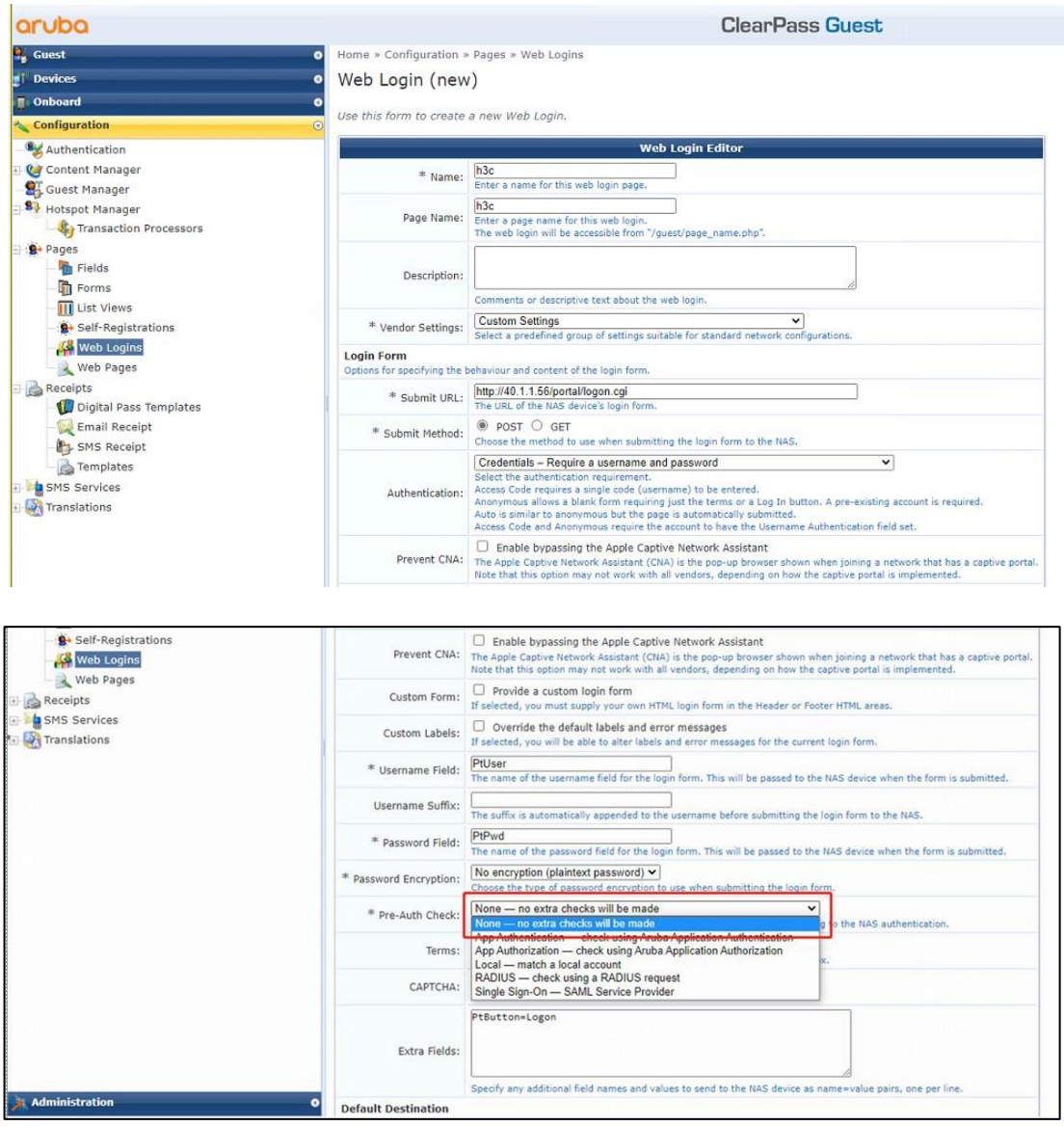
e. Username FieldフィールドにPtUser、Password FieldフィールドにPtPwdと入力しExtra FieldsフィールドにPtButton=Logonと入力します。

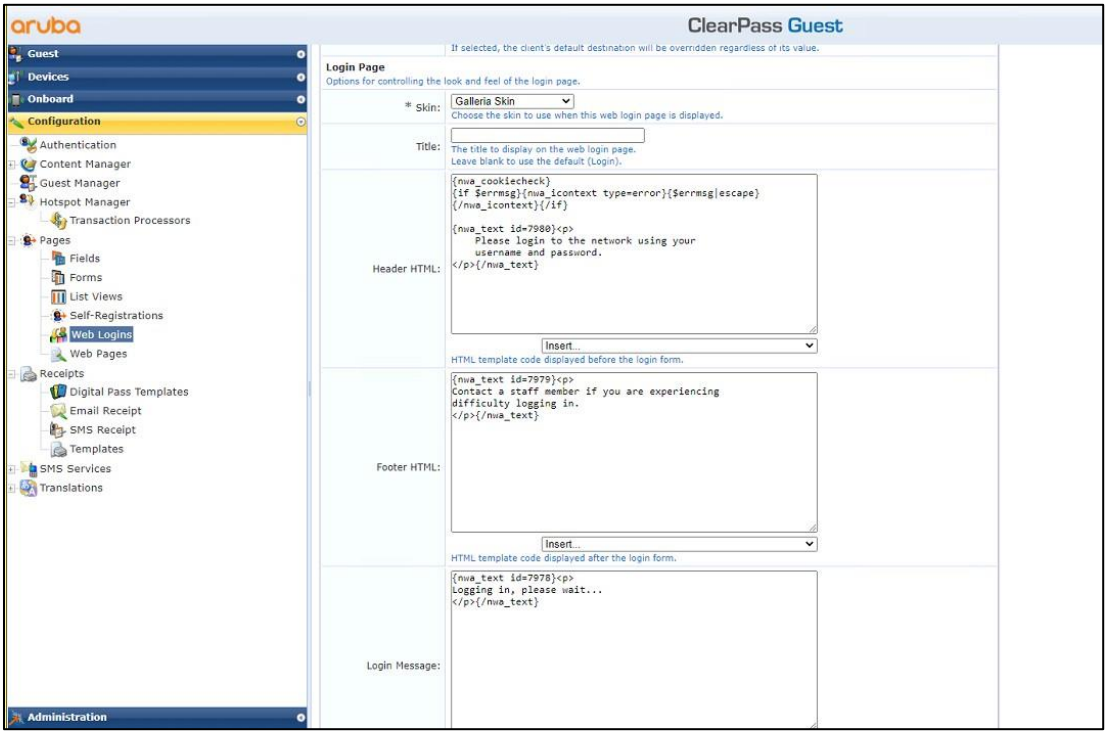
Username Field、Password Field、およびExtra Fieldsフィールドの設定は変更しないことをお勧めします。

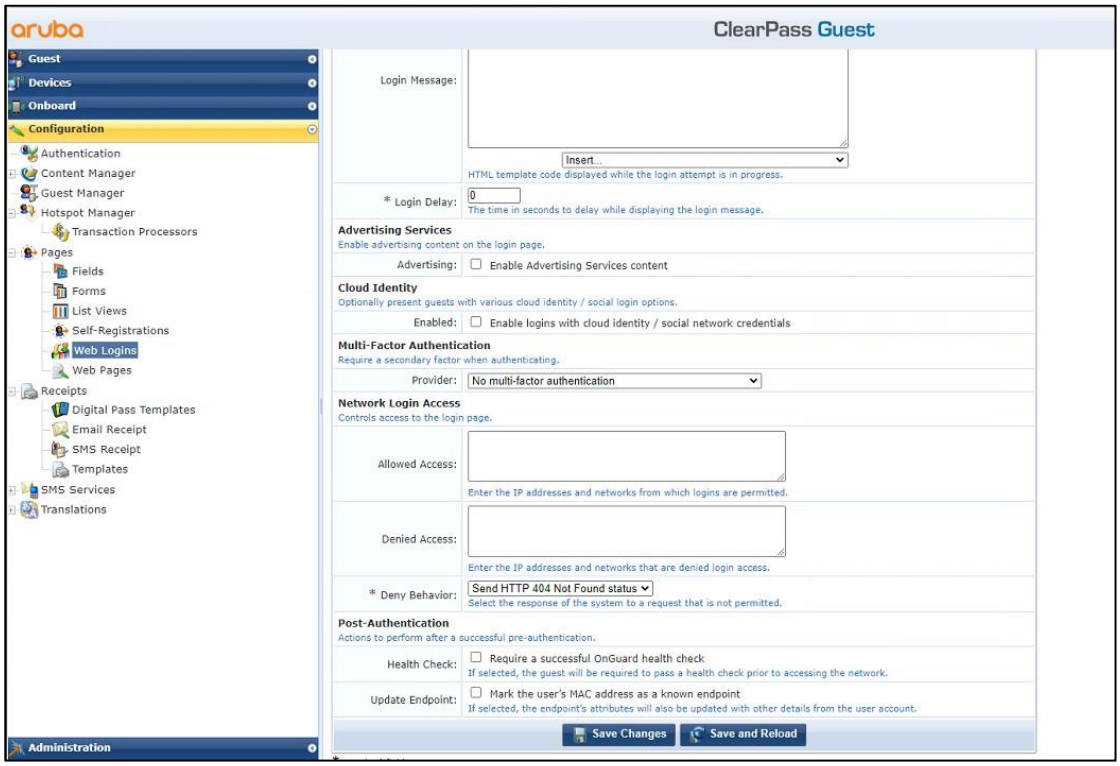
f. 他のパラメータにはデフォルト値を使用します。

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



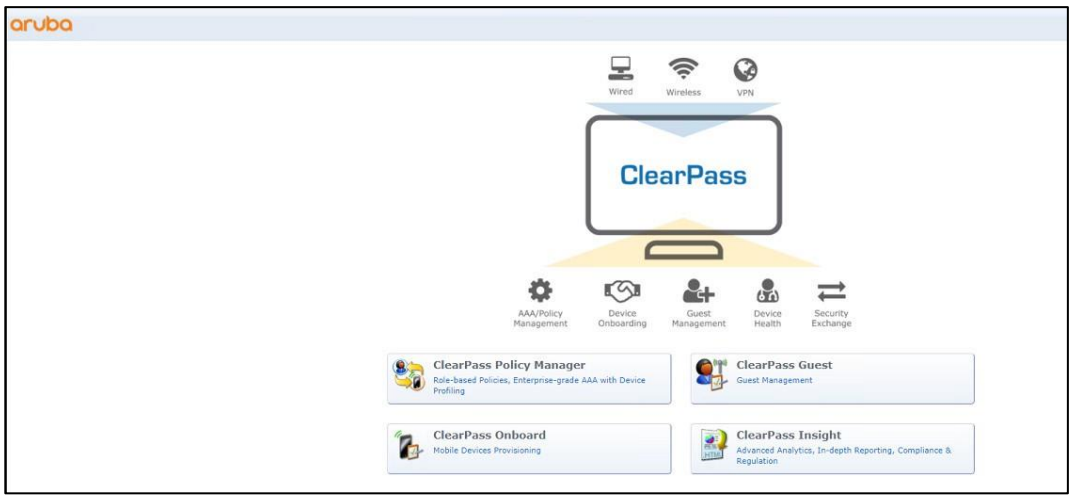




2. ClearPass Policy Managerにログインします。

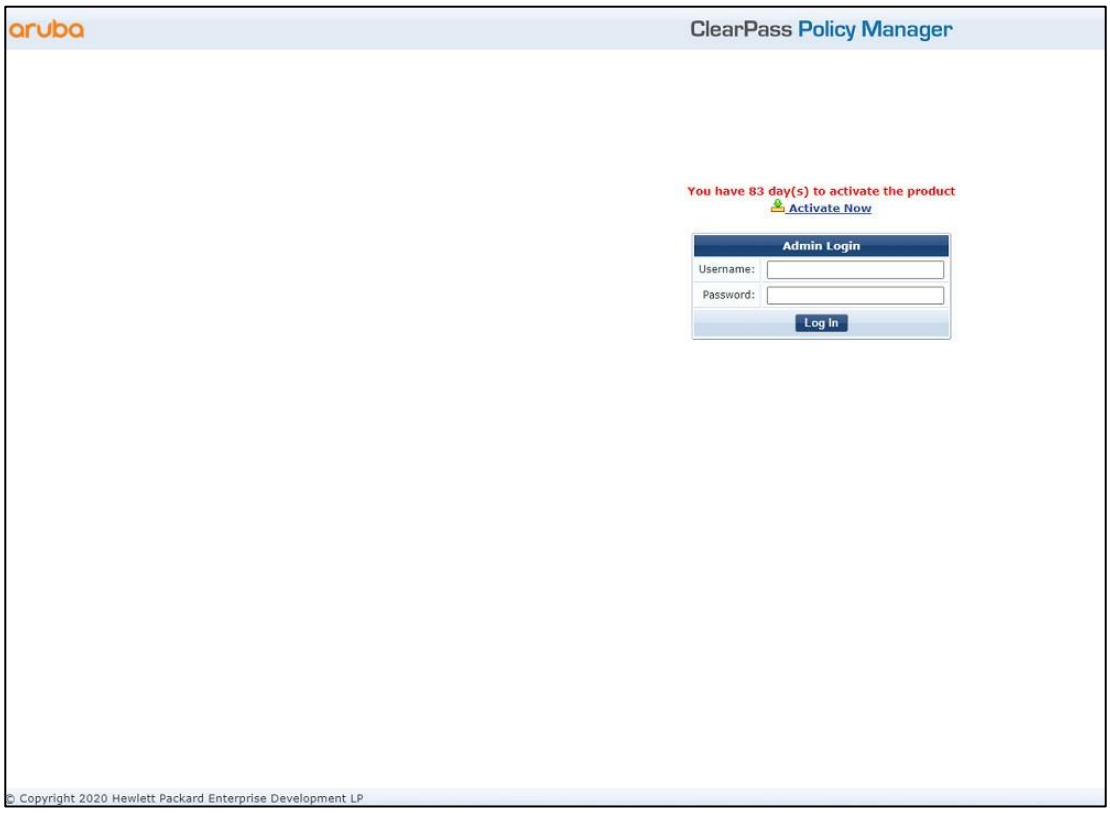
#サーバーのWebインターフェースにアクセスするには、Webブラウザのアドレスバーに ClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。

図42 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。

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。

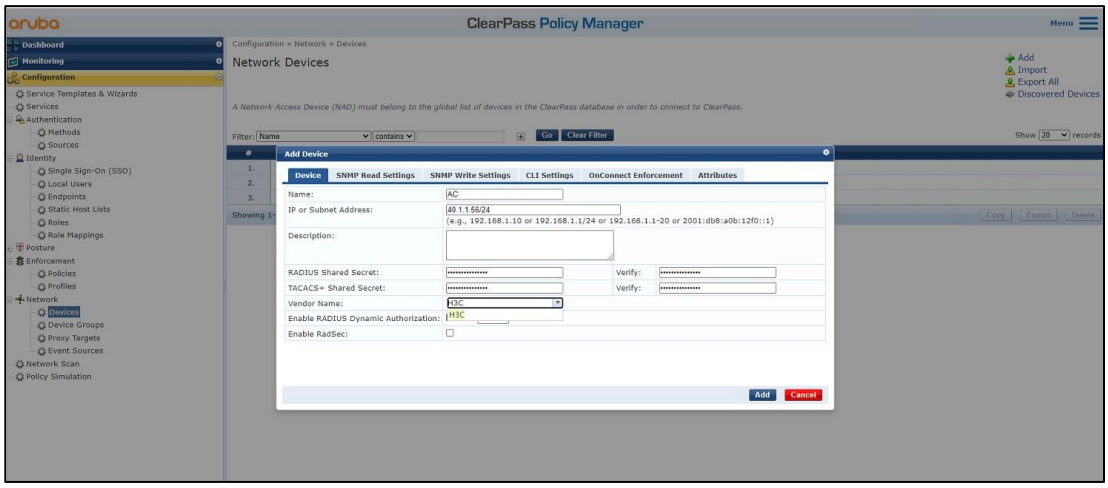
ここで指定した共有シークレットが、AC上のRADIUSサーバーに指定した共有キーと同じである

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



4. ユーザーの追加:

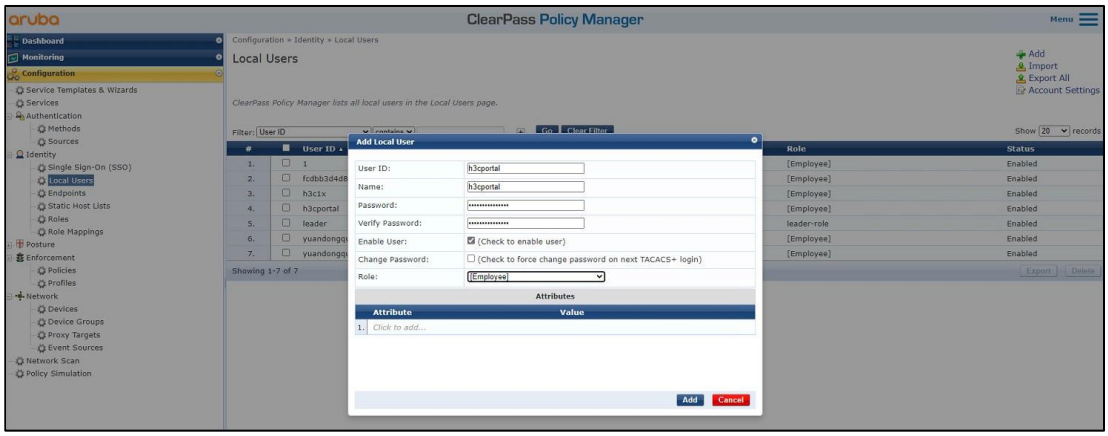
#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたページで、右上隅にあるAddをクリックします。

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。

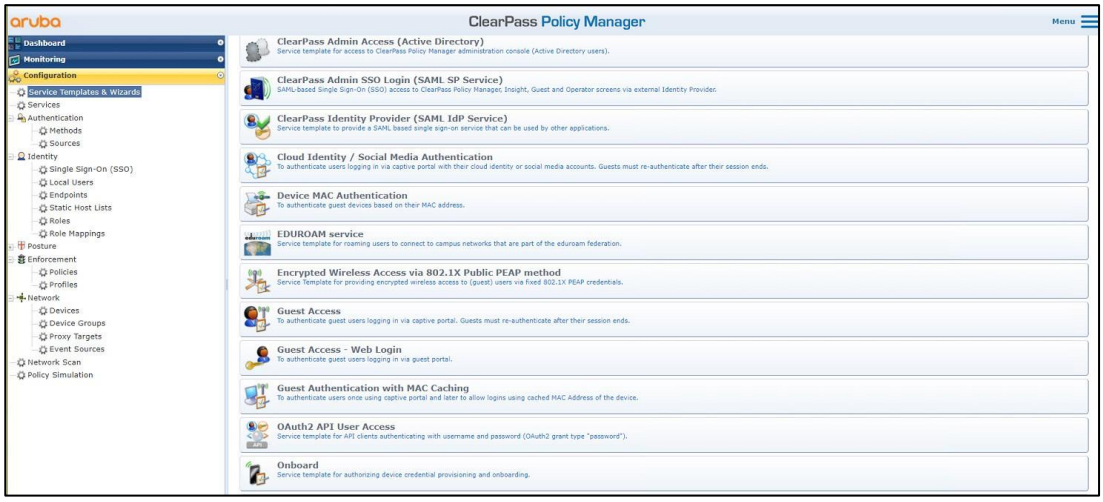
45 ユーザーの追加



5. ゲストアクセスの設定:

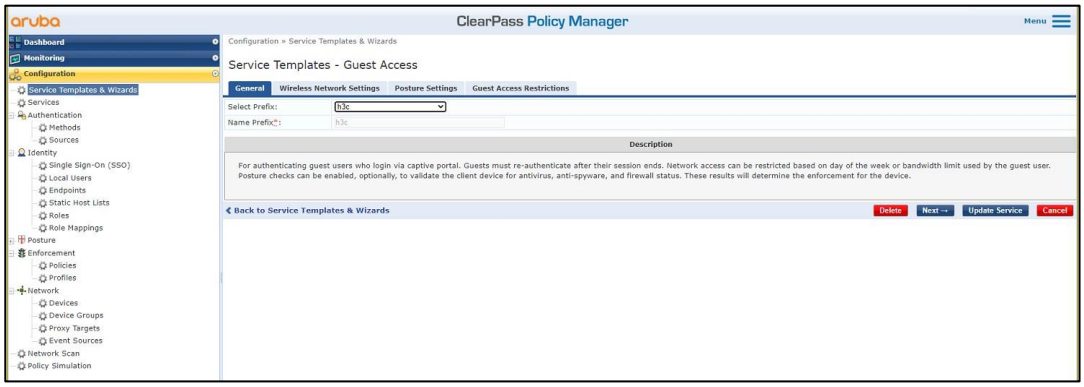
#左側のナビゲーションペインで、Configuration > Service Templates & Wizardsの順に選択します。表示されたページで、Guest Accessを選択します。

図46 ゲストアクセス



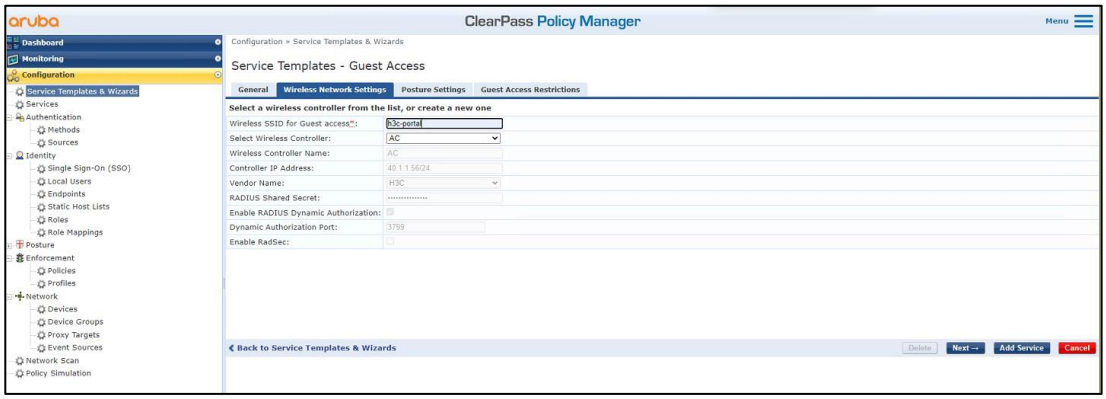
Generalタブで、Select Prefixフィールドのh3cを選択します。

図47 Generalタブ



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。

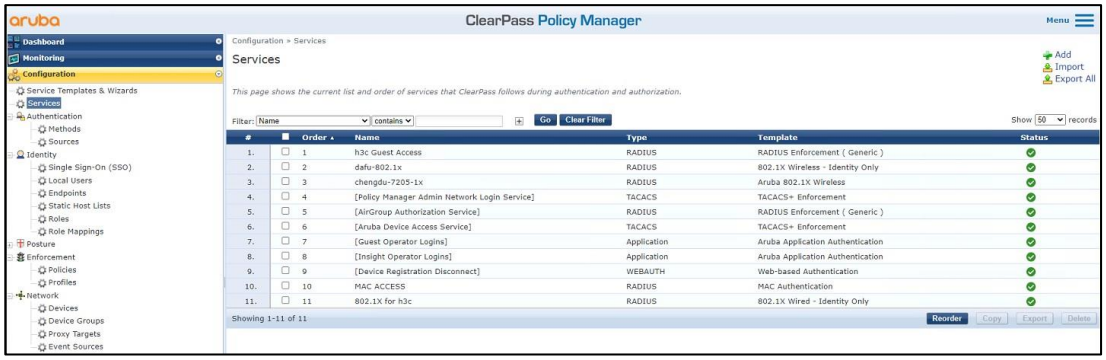
図48 ワイヤレスネットワーク設定の構成



6. サービスを追加します。

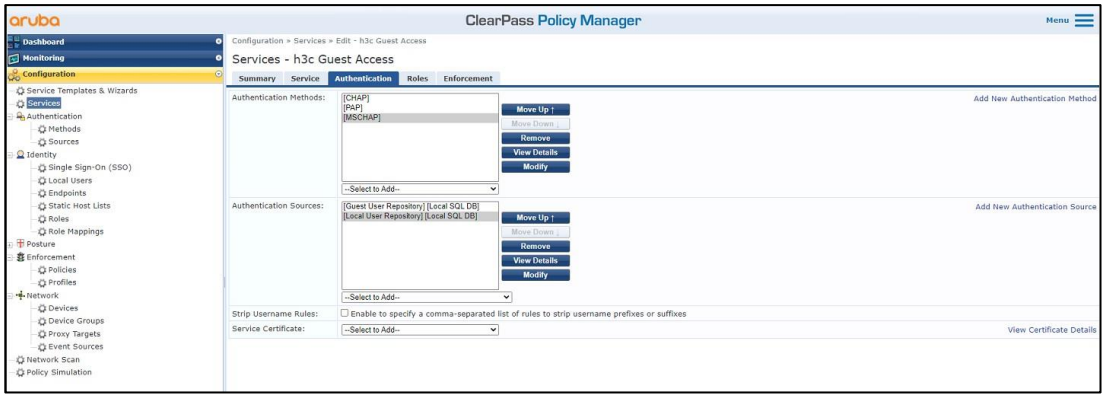
#左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、サービスh3c Guest Accessを追加し、サービスの順序を変更して、サービスh3c Guest Accessを最初のサービスに移動します。

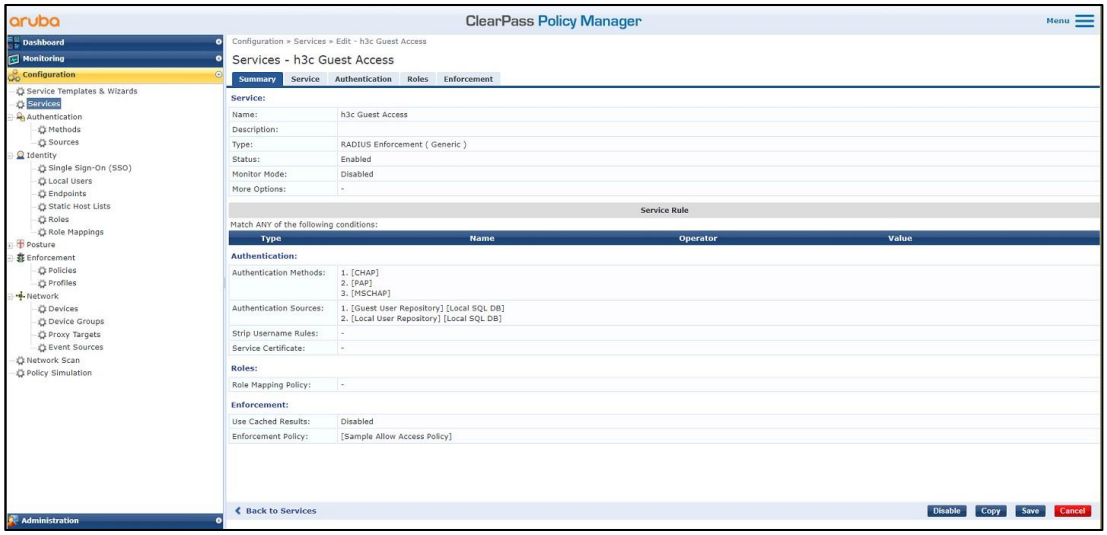
図49 サービスh3c Guest Accessの追加



#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。

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)。
2. 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 clients: 1
MAC address    User name     AP name       R IP address VLAN
fcdb-b3d4-d88c N/A           ap1            1 40.8.0.129 1308

[AC] display wlan client verbose
Total number of clients: 1
MAC address                          : fcdb-b3d4-d88c
IPv4 address                         : 40.8.0.129
IPv6 address                         : N/A
Username                             : N/A
AID                                  : 1
AP ID                                : 26
AP name                              : ap1
Radio ID                             : 1
SSID                                 : h3c-portal
BSSID                                : ac74-0906-e860
VLAN ID                              : 1308
Sleep count                          : 760
Wireless mode                        : 802.11ac
Channel bandwidth                    : 20MHz
SM power save                        : Disabled
Short GI for 20MHz                   : Supported
Short GI for 40MHz                   : Supported
Short GI for 80MHz                   : Supported
Short GI for 160/80+80MHz            : Not supported
STBC RX capability                   : Not supported
STBC TX capability                   : Supported
LDPC RX capability                   : Supported
Beamformee STS capability            : 1
Number of Sounding Dimensions        : 1
SU beamformee capability             : Supported
MU beamformee capability             : Supported
Block Ack                            : TID 0 Both
                                       TID 1 Out
                                       TID 6 In
Supported VHT-MCS set                : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                       NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set                 : 0, 1, 2, 3, 4, 5, 6, 7,
                                       8, 9, 10, 11, 12, 13, 14,15
Supported rates                      : 6, 9, 12, 18, 24, 36,
                                       48, 54 Mbps
QoS mode                             : WMM
Listen interval                      : 10
RSSI                                 : 53
Rx/Tx rate                           : 173.3/173.3 Mbps
Authentication method                : Open system
Security mode                        : PRE-RSNA
AKM mode                             : Not configured
Cipher suite                         : N/A
User authentication mode             : Bypass
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                           : 0days 0hours 11minutes 54seconds
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
   MAC                 IP              VLAN  Interface
   fcdb-b3d4-d88c      40.8.0.129      1308  WLAN-BSS1/0/614
   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: 0x10000009
   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
```

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

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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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

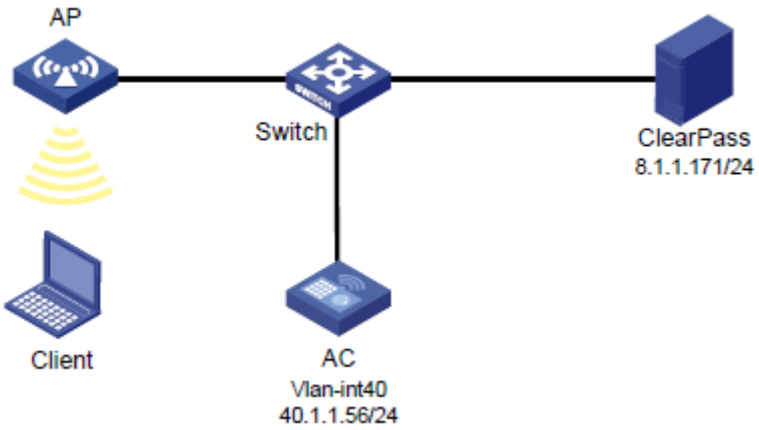
ネットワーク構成

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。

図52 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

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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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
#
```

#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。

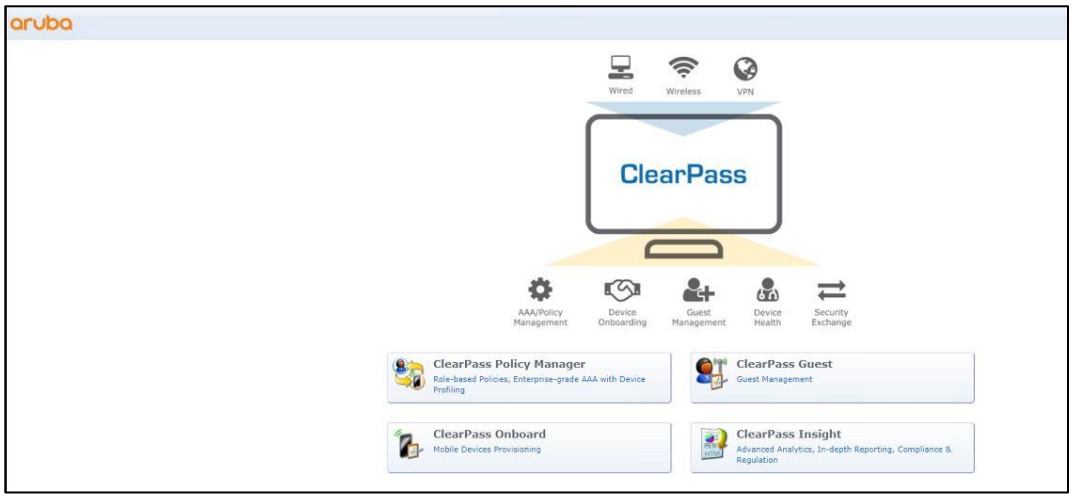
```
#
dhcp server ip-pool vlan1308
   gateway-list 40.8.0.1
   network 40.8.0.0 mask 255.255.0.0
   dns-list 40.8.0.1
#
return
```

ClearPassサーバーの設定

1. ClearPassサーバーにログインします。

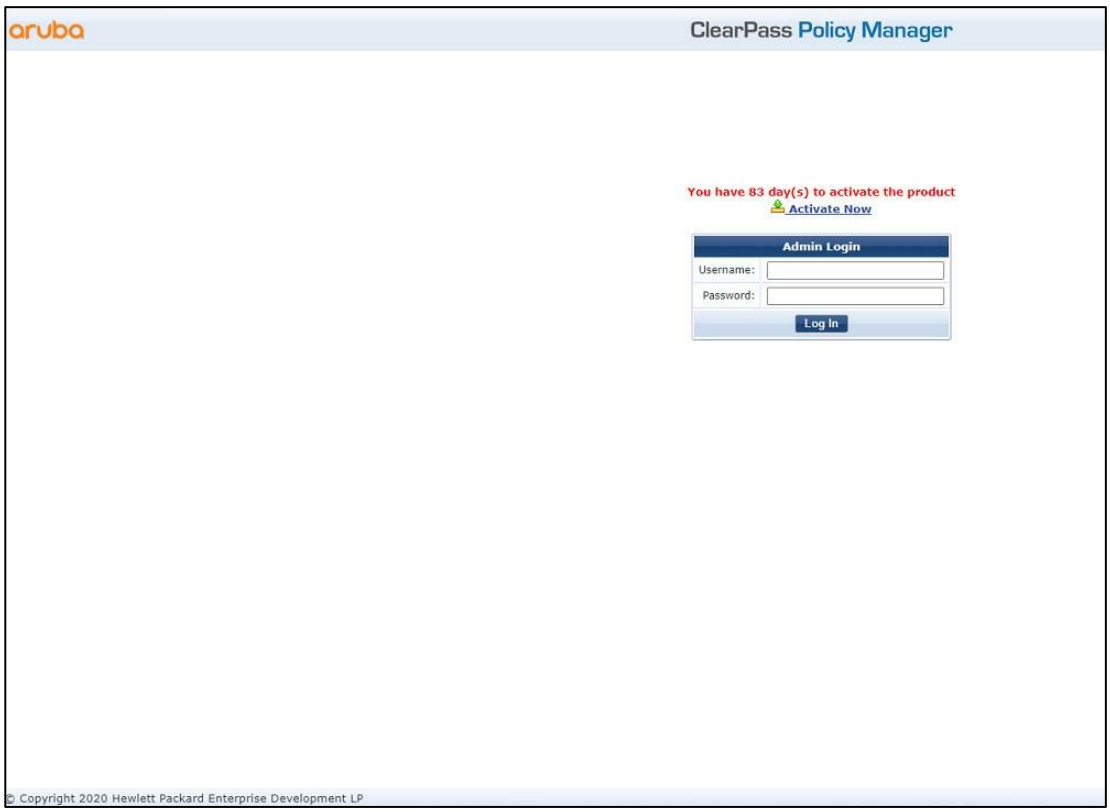
   #サーバーのWebインターフェースにアクセスするには、Webブラウザのアドレスバーに ClearPass サーバーの管理IPアドレスを入力します。この例では、管理IPアドレスは8.1.1.171です。

   図53 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。

図54 ClearPass Policy Managerへのログイン



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。

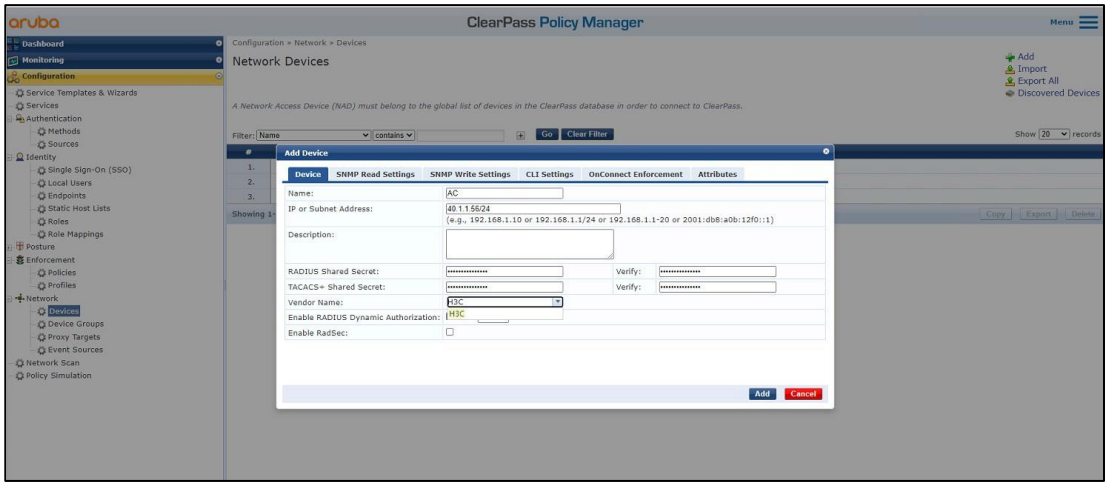
b. RADIUS共有秘密を設定します。

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



3. ユーザーの追加:

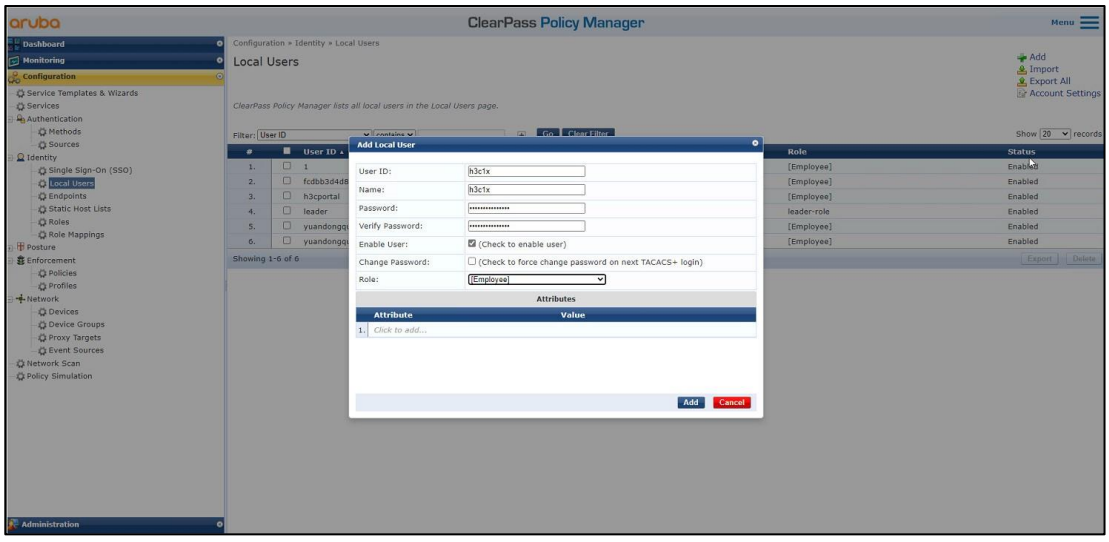
#左側のナビゲーションペインで、Configuration > Identity > Local Usersを選択します。開いたページで、右上隅にあるAddをクリックします。

a. ユーザーID、名前、およびパスワードをh3c1xl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。

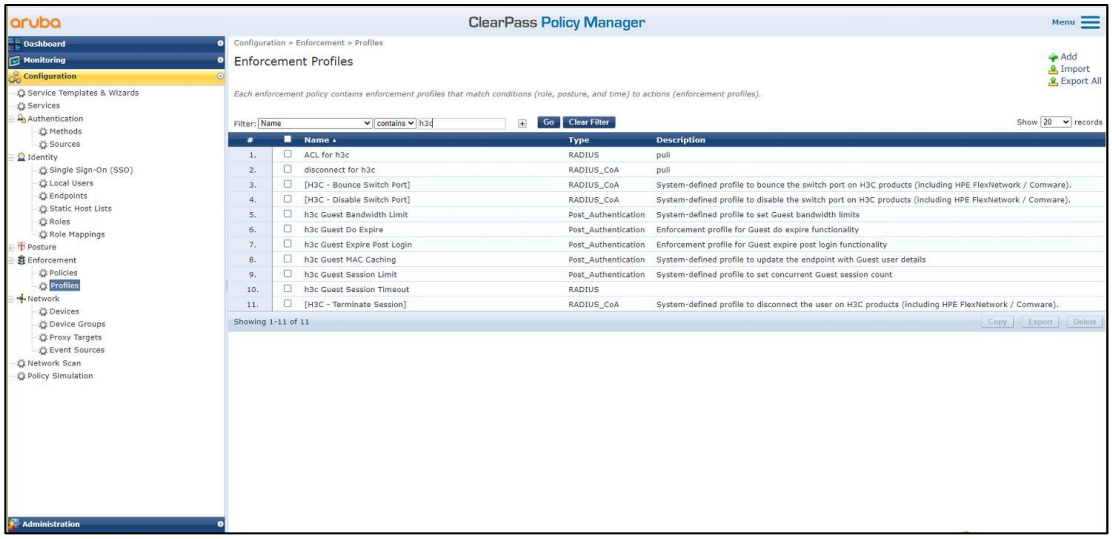
図56 ユーザーの追加



4. enforcementプロファイルを追加します。

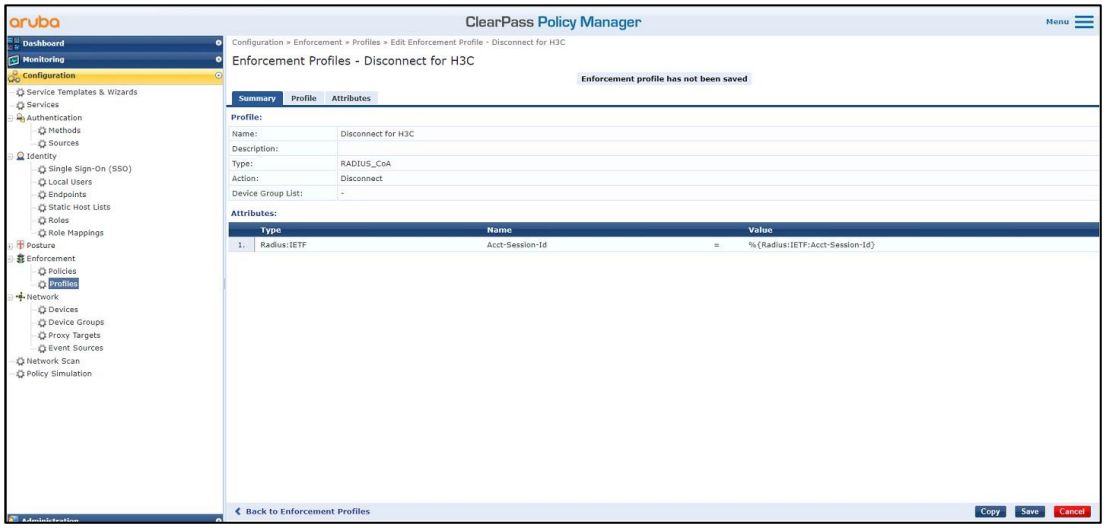
左側のナビゲーションペインで、Configuration > Enforcement > Profilesを選択します。開いたページで、右上隅にある**Add**をクリックします。

図57 enforcementプロファイルの追加



#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

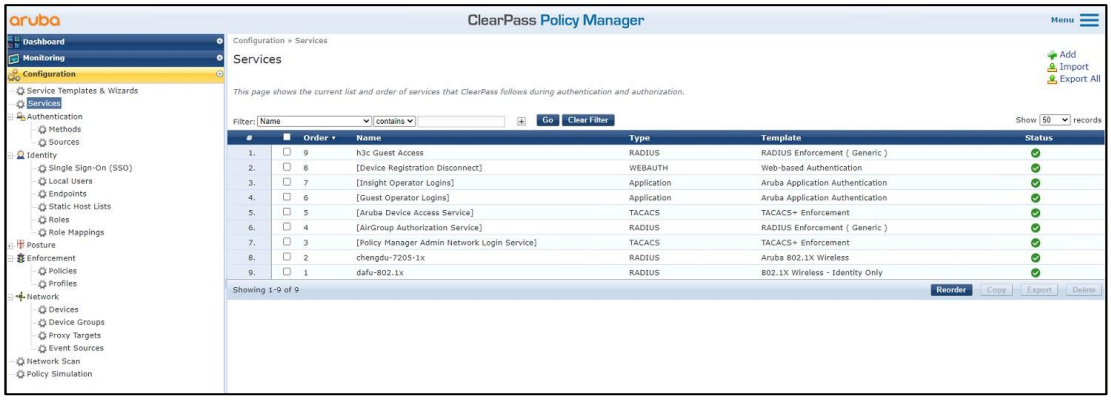


5. 強制ポリシーを追加します。詳細については、「例:VLANおよびACL割り当てを使用したClearPassベースの802.1X認証の設定」を参照してください。

6. サービスを追加します。

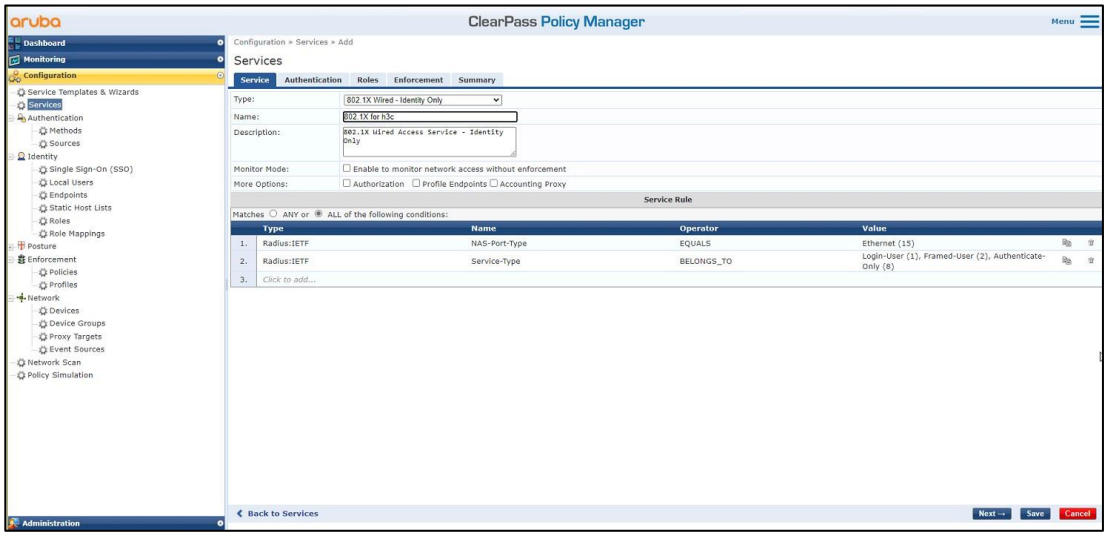
#左側のナビゲーションペインで、Configuration > Servicesを選択します。表示されたページで、右上隅のAddをクリックします。

図59 サービスページ



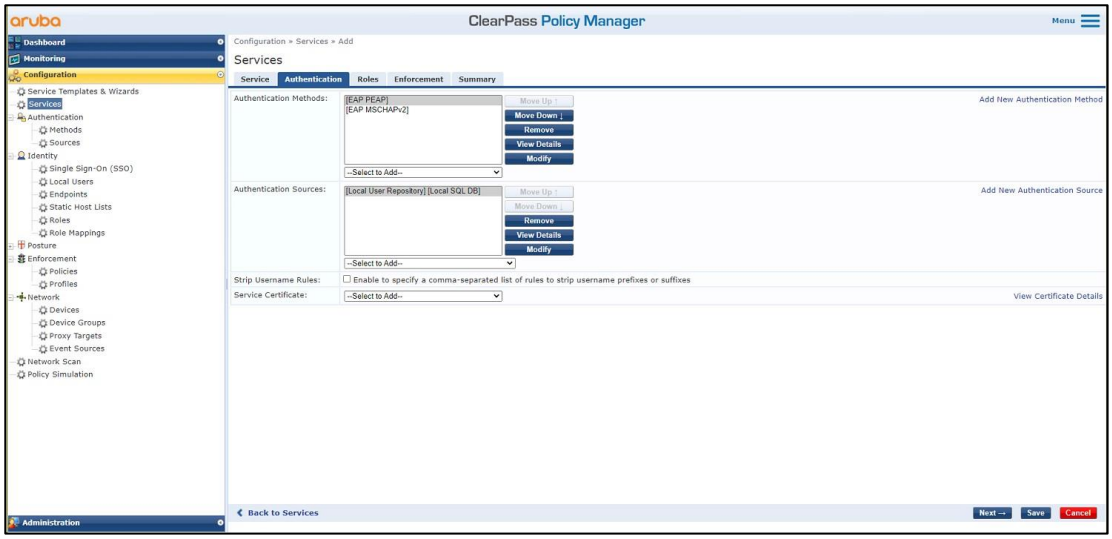
Serviceタブで、**Type**フィールドから802.1X Wireless-Identity Onlyを選択し、h3cの名前を802.1Xに設定します。

図60 サービスの追加



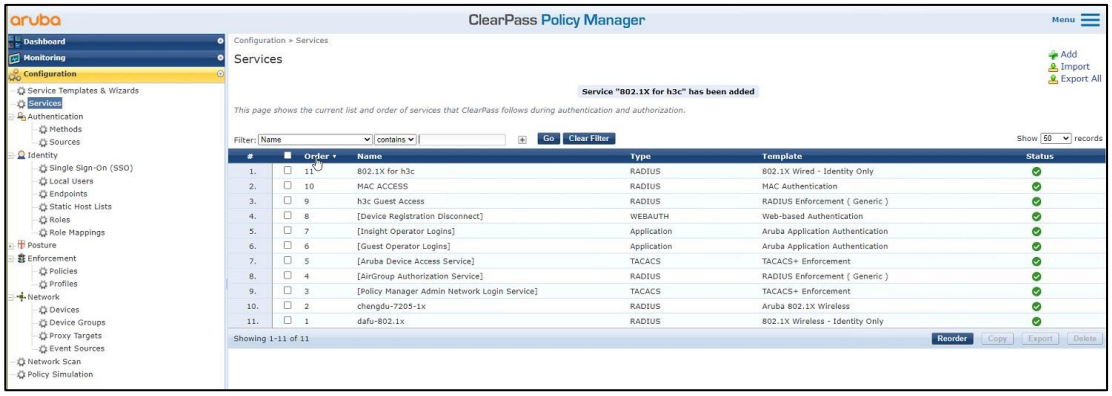
Authenticationタブで、**Authentication Methods**フィールドで**[EAP MSCHAPv2]**と**[EAP PEAP]**を選択し、Authentication Sourcesフィールドで**[Local User Repository]**を選択します。**Enforcement**タブで、**Disconnect for H3C**を選択し、設定を保存します。

図61 サービスの構成



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



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。

```
[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
Total 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/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 : RSN
AKM mode : 802.1X
Cipher suite : CCMP
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
Key derivation : SHA1
PMF status : N/A
Forwarding policy name : Not configured
Online time : 0days 0hours 0minutes 13seconds
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 : 40.8.0.129
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。

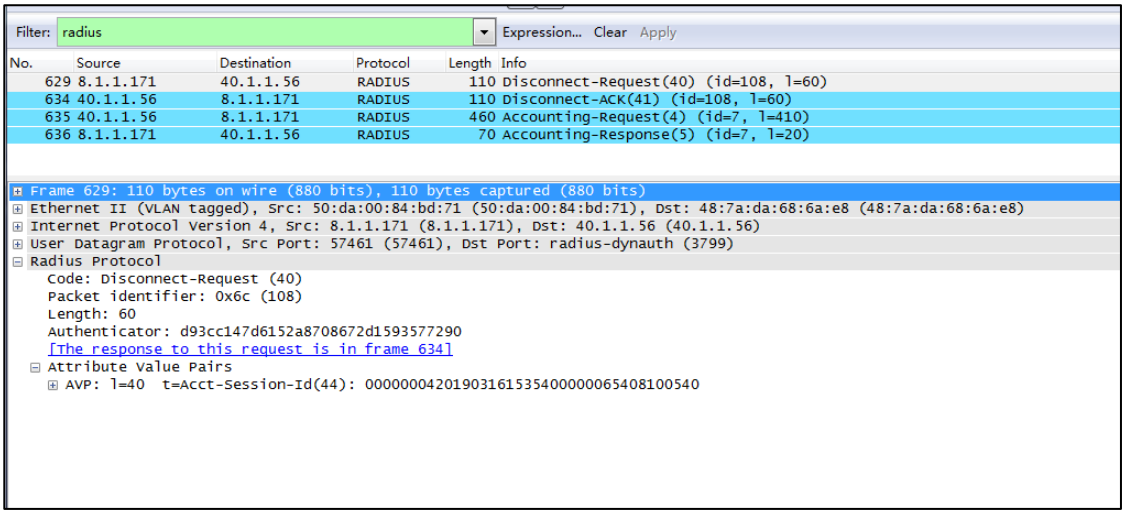
#表示されたページで、クライアントが802.1X EAP-PEAP認証を通過したことを確認します。

図63 オンラインユーザーの表示

#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



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$3$y9gLDgP10B8T9ry5u3AHTHOadEYl7g==
  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
```