
aruba
a Hewlett Packard
Enterprise company
emea atmosphere '17
THE innovation edge

Agenda

- Comware 5 and Comware 7 device based AAA:
  - RADIUS
  - TACACS+ (with RBAC)
- Comware 5 and Comware 7 endpoint device AAA:
  - MAC Authentication
  - 802.1X Authentication
  - Captive Portal

Device based AAA

Device based AAA support matrix

ClearPass	Comware 5	Comware 7
RADIUS based AAA	■	■
TACACS+ based AAA	■	■
TACACS+ based AAA with RBAC	■	■

Comware 5 and RADIUS with ClearPass

Switch configuration

```
ssh server enable
public-key local create rsa

radius scheme clearpass
server-type extended
primary authentication 10.1.254.21 key simple secretpassword
primary accounting 10.1.254.21 key simple secretpassword
user-name-format without-domain
nas-ip 10.1.254.201

domain radius
authentication login radius-scheme clearpass local
authorization login radius-scheme clearpass local
accounting login radius-scheme clearpass local

user-interface vty 0 2
authentication-mode scheme
protocol inbound ssh

domain default enable radius
```

Comware 5 and RADIUS with ClearPass

ClearPass Configuration

h3c.xml

– Import new H3C dictionary (download from arubanetworks.com)

– Configure a NAD

– Create users/roles/rolemappings

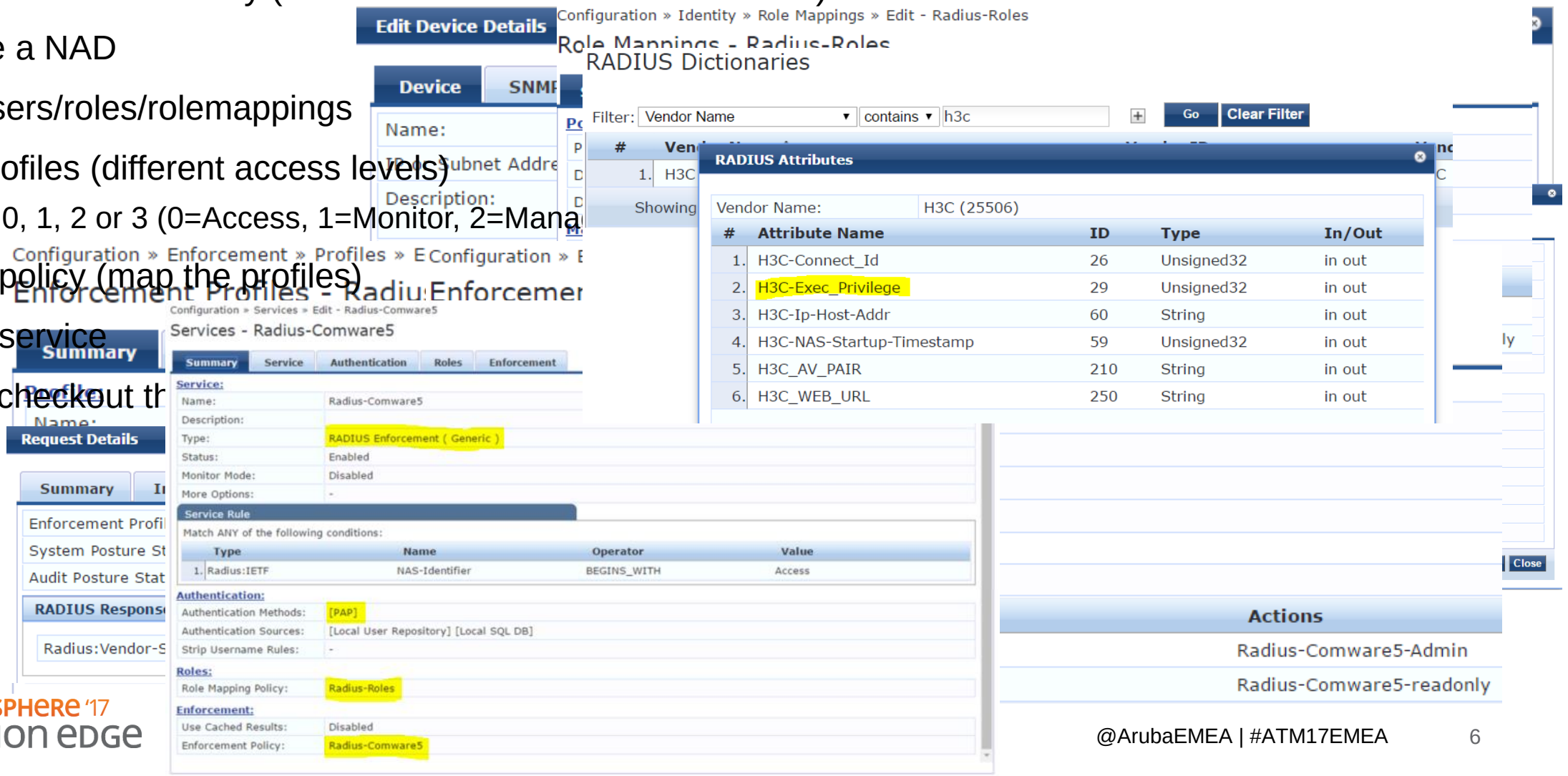
– Create profiles (different access levels)

  – Value = 0, 1, 2 or 3 (0=Access, 1=Monitor, 2=Mana

– Create a policy (map the profiles)

– Create a service

– Test and checkout th



Comware 7 and RADIUS with ClearPass

Switch configuration

```
ssh server enable
public-key local create rsa

radius scheme clearpass
server-type extended
primary authentication 10.1.254.21 key simple secretpassword
primary accounting 10.1.254.21 key simple secretpassword
user-name-format without-domain
nas-ip 10.1.254.201

domain radius
authentication login radius-scheme clearpass local
authorization login radius-scheme clearpass local
accounting login radius-scheme clearpass local

user-interface vty 0 2
authentication-mode scheme
protocol inbound ssh

domain default enable radius
```

Comware 7 and RADIUS with ClearPass

ClearPass Configuration

– Configure a NAD

– Create users/roles/rolemappings

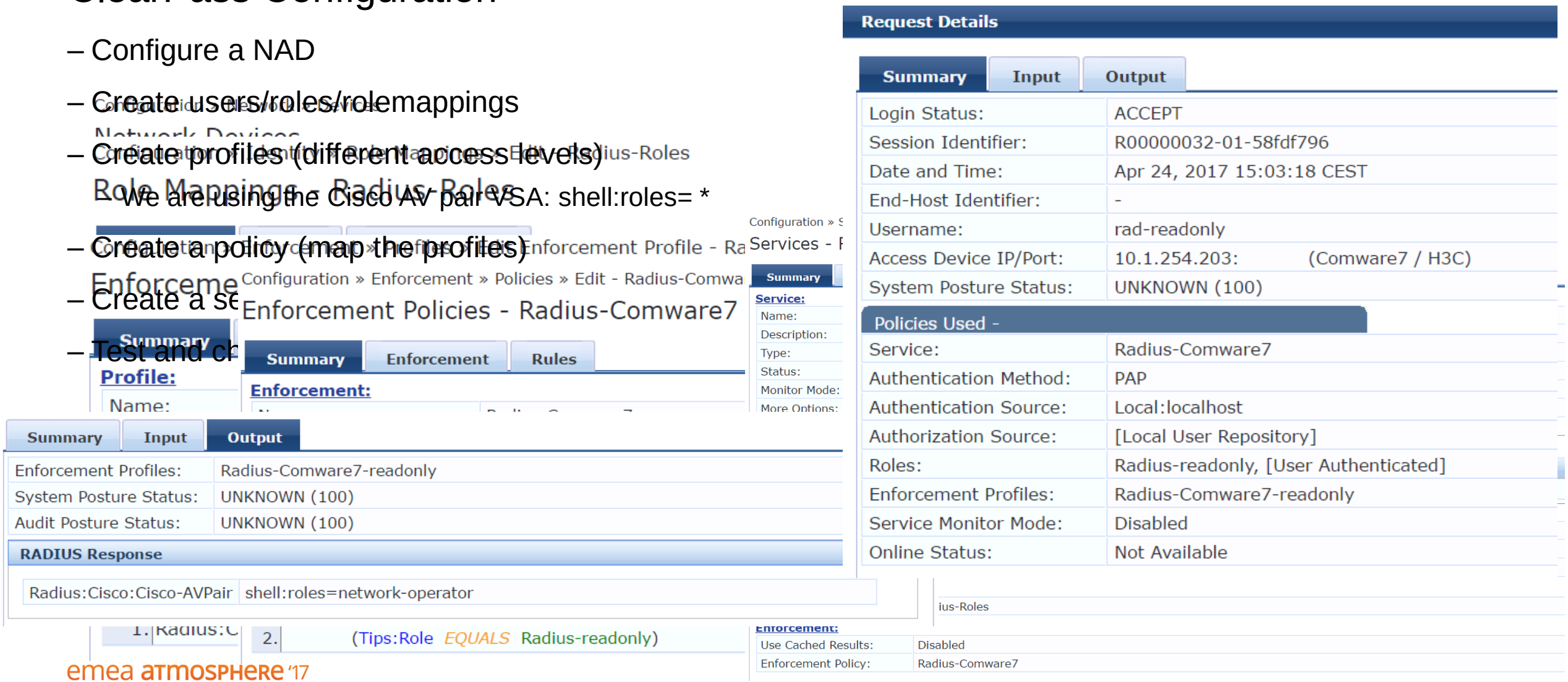
– Create profiles (different access levels)

– We are using the Cisco AV pair VSA: shell:roles= *

– Create a policy (map the profiles)

– Create a se

– Test and ch



Comware 5 and Tacacs with ClearPass and RBAC

Switch configuration

```
ssh server enable
public-key local create rsa

hwtacacs scheme ClearPass
primary authentication 10.1.254.21 key simple secretpassword
primary authorization 10.1.254.21 key simple secretpassword
primary accounting 10.1.254.21 key simple secretpassword

domain tacacs
authentication login hwtacacs-scheme ClearPass local
authorization login hwtacacs-scheme ClearPass local
accounting login hwtacacs-scheme ClearPass local
authorization command hwtacacs-scheme ClearPass local
accounting command hwtacacs-scheme ClearPass

domain default enable tacacs

user-interface vty 0 2
authentication-mode scheme
command authorization
command accounting
protocol inbound ssh
```

Comware 5 and Tacacs with ClearPass and RBAC

ClearPass Configuration

– Configure a NAD

– Create users/roles/rolemappings

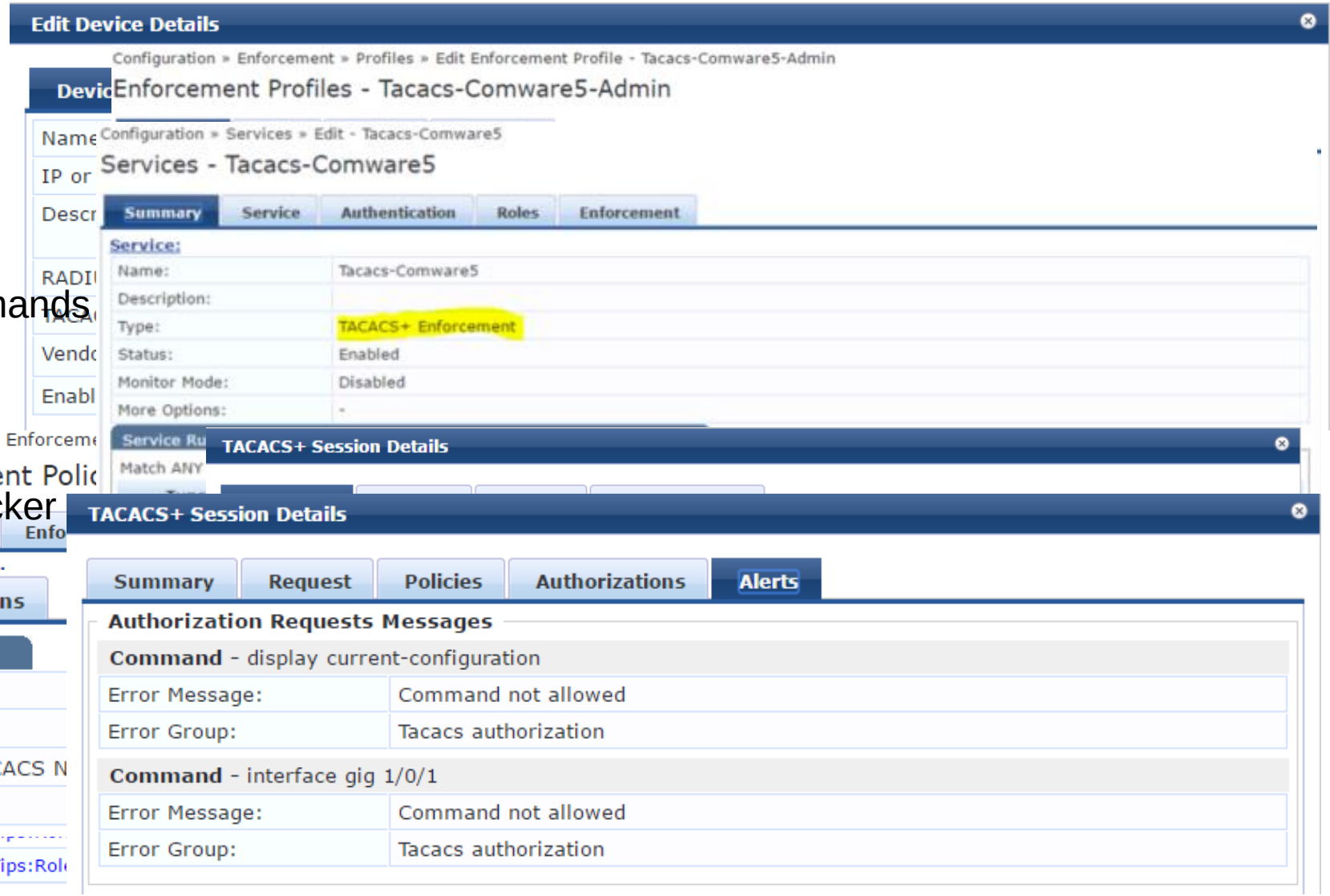
– Create profiles:
  Assign Shell service with priv-lvl
  For RBAC, deny unmatched commands

– Create a policy (map the profiles)

– Create a service

– Test and checkout the Access Tracker

– Checkout RBAC



Comware 7 and Tacacs with ClearPass and RBAC

Switch configuration

```
ssh server enable
public-key local create rsa

hwtacacs scheme ClearPass
primary authentication 10.1.254.21 key simple secretpassword
primary authorization 10.1.254.21 key simple secretpassword
primary accounting 10.1.254.21 key simple secretpassword

domain tacacs
authentication login hwtacacs-scheme ClearPass local
authorization login hwtacacs-scheme ClearPass local
accounting login hwtacacs-scheme ClearPass local
authorization command hwtacacs-scheme ClearPass local
accounting command hwtacacs-scheme ClearPass

domain default enable tacacs

user-interface vty 0 2
authentication-mode scheme
command authorization
command accounting
protocol inbound ssh
```

Comware 7 and Tacacs with ClearPass and RBAC

ClearPass Configuration

– Configure a NAD

– Create users/roles/rolemappings

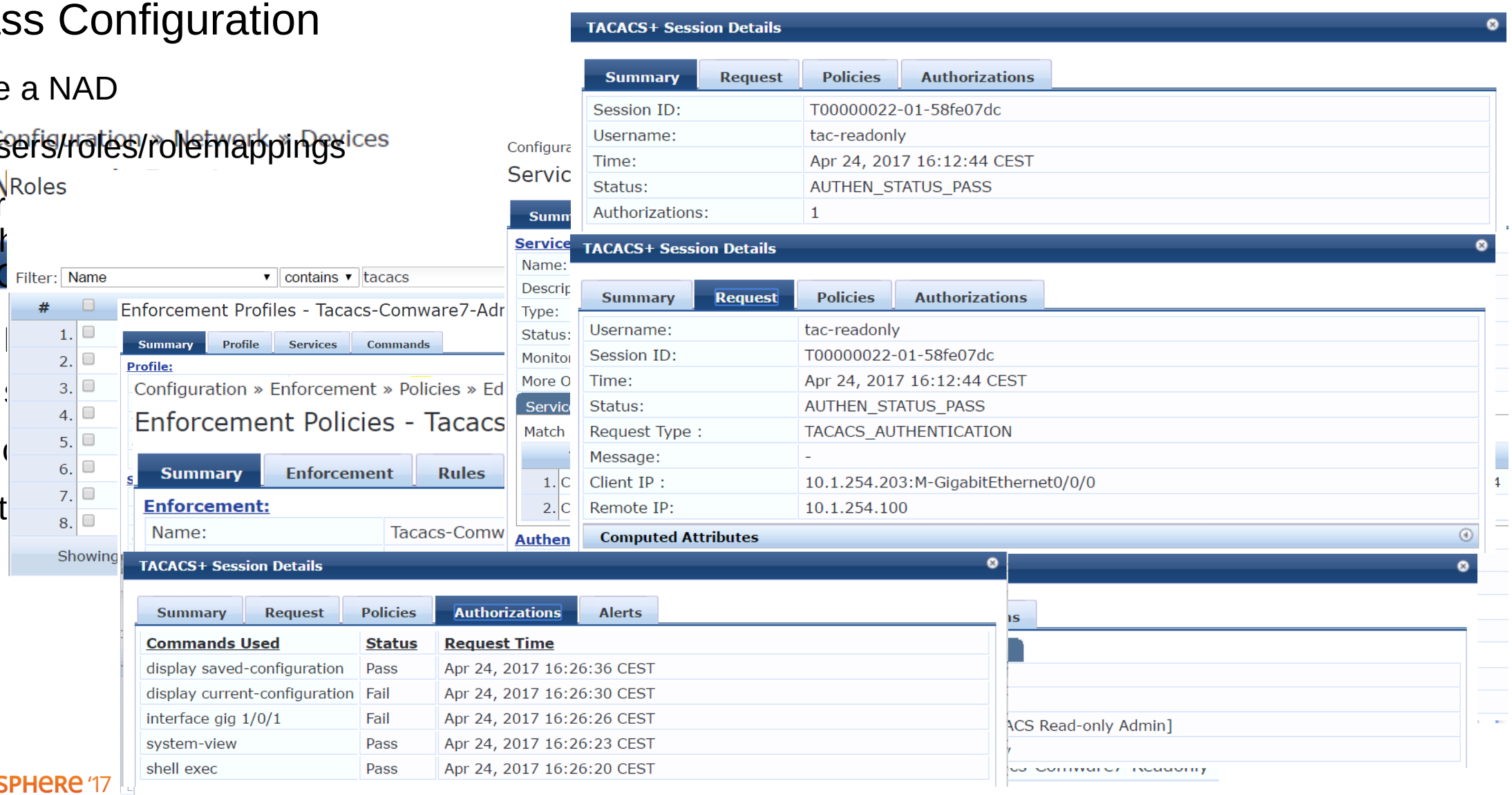
– Create pr
  Assign Sh
  For RBAC

– Create a

– Create a

– Test and

– Checkout



Endpoint based AAA

Device based AAA support matrix

ClearPass	Comware 5	Comware 7
Captive Portal		■
MAC Authentication	■	■
802.1X	■	■

Comware 5 & 7 and MAC Authentication/802.1X

- RADIUS based enforcements
  - ACL is configured locally on the switch
  - VLAN assignment can be based on VLAN Name or VLAN ID
- Comware does not accept an ACL **name** via the RADIUS filter-id or url-redirect attributes
  - ACL **number** must be sent
  - If you do not send an ACL in the RADIUS response and there is no ACL statically configured on the port, all traffic is permitted for that session

Comware 5 & 7 and MAC Authentication/802.1X

Switch Configuration

– Configure the RADIUS scheme and Domain

– Enable port-security globally

– Configure security parameters per port

– Other configurations include VLAN's and ACL's

```
radius scheme accesssecurity
 primary authentication 10.1.254.21 key simple secretpassword
 primary accounting 10.1.254.21 key simple secretpassword
 accounting-on enable
 user-name-format without-domain
 port-security enable (only on Comware 7)
domain accesssecurity
 authentication lan-access radius-scheme accesssecurity local
 authorization lan-access radius-scheme accesssecurity local
 accounting lan-access radius-scheme accesssecurity local
 undo dot1x multicast-trigger
 undo dot1x handshake
 mac-authentication max-user 10
 mac-authentication host-mode multi-vlan
 port-security port-mode userlogin-secure-or-mac-ext
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
 mac-vlan enable
 stp edged-port
```

Comware 5 & 7 and MAC Authentication/802.1X

ClearPass Configuration

– Configure the Network Access Device

– Configure users/roles/role mappings

– Create profiles that contains the VLAN/ACL assignments (different ones for MAC Auth and 802.1X)

– Create policies with rule mappings for MAC Auth and 802.1X

– Create a service for MAC authentication and 802.1X authentication

Network Devices
Role Mappings - AD-Rolemapping

Summary | Policy | Mapping Rules

Policy:

Policy Name:	AD-Rolemapping
Description:	
Default Role:	AD-Guest

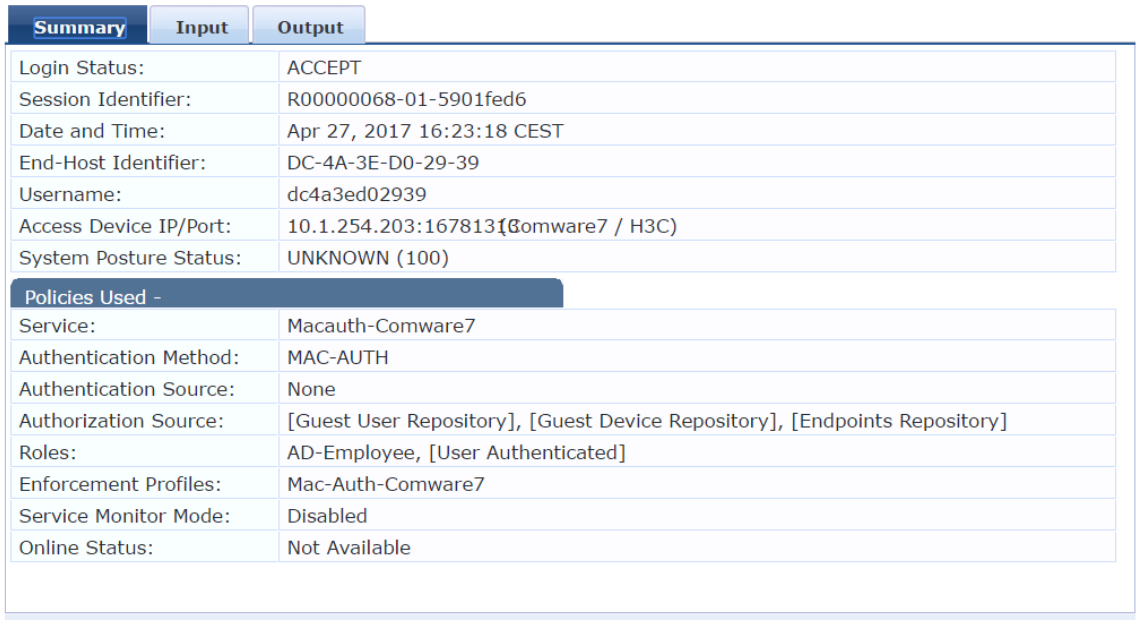
Mapping Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Role Name
1.	(Authorization:AD:Groups *EQUALS* employees)	AD-Employee
2.	(Authorization:AD:Groups *EQUALS* contractors)	AD-Contractor
3.	(Authorization:AD:Groups *EQUALS* guests)	AD-Guest
4.	(Authorization:AD:Groups *EQUALS* voice)	AD-Voice

Comware 5 & 7 and MAC Authentication/802.1X

– Test and check out the Access Tracker (MAC Authentication):

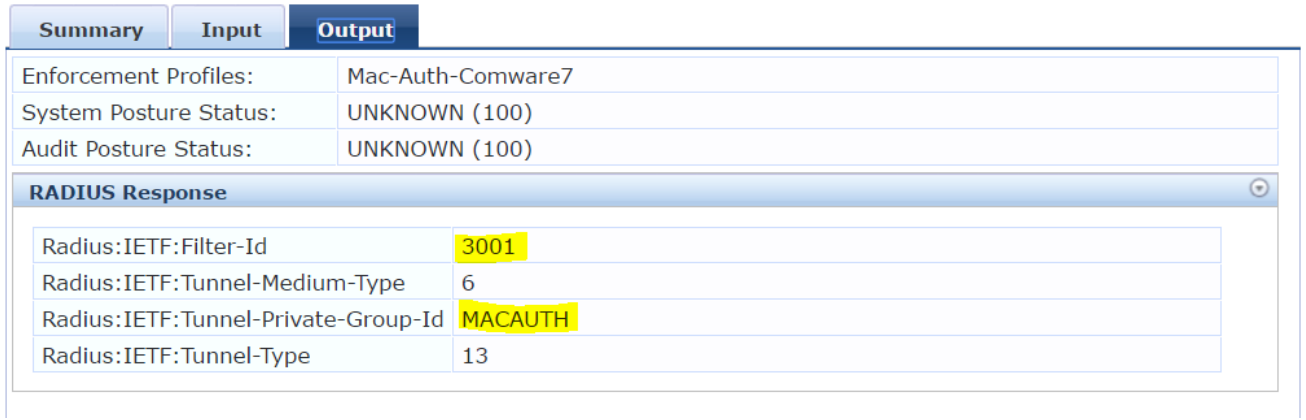


Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	R00000068-01-5901fed6
Date and Time:	Apr 27, 2017 16:23:18 CEST
End-Host Identifier:	DC-4A-3E-D0-29-39
Username:	dc4a3ed02939
Access Device IP/Port:	10.1.254.203:16781316 (Comware7 / H3C)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Macauth-Comware7
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository]
Roles:	AD-Employee, [User Authenticated]
Enforcement Profiles:	Mac-Auth-Comware7
Service Monitor Mode:	Disabled
Online Status:	Not Available



Summary | Input | Output

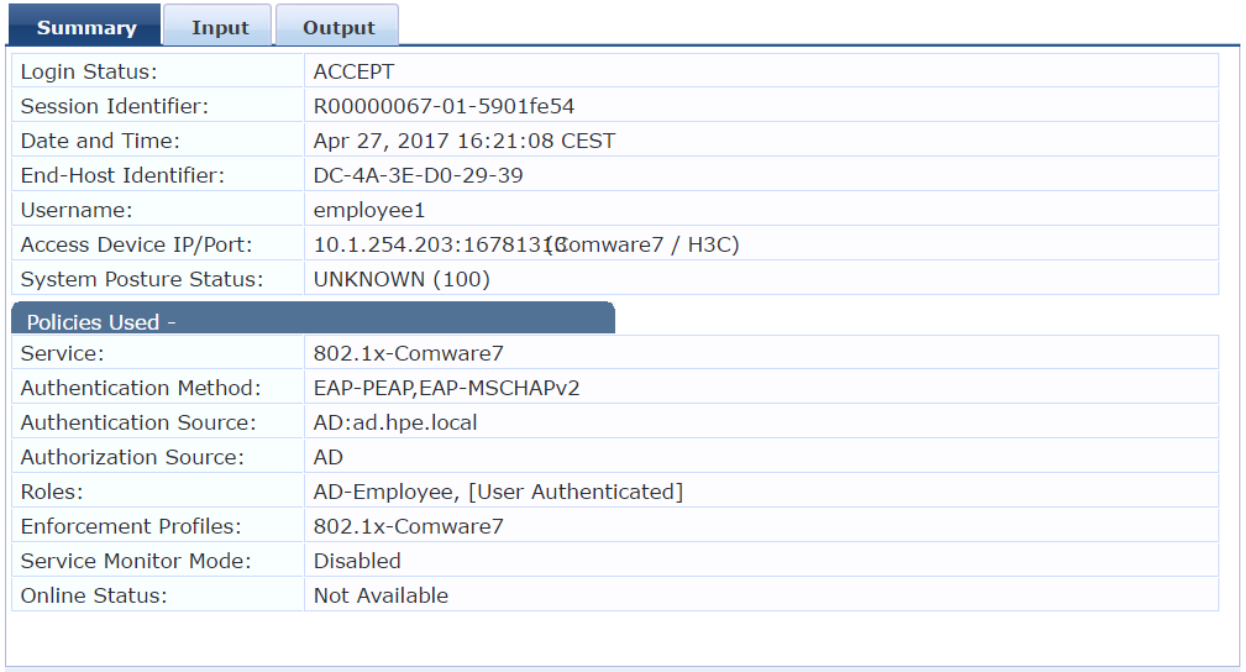
Enforcement Profiles:	Mac-Auth-Comware7
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

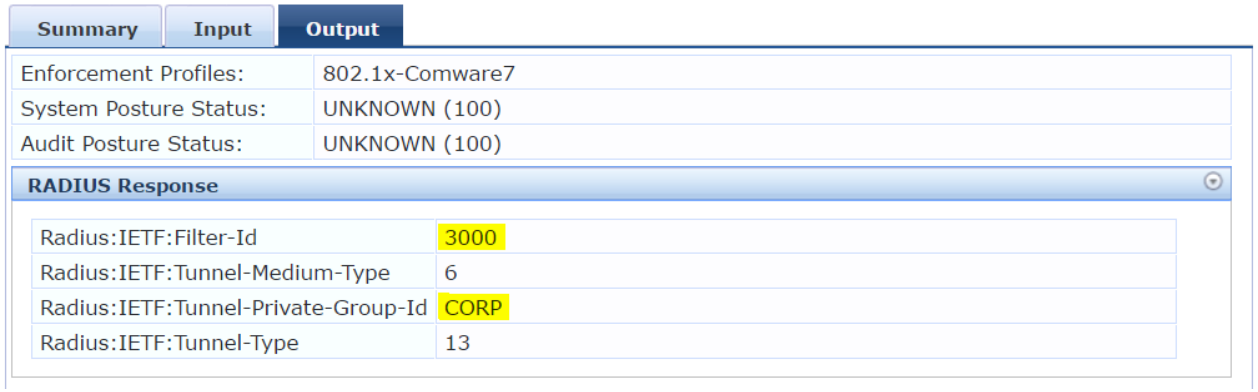
RADIUS Response

Radius:IETF:Filter-Id	3001
Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	MACAUTH
Radius:IETF:Tunnel-Type	13

Comware 5 & 7 and MAC Authentication/802.1X

– Test and check out the Access Tracker (802.1X Authentication):





Comware 5 & 7 and MAC Authentication/802.1X

- Check out the switch (802.1X Authentication):
  - Comware 5:
    - `display dot1x session interface gigabitethernet 1/0/1`
    - `display dot1x interface gigabitethernet 1/0/1`
  - Comware 7:
    - `display dot1x connection interface gigabitethernet 1/0/1`
    - `display dot1x interface gigabitethernet 1/0/1`
- Check out the switch (MAC Authentication):
  - Comware 5 & 7:
    - `display mac-authentication interface gigabitethernet 1/0/1`

```
[Comware7]display dot1x interface GigabitEthernet 1/0/1
 Global 802.1X parameters:
   802.1X authentication   : Enabled
   EAP authentication      : Enabled
   Max-tx period           : 10 s
   Handshake period        : 15 s
   Quiet timer             : Disabled
       Quiet period        : 60 s
   Supp timeout            : 10 s
   Server timeout          : 100 s
   Reauth period           : 3600 s
   Max auth requests       : 2
   SmartOn supp timeout    : 30 s
   SmartOn retry counts    : 3
   EAD assistant function  : Disabled
       EAD timeout         : 30 min
   Domain delimiter        : @
 Max 802.1X users          : 4294967295 per slot
 Online 802.1X users       : 1
 GigabitEthernet1/0/1  is link-up
   802.1X authentication       : Enabled
   Handshake                   : Enabled
   Handshake reply             : Disabled
   Handshake security          : Disabled
   Unicast trigger             : Disabled
   Periodic reauth             : Disabled
   Port role                   : Authenticator
   Authorization mode          : Auto
   Port access control         : MAC-based
   Multicast trigger           : Disabled
   Mandatory auth domain       : Not configured
   Guest VLAN                  : Not configured
   Auth-Fail VLAN              : Not configured
   Critical VLAN               : Not configured
   Critical voice VLAN         : Disabled
   Re-auth server-unreachable  : Logoff
   Max online users            : 4294967295
   SmartOn                     : Disabled
   Send Packets Without Tag    : Disabled
   Add Guest VLAN delay        : Disabled

   EAPOL packets: Tx 242, Rx 87
   Sent EAP Request/Identity packets : 207
        EAP Request/Challenge packets: 29
        EAP Success packets: 4
        EAP Failure packets: 2
   Received EAPOL Start packets : 2
            EAPOL LogOff packets: 0
            EAP Response/Identity packets : 56
            EAP Response/Challenge packets: 29
            Error packets: 0
   Online 802.1X users: 1
          MAC address       Auth state
          dc4a-3ed0-2939    Authenticated
```

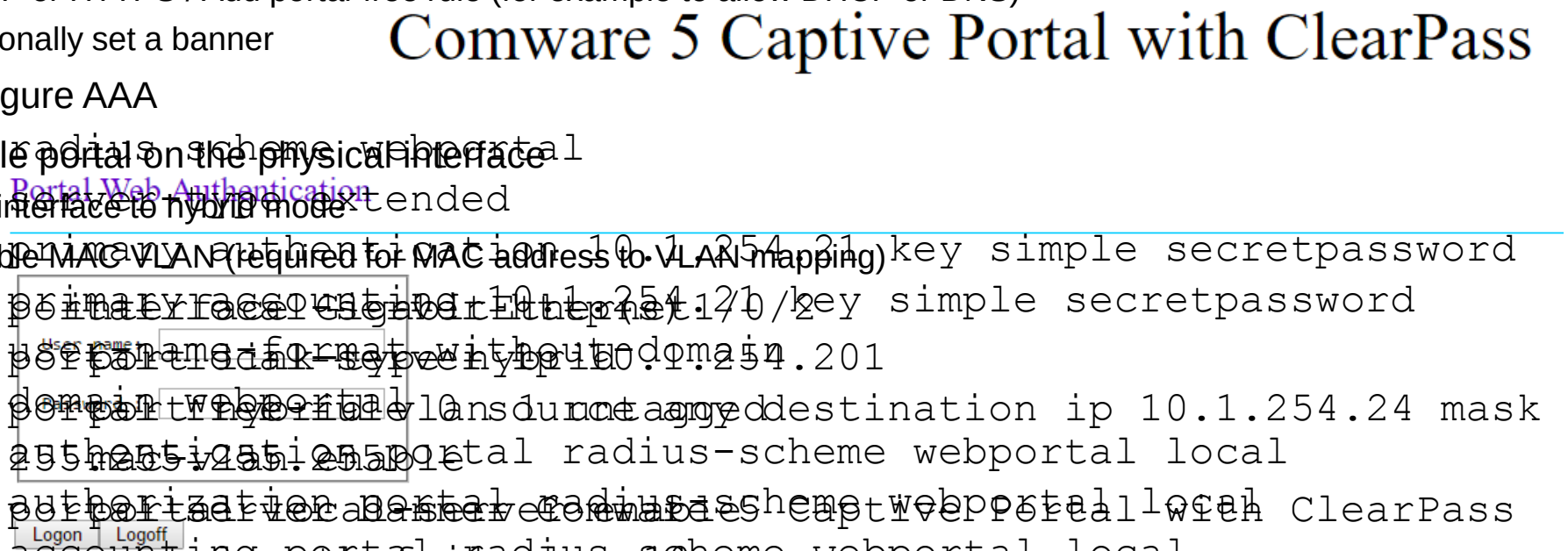
```
[Comware7]display dot1x connection interface GigabitEthernet 1/0/1
Slot ID: 1
User MAC address: dc4a-3ed0-2939
Access interface: GigabitEthernet1/0/1
Username: employee1
Authentication domain: accesssecurity
Authentication method: EAP
Initial VLAN: 1
Authorization untagged VLAN: 10
Authorization tagged VLAN list: N/A
Authorization ACL ID: 3000
Authorization user profile: N/A
Termination action: N/A
Session timeout period: N/A
Online from: 2011/01/01 02:42:21
Online duration: 0h 1m 2s

Total 1 connections matched.
```

Comware 5 and ClearPass Captive Portal

– Comware 5 only supports local web portal

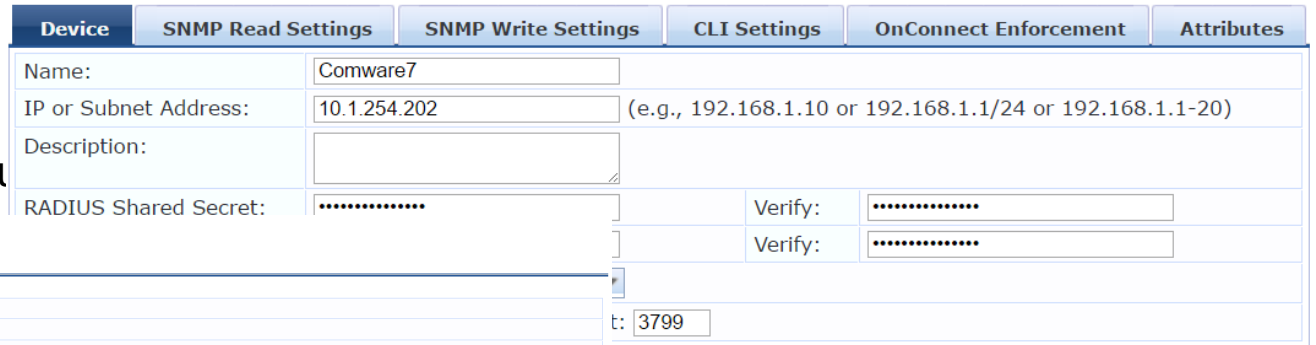
– The local web portal can use ClearPass as AAA service (including VLAN and ACL push)

– Configuration steps on the switch:
  – Configure the portal parameters
    – HTTP or HTTPS / Add portal-free rule (for example to allow DHCP or DNS)
    – Optionally set a banner
  – Configure AAA
  – Enable portal on the physical interface
    – Set interface to hybrid mode
    – Enable MAC VLAN (required for MAC address to VLAN mapping)



Comware 7 and ClearPass Captive Portal

– Selected Comware 7 devices support Change of Authorization (CoA):
  – HPE 5130EI (R3115P07)
  – HPE 5130HI (R1308)
  – HPE 5510HI (D1308)
– Supported CoA commands:
  – Terminate Session: traditional disconnect message; reinitializes authenticator state
  – Bounce Host Port: bounces the port by disabling and re-enabling the port ← ClearPass uses this one for the Captive Portal
  – Disable Host Port: administratively disables the port
– Important:
  – NAD has to be configured as Cisco device (for now)
  – URL redirection and ACL assignment is achieved throu



Enforcement Profiles - Portal-Comware7-Redirect

Summary | Profile | Attributes

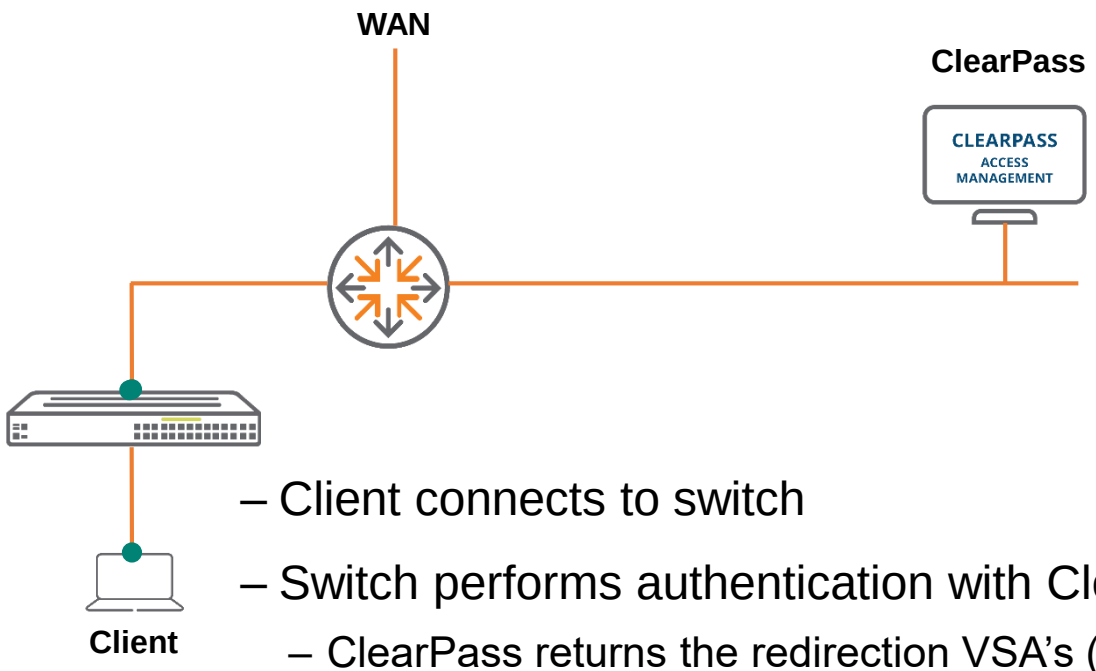
Profile:

Name:	Portal-Comware7-Redirect
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:H3C	H3C_AV_PAIR	=	url-redirect=https://10.1.254.21/guest/comware.php?mac=%{Connection:Client-Mac-Address-Colon}
2.	Radius:H3C	H3C_AV_PAIR	=	url-redirect-acl=3001
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Private-Group-Id	=	11
5.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
6.	Radius:IETF	Session-Timeout	=	60

Comware 7 and ClearPass Captive Portal process




```
[Comware7-GigabitEthernet1/0/1]disp mac-auth con int gig 1/0/1
Total connections: 1
Slot ID: 1
User MAC address: dc4a-3ed0-2939
Access interface: GigabitEthernet1/0/1
Username: dc4a3ed02939
User access state: Successful
Authentication domain: cppm
Initial VLAN: 1
Authorization untagged VLAN: 11
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL ID: 3002
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: N/A
Online from: 2013/01/01 04:37:18
Online duration: 0h 6m 36s
```

- Client connects to switch
- Switch performs authentication with ClearPass (Mac Auth)
  - ClearPass returns the redirection VSA's (ACL to allow DHCP/DNS/Webportal)
- Client redirects to the Web Portal, authenticates (Web Auth) and client logs in
- Upon successful authentication Web Auth Service issues port bounce
- Switch performs authentication with ClearPass (Mac Auth) → Successful guest authentication
  - ClearPass returns the "authenticated guest" VSA's (guest VLAN and ACL) and client gains access

Comware 7 and ClearPass Captive Portal

Switch Configuration

– Configure the RADIUS scheme and Domain

– Enable port-security globally and create a RADIUS dynamic-author server (required for CoA)

– Configure security parameters per port

– Other configurations include VLAN's and ACL's

```
radius scheme ClearPass
 primary authentication 10.1.254.21 key simple secretpassword
 primary accounting 10.1.254.21 key simple secretpassword
 user-name-format without-domain
domain ClearPass
 authentication lan-access radius-scheme ClearPass local
 authorization lan-access radius-scheme ClearPass local
 accounting lan-access radius-scheme ClearPass local
```

```
vlan 10
vlan 11
interface gigabitethernet 1/0/24
 description uplink
 port link-type trunk
 port trunk permit vlan 10 to 11
```

Comware 7 and ClearPass Captive Portal (I)

ClearPass Configuration

– Ensure you have the latest H3C RADIUS Dictionary

  – <Attribute profile="in out" type="String" name="H3C_AV_PAIR" id="210"/>

– Configure the NAD device (set Vendor name to Cisco)

RADIUS Dictionaries

's for redirect and ACL)

Filter: Vendor Name ▾ contains ▾ h3c Go Clear Filter

#	Vendor Name ▲	Vendor ID	Vendor Prefix
1.	H3C	25506	H3C

Enforcement Profiles - Portal-Comware7

Summary | Profile | Attributes

Profile:

Name:	Portal-Comware7
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Tunnel-Type	=	VLAN (13)
2.	Radius:IETF	Tunnel-Private-Group-Id	=	11
3.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
4.	Radius:IETF	Filter-Id	=	3002

54.21/guest/comware.php?mac=%
dress-Colon}

Comware 7 and ClearPass Captive Portal (II)

ClearPass Configuration

– Create a policy for MAC Authentication

  – Assign guest role to authenticated guest user (authenticated through web portal)

  – Assign redirect role to authenticated MAC user

Enforcement Policies - Portal-Comware7-Redirect and Access

Summary | Enforcement | Rules

Enforcement Policies - Portal-Comware7-Portbounce

Summary | Enforcement | Rules

Enforcement:

Name:	Portal-Comware7-Portbounce
Description:	
Enforcement Type:	WEBAUTH
Default Profile:	[Update Endpoint Known]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Posture *EXISTS*)	[Cisco - Bounce-Host-Port], [Update Endpoint Known]

Comware 7 and ClearPass Captive Portal (III)

ClearPass Configuration

– Create a service for MAC Authentication

  – Automatically authenticates all MAC Auth requests

  – Depending on “User Authenticated” or “[Guest]” TIPS role either redirect or allow access (enforced through policy)

  – Cache results to allow automatic MAC re-authentication (MAC information cached in ClearPass)

– Services - Macauth-Comware

  Summary | Service | Authentication | Roles | Enforcement

  sful web authentication

Services - Portal-Comware7-Bounce

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	Portal-Comware7-Bounce
Description:	
Type:	Web-based Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ANY of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ANY	Authentication

Authentication:

Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-

Roles:

Role Mapping Policy:	[Guest Roles]

Enforcement:

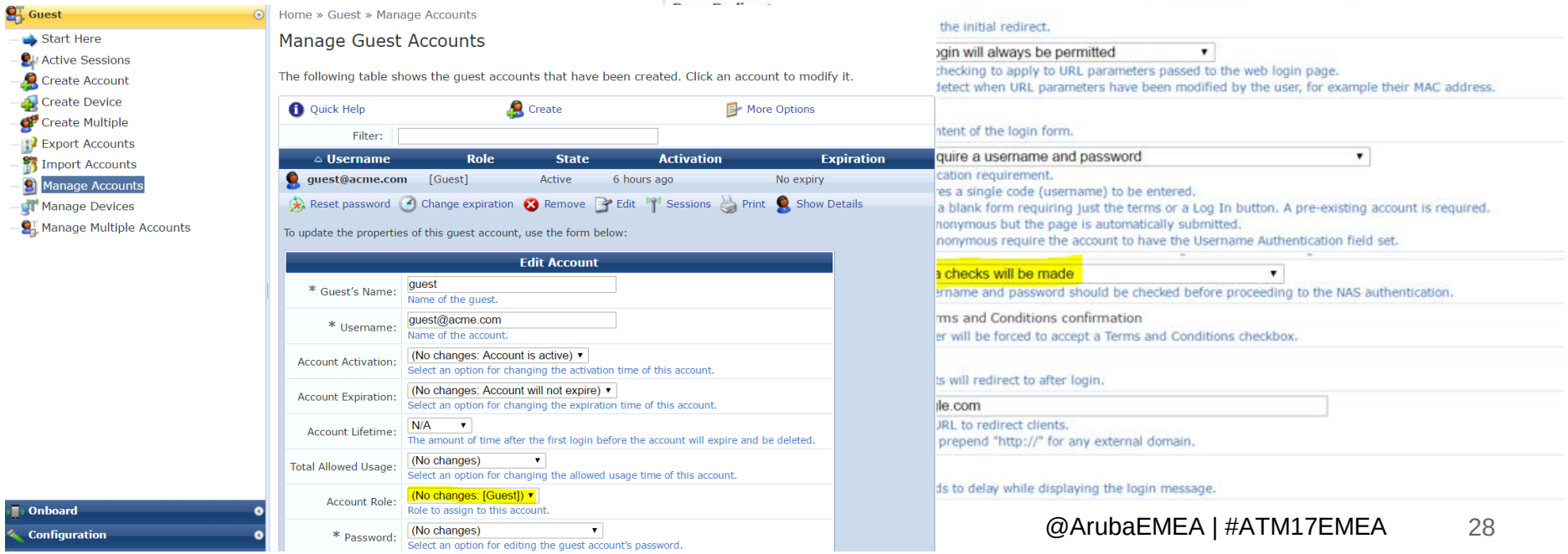
Use Cached Results:	Disabled
Enforcement Policy:	Portal-Comware7-Portbounce

Comware 7 and ClearPass Captive Portal (IV)

ClearPass Configuration

– Create a web portal page
  – Vendor: Aruba Networks
  – Login method: Server initiated to support CoA (MAC Address is provided through the H3C-AVPair VSA)
  – Set login delay long enough for the port to re-authenticate after port bounce

– Create guest user accounts (assign to the appropriate role n



Comware 7 and ClearPass Captive Portal (V)

ClearPass Configuration

– Put it to the test….

Access Tracker May 02, 2017 16:36:51 CEST

Auto Refresh

[All Requests] | ClearPass (10.1.254.21) | Last 1 day before Today | Edit

Filter: Request ID contains Go Clear Filter Show 10 records

#	Server	Source	Username	Service	Login Status	Request Timestamp	Auth Type
1.	10.1.254.21	RADIUS	dc4a3ed02939	Macauth-Comware	ACCEPT	2017/05/02 14:01:33	
2.	10.1.254.21	WEBAUTH	guest@acme.com	Portal-Comware7-Bounce	ACCEPT	2017/05/02 14:01:22	Guest
3.	10.1.254.21	RADIUS	dc4a3ed02939	Macauth-Comware	ACCEPT	2017/05/02 14:00:54	

Request Details

Summary | Input | Output | Accounting | RADIUS CoA

Login Status:	ACCEPT
Session Identifier:	R00000236-01-590874f6
Date and Time:	May 02, 2017 14:00:54 CEST
End-Host Identifier:	DC-4A-3E-D0-29-39
Username:	dc4a3ed02939
Access Device IP/Port:	10.1.254.202:167813{Comware7 / Cisco)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Macauth-Comware
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Endpoints Repository]
Roles:	[User Authenticated]
Enforcement Profiles:	Portal-Comware7-Redirect
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 3 of 1-10 records Change Status Show Config

Request Details

Summary | Input | Output | Accounting | RADIUS CoA

Enforcement Profiles:	Portal-Comware7-Redirect
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:H3C:H3C_AV_PAIR	url-redirect-acl=3001
Radius:H3C:H3C_AV_PAIR	url-redirect=https://10.1.254.21/guest/comware.php?mac=dc:4a:3e:d0:29:39
Radius:IETF:Session-Timeout	60
Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	11
Radius:IETF:Tunnel-Type	13

Showing 3 of 1-10 records Change Status Show Configuration Export Show Logs Close

Request Details

Summary | Input | Output | Accounting | RADIUS CoA

CoA Action# 1

Date and Time	May 02, 2017 14:01:24 CEST
Application Name	Policy Manager
RADIUS CoA Action Type	CoA
RADIUS CoA Action Name	[Cisco - Bounce-Host-Port]
Status Code	1
Status Message	Radius [Cisco - Bounce-Host-Port] successful for client dc4a3ed02939.
RADIUS CoA Attributes	Calling-Station-Id = DC-4A-3E-D0-29-39 Cisco-AVPair = subscriber:command=bounce-host-port

Comware 7 and ClearPass Captive Portal (VI)

ClearPass Configuration

– Put it to the test….

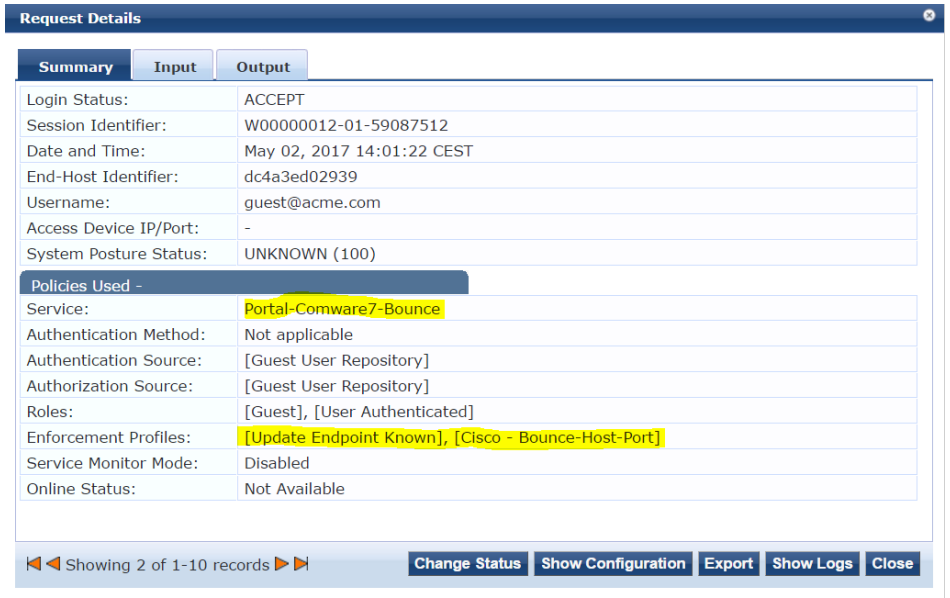
Access Tracker May 02, 2017 16:36:51 CEST

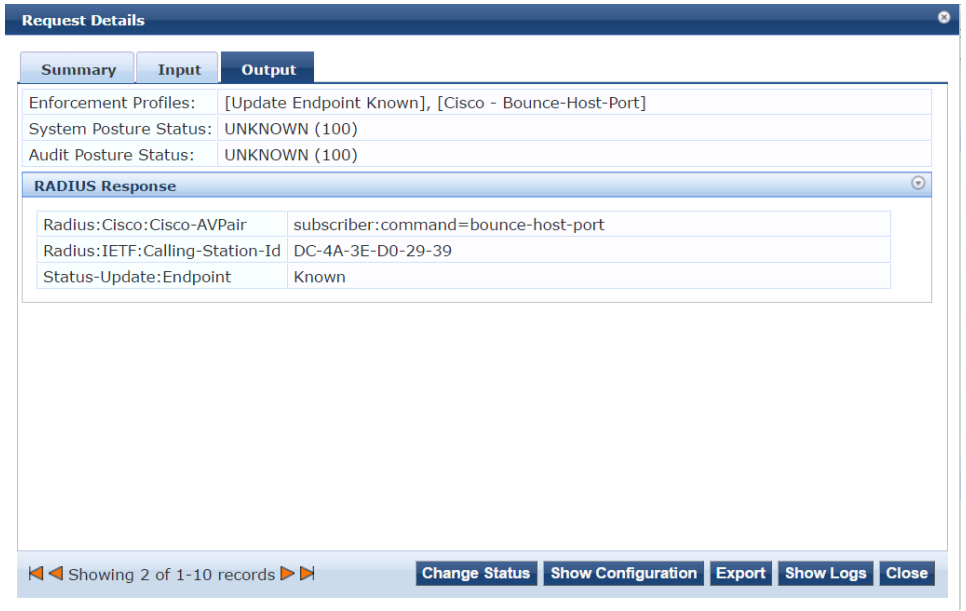
Auto Refresh

[All Requests] | ClearPass (10.1.254.21) | Last 1 day before Today | Edit

Filter: Request ID | contains | Go | Clear Filter | Show 10 records

#	Server	Source	Username	Service	Login Status	Request Timestamp	Auth Type
1.	10.1.254.21	RADIUS	dc4a3ed02939	Macauth-Comware	ACCEPT	2017/05/02 14:01:33	
2.	10.1.254.21	WEBAUTH	guest@acme.com	Portal-Comware7-Bounce	ACCEPT	2017/05/02 14:01:22	Guest
3.	10.1.254.21	RADIUS	dc4a3ed02939	Macauth-Comware	ACCEPT	2017/05/02 14:00:54	





Comware 7 and ClearPass Captive Portal (VII)

ClearPass Configuration

– Put it to the test….

Access Tracker May 02, 2017 16:36:51 CEST

Auto Refresh

[All Requests] | ClearPass (10.1.254.21) | Last 1 day before Today | Edit

Filter: Request ID contains Go Clear Filter Show 10 records

#	Server	Source	Username	Service	Login Status	Request Timestamp	Auth Type
1.	10.1.254.21	RADIUS	dc4a3ed02939	Macauth-Comware	ACCEPT	2017/05/02 14:01:33	
2.	10.1.254.21	WEBAUTH	guest@acme.com	Portal-Comware7-Bounce	ACCEPT	2017/05/02 14:01:22	Guest
3.	10.1.254.21	RADIUS	dc4a3ed02939	Macauth-Comware	ACCEPT	2017/05/02 14:00:54	

Request Details – Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000237-01-5908751d
Date and Time:	May 02, 2017 14:01:33 CEST
End-Host Identifier:	DC-4A-3E-D0-29-39
Username:	dc4a3ed02939
Access Device IP/Port:	10.1.254.202:167813[illegible]omware7 / Cisco)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Macauth-Comware
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Endpoints Repository]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	Portal-Comware7
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-10 records | Change Status | Show Configurati

Request Details – Summary | Input | Output | Accounting

Enforcement Profiles:	Portal-Comware7
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:IETF:Filter-Id	3002
Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	11
Radius:IETF:Tunnel-Type	13

Showing 1 of 1-10 records | Change Status | Show Configuration | Export | Show Logs | Close

Request Details – Summary | Input | Output | Accounting

Account Session ID:	00000004201301010437180000003208100349
Start Timestamp:	May 02, 2017 14:01:33 CEST
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1

Network Details

NAS IP Address:	10.1.254.202:16781313
NAS Port Type:	Ethernet
Calling Station ID:	DC-4A-3E-D0-29-39
Called Station ID:	40-B9-3C-A5-47-28
Framed IP Address:	-
Account Auth:	RADIUS

Utilization

Active Time:	0 Sec

Showing 1 of 1-10 records | Change Status | Show Configuration | Export | Show Logs | Close

aruba
a Hewlett Packard Enterprise company

emea atmosphere '17

THE innovation edge