

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/role mappings

- Create profiles (different access levels)
 - Value = 0, 1, 2 or 3 (0=Access, 1=Monitor, 2=Manage)

- Create a policy (map the profiles)

- Create a service

- Test and checkout the configuration

The screenshot displays the ClearPass configuration interface for RADIUS roles and services. The top navigation bar shows the path: Configuration » Identity » Role Mappings » Edit - Radius-Roles. The main content area is titled 'Role Mappings - Radius-Roles' and 'RADIUS Dictionaries'. A filter is applied: Vendor Name contains h3c. The 'RADIUS Attributes' table lists attributes for H3C (25506):

#	Attribute Name	ID	Type	In/Out
1.	H3C-Connect_Id	26	Unsigned32	in out
2.	H3C-Exec_Privilege	29	Unsigned32	in out
3.	H3C-Ip-Host-Addr	60	String	in out
4.	H3C-NAS-Startup-Timestamp	59	Unsigned32	in out
5.	H3C_AV_PAIR	210	String	in out
6.	H3C_WEB_URL	250	String	in out

The 'Services - Radius-Comware5' section shows the configuration for the 'Radius-Comware5' service. The 'Summary' tab is active, displaying the following details:

- Service:** Name: Radius-Comware5, Description: Radius-Comware5
- Type:** RADIUS Enforcement (Generic)
- Status:** Enabled
- Monitor Mode:** Disabled
- More Options:** -

The 'Service Rule' section shows a match condition: Match ANY of the following conditions:

Type	Name	Operator	Value
1.	Radius:IETF	NAS-Identifier	BEGINS_WITH

The 'Authentication' section shows the following configuration:

- Authentication Methods:** PAP
- Authentication Sources:** [Local User Repository] [Local SQL DB]
- Strip Username Rules:** -

The 'Roles' section shows the following configuration:

- Role Mapping Policy:** Radius-Roles

The 'Enforcement' section shows the following configuration:

- Use Cached Results:** Disabled
- Enforcement Policy:** Radius-Comware5

The 'Actions' section shows the following configuration:

- Radius-Comware5-Admin**
- Radius-Comware5-readonly**

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/role mappings
- Create profiles (different access levels)
- We are using the Cisco AV pair VSA: shell:roles= *
- Create a policy (map the profiles)
- Create a service
- Test and check

Request Details	
Summary	Input
Login Status:	ACCEPT
Session Identifier:	R00000032-01-58fdf796
Date and Time:	Apr 24, 2017 15:03:18 CEST
End-Host Identifier:	-
Username:	rad-readonly
Access Device IP/Port:	10.1.254.203: (Comware7 / H3C)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Radius-Comware7
Authentication Method:	PAP
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	Radius-readonly, [User Authenticated]
Enforcement Profiles:	Radius-Comware7-readonly
Service Monitor Mode:	Disabled
Online Status:	Not Available
ius-Roles	
Use Cached Results:	Disabled
Enforcement Policy:	Radius-Comware7

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/role mappings
- 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

The screenshot displays the ClearPass configuration interface. The top section, titled "Edit Device Details", shows the configuration for "Tacacs-Comware5-Admin". The "Service" tab is selected, showing the "Service" details for "Tacacs-Comware5". The "Type" is set to "TACACS+ Enforcement". The "Status" is "Enabled" and the "Monitor Mode" is "Disabled".

The bottom section, titled "TACACS+ Session Details", shows the "Alerts" tab. It displays two authorization requests with error messages:

Command	Error Message	Error Group
display current-configuration	Command not allowed	Tacacs authorization
interface gig 1/0/1	Command not allowed	Tacacs authorization

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/role mappings
- Create profiles
- Assign Services
- For RBAC
- Create a
- Create a
- Test and
- Checkout

The screenshot displays the ClearPass configuration interface. On the left, a navigation pane shows the path: Configuration » Network » Devices. The main area is divided into several sections:

- Enforcement Profiles - Tacacs-Comware7-Adm**: A table with columns #, Name, and a checkbox. It lists 8 profiles, with the first one selected.
- Enforcement Policies - Tacacs**: A section with tabs for Summary, Profile, Services, and Commands. The Summary tab is active, showing a table with columns: Name, Status, Monitor, More O, Match, and Authen. It lists 2 policies.
- TACACS+ Session Details**: Three overlapping windows showing session information for a user named 'tac-readonly'.

TACACS+ Session Details (Top Window):

Summary	Request	Policies	Authorizations
Session ID:	T00000022-01-58fe07dc		
Username:	tac-readonly		
Time:	Apr 24, 2017 16:12:44 CEST		
Status:	AUTHEN_STATUS_PASS		
Authorizations:	1		

TACACS+ Session Details (Middle Window):

Summary	Request	Policies	Authorizations
Username:	tac-readonly		
Session ID:	T00000022-01-58fe07dc		
Time:	Apr 24, 2017 16:12:44 CEST		
Status:	AUTHEN_STATUS_PASS		
Request Type :	TACACS_AUTHENTICATION		
Message:	-		
Client IP :	10.1.254.203:M-GigabitEthernet0/0/0		
Remote IP:	10.1.254.100		

TACACS+ Session Details (Bottom Window):

Summary	Request	Policies	Authorizations	Alerts
Commands Used				
display saved-configuration	Pass	Apr 24, 2017 16:26:36 CEST		
display current-configuration	Fail	Apr 24, 2017 16:26:30 CEST		
interface gig 1/0/1	Fail	Apr 24, 2017 16:26:26 CEST		
system-view	Pass	Apr 24, 2017 16:26:23 CEST		
shell exec	Pass	Apr 24, 2017 16:26:20 CEST		

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

```
radius-scheme accesssecurity
primary authentication 10.1.254.21 key simple secretpassword
primary accounting 10.1.254.21 key simple secretpassword
interface GigabitEthernet0/1/0/1
accesssecurity enable
port-security enable
port-security mode bridge
port-security mode permit (only on Comware 7)
port hybrid vlan 1 untagged
authentication lan-access radius-scheme accesssecurity local
mac-vlan enable
authorization lan-access radius-scheme accesssecurity local
stp edged-port
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
```

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

Enforcement Summary Policy Mapping Rules

Services - Macau

Summary Service

Type:

Status:

Monitor Mode:

More Options:

Service Rule

Match ALL of the follow

Type

1. Radius:IETF

2. Radius:IETF

3. Connection

4. Radius:IETF

Authentication:

Authentication Methods:

Authentication Sources:

Strip Username Rules:

Authorization:

Authorization Details:

Roles:

Role Mapping Policy:

Enforcement:

Use Cached Results: Enabled

Enforcement Policy: MACAuth-Comware7

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

Enforcement:

Use Cached Results: Disabled

Enforcement Policy: 802.1x-Comware7

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:	10.1.254.203:1678131(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):

Summary	Input	Output
Login Status:	ACCEPT	
Session Identifier:	R00000067-01-5901fe54	
Date and Time:	Apr 27, 2017 16:21:08 CEST	
End-Host Identifier:	DC-4A-3E-D0-29-39	
Username:	employee1	
Access Device IP/Port:	10.1.254.203:167813{Comware7 / H3C}	
System Posture Status:	UNKNOWN (100)	
Policies Used -		
Service:	802.1x-Comware7	
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2	
Authentication Source:	AD:ad.hpe.local	
Authorization Source:	AD	
Roles:	AD-Employee, [User Authenticated]	
Enforcement Profiles:	802.1x-Comware7	
Service Monitor Mode:	Disabled	
Online Status:	Not Available	

Summary	Input	Output
Enforcement Profiles:	802.1x-Comware7	
System Posture Status:	UNKNOWN (100)	
Audit Posture Status:	UNKNOWN (100)	
RADIUS Response		
Radius:IETF:Filter-Id	3000	
Radius:IETF:Tunnel-Medium-Type	6	
Radius:IETF:Tunnel-Private-Group-Id	CORP	
Radius:IETF:Tunnel-Type	13	

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 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.
```

```
[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 : 0
  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
```

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 5 Captive Portal with ClearPass

```
radius-scheme webportal
portal web-authentication 10.1.254.21 key simple secretpassword
primary-accounting 10.1.254.121/24 key simple secretpassword
use format without domain
portal link-type hybrid
portal webportal vlansource any destination ip 10.1.254.24 mask
255.255.255.255
authentication portal radius-scheme webportal local
authorization portal radius-scheme webportal local ClearPass
accounting portal radius-scheme webportal local
domain default enable webportal
```

Comware 7 and ClearPass Captive Portal

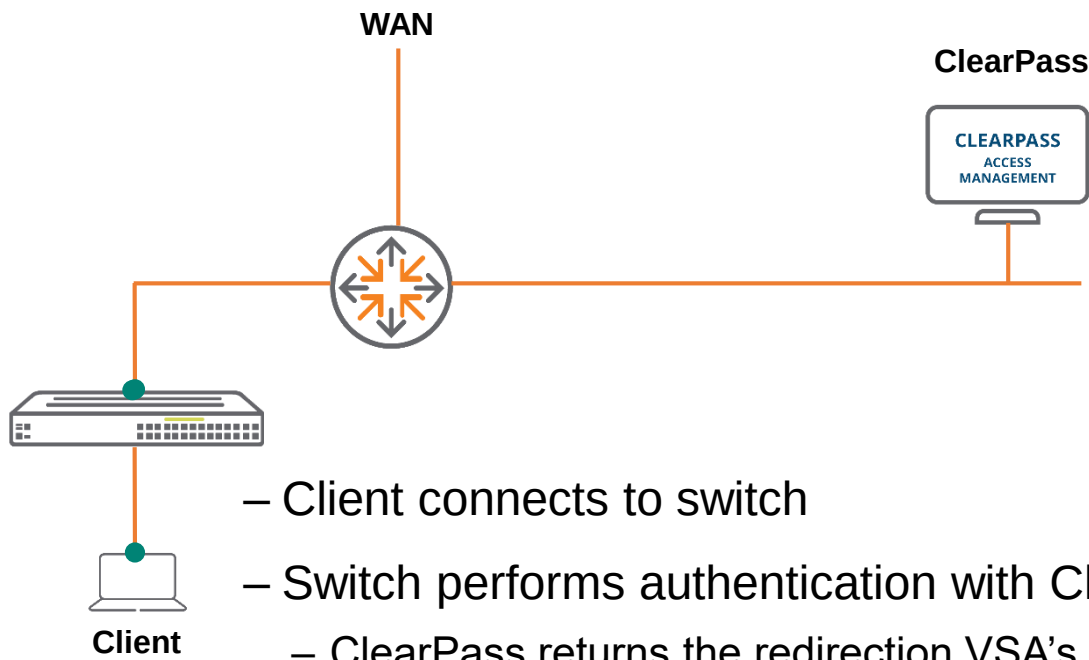
- Selected Comware 7 devices support Change of Authorization (CoA):
 - HPE 5130EI (R3115P07)
 - HPE 5130HI (R1308)
 - HPE 5510HI (D1308)
- Supported CoA commands:
 - Terminate Session: traditional disconnect message; reinitializes authenticator state
 - Bounce Host Port: bounces the port by disabling 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 through

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

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enforcement	Attributes
Name:	Comware7				
IP or Subnet Address:	10.1.254.202 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)				
Description:					
RADIUS Shared Secret:					Verify:
					Verify:
	t: 3799				

Comware 7 and ClearPass Captive Portal process



```
[Comware7-GigabitEthernet1/0/1]disp mac-auth con int gig 1/0/1
[Comware7]Total connections: 1
%Jan 1 04:37:18 Slot ID: 1
et1/0/1-MAC address: dc4a-3ed0-2939
address; Access interface: GigabitEthernet1/0/1
Username: dc4a3ed02939
[Comware7-User access state: Successful
GOF: -IfNAuthentication domain: cppm
a3ed02939-Initial VLAN: 1
%Jan 1 04:37:18 Authorization untagged VLAN: 11
erface GigabitEthernet1/0/1 Authorization tagged VLAN: N/A
%Jan 1 04:37:18 Authorization USI: N/A
he interface Authorization ACL ID: 3002
erface GigabitEthernet1/0/1 Authorization user profile: N/A
%Jan 1 04:37:18 Authorization CAR: N/A
he interface Authorization URL: N/A
%Jan 1 04:37:18 Termination action: Default
et1/0/1-MAC address; 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

[illegible]

Comware 7 and ClearPass Captive Portal (I)

ClearPass Configuration



h3c.xml

- 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 <i>EXISTS</i>)	[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

sful web authentication

Summary	Service	Authentication	Roles	Enforcement
---------	---------	----------------	-------	-------------

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

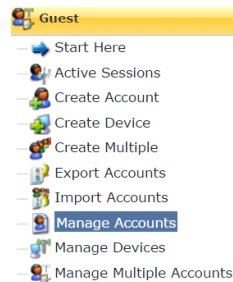
- Create a web portal page
 - Vendor: Aruba Networks
 - Login method: Server initiated to support CoA (MAC Address is provided through the H3C-AVPair VSA)
 - Set login delay long enough for the port to re-authenticate after port bounce
- Create guest user accounts (assign to the appropriate role n

Home » Configuration » Pages » Web Logins

Web Login (comware)

Use this form to make changes to the Web Login **comware**.

Web Login Editor	
* Name:	comware Enter a name for this web login page.
Page Name:	comware Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	 Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Server-initiated — Change of authorization (RFC 3576) sent to controller Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.



Home » Guest » Manage Accounts

Manage Guest Accounts

The following table shows the guest accounts that have been created. Click an account to modify it.

Quick Help		Create	More Options	
Filter:				
Username	Role	State	Activation	Expiration
guest@acme.com	[Guest]	Active	6 hours ago	No expiry
Reset password Change expiration Remove Edit Sessions Print Show Details				
To update the properties of this guest account, use the form below:				
Edit Account				
* Guest's Name:	guest Name of the guest.			
* Username:	guest@acme.com Name of the account.			
Account Activation:	(No changes: Account is active) ▾ Select an option for changing the activation time of this account.			
Account Expiration:	(No changes: Account will not expire) ▾ Select an option for changing the expiration time of this account.			
Account Lifetime:	N/A ▾ The amount of time after the first login before the account will expire and be deleted.			
Total Allowed Usage:	(No changes) ▾ Select an option for changing the allowed usage time of this account.			
Account Role:	(No changes: [Guest]) ▾ Role to assign to this account.			
* Password:	(No changes) ▾ Select an option for editing the guest account's password.			

the initial redirect.
login will always be permitted ▾
checking to apply to URL parameters passed to the web login page.
detect when URL parameters have been modified by the user, for example their MAC address.
Content of the login form.
Require a username and password ▾
Authentication requirement.
Requires a single code (username) to be entered.
A blank form requiring just the terms or a Log In button. A pre-existing account is required.
Anonymous but the page is automatically submitted.
Anonymous require the account to have the Username Authentication field set.
Checks will be made ▾
Username and password should be checked before proceeding to the NAS authentication.
Terms and Conditions confirmation
User will be forced to accept a Terms and Conditions checkbox.
Users will redirect to after login.
File.com
URL to redirect clients.
Prepend "http://" for any external domain.
Delay to delay while displaying the login message.

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: 10.1.254.202:1678131[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 

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

SummaryInputOutput

Login Status:ACCEPT

Session Identifier:W00000012-01-59087512

Date and Time:May 02, 2017 14:01:22 CEST

End-Host Identifier:dc4a3ed02939

Username:guest@acme.com

Access Device IP/Port:-

System Posture Status:UNKNOWN (100)

Policies Used -

Service:Portal-Comware7-Bounce

Authentication Method:Not applicable

Authentication Source:[Guest User Repository]

Authorization Source:[Guest User Repository]

Roles:[Guest], [User Authenticated]

Enforcement Profiles:[Update Endpoint Known], [Cisco - Bounce-Host-Port]

Service Monitor Mode:Disabled

Online Status:Not Available

Showing 2 of 1-10 recordsChange StatusShow ConfigurationExportShow LogsClose

Request Details

SummaryInputOutput

Enforcement Profiles:[Update Endpoint Known], [Cisco - Bounce-Host-Port]

System Posture Status:UNKNOWN (100)

Audit Posture Status:UNKNOWN (100)

RADIUS Response

Radius:Cisco:Cisco-AVPairsubscriber:command=bounce-host-port

Radius:IETF:Calling-Station-IdDC-4A-3E-D0-29-39

Status-Update:EndpointKnown

Showing 2 of 1-10 recordsChange StatusShow ConfigurationExportShow LogsClose

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:	10.1.254.202:16781313 (Comware7 / 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 Configuration	

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		

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 StatusShow ConfigurationExportShow LogsClose

emea atmosphere '17 THE innovation edge