A) Steps of Integration Instant AP with ClearPass

1- Go to Configuration Menu and select System.

2- Give a name to your Instant AP and then specify a virtual Controller IP.

3- Enable the Dynamic RADIUS Proxy

Thus, regardless of the IP address that the AP gets through DHCP and it always be reachable on the above IP address specified.

4- Configure the Aruba Instant SSID

BASIC

* Create a SSID
* Give it a name
* Choose its type (wireless)
* Choose primary usage (role)

VLAN

* Choose the client IP assigment type that will be useful for you
* Choose the client VLAN assigment type

SECURITY

* Choose the security level
* On Authentication Server part, create an authentication server

--> Type (RADIUS)

--> Give a name

--> Assign an virtual IP address which is primary active on the Publisher

--> Type the shared key that used by RADIUS Server

--> Enable the Dynamic Authorization

--> Click Ok, then continue

NOTE: At first glance, the RBAC approach may seem to offer some benefits, such as reduced administrative work and operational efficiency. Seemingly, you define roles, and you’re ready to go.

But unfortunately, this is not the case. Today’s digital enterprise is driven by complex environments that are highly distributed with hundreds of applications, many systems, hybrid legacy and cloudified, microservices-driven infrastructures, and hundreds, sometimes even thousands of roles that are continually changing and require the creation of a new access scenario with each change.

It is impossible to keep track of ever-evolving assets and which user is receiving access to which resources and gain the requisite visibility into access risks.

Ultimately, RBAC is a static authorization methodology attempting to control access in a dynamic business and IT environment.

As such the role-based, static approach no longer suffices.

PBAC-driven dynamic authorization and how it helps to overcome the challenge

The key to overcoming the challenge is the implementation of dynamic authorization, where authorization and access to resources, including the network, applications, data, and any other asset is granted dynamically in real-time.

And what makes dynamic authorization possible is replacing role-based access control with policy-based access control (PBAC). With this method, roles are combined with policies that are comprised of logical rules for evaluating in real time the level of permissions and privileges that should be granted.

* Do the same things Authentication server 2 with AuthN server 1
* Choose the accounting type as ‘Use authN servers’
* Specify Accounting Interval as 3 minute
* As a best practice, you can enable the Opportunistic Key, 802.11r, 802.11k, 802.11v
* Then click next

ACCESS

* Leave the Access Rules option as Unrestricted then click to finish.

B) *Go to ClearPass Policy Manager – Configuration – Network –* Devices and follow the following instructions:

1. Go to Device tap
2. Specify an IP or Subnet Address for the Instant AP (You can assign the virtual IP that you assigned within the Instant AP configuration, because both are serving the same purpose!)
3. Put a good description to your configuration like “Aruba Instant for ClearPass Workshop
4. Put in the same RADIUS shared secret that you put in the Instant AP
5. As last enable the Dynamic AuthZ, then click Add button and try again to reconnect!

C) Create a service for ClearPass

1. Go to ClearPass Policy Manager – Configuration – Services
2. Then click the top right green + button to add a new service
3. Come to Service tap and follow the instructions:
   * Choose the service type as 802.1X Wireless
   * Give a name that service
   * Type a good desc like 802.1X Wireless Access Service
   * Leave as it be the following settings then click next
4. In the Authentication tab; you have the authN methods, choose methods that you will need, or remove (For example, you can only choose [EAP TLS] here)
5. Add a new AuthN Source by clicking the add a new Authentication Source that is in the right of page
   1. In here, give a name your source (ex. Arubalab AD)
   2. Put a desc like “Arubalab Active Directory Servers”
   3. Choose the type as Active Directory
   4. Click next
   5. In the Primary tab;
6. Type the hostname of the primary domain controller (dc01.arubalab.loc)
7. Now put in the Bind DN (it can be any user name like user1). So, the result will be ‘user1@arubalab.loc’
8. Here you can specify a password for the user
9. Then check if the Base DN works by pressing the ‘Search Base DN’ button
10. Then if there isn’t any problem, you will see the over the Base DN the active directory on the LDAP Browser.
11. Click save and leave there.

Now you can add the (Arubalab AD [Active Directory]) AD as an authentication source.

1. Then click next to continue
2. Skip the role mapping for now as you’ll come to it later
3. In the Enforcement tab, for now leave the Enforcement Policy as [Sample Allow Policy], so it will just allow access, if this authentication is successful.

D) Go to the ClearPass Policy Manager – Administration – Certificates – Certificate Store, then follow the instructions:

What is RADIUS Certificate and what is it used for?

A RADIUS server certificate is used to prove that the RADIUS server a client is authenticating to is in fact the correct server. Based on the CN on the certificate, the end-user can feel secure knowing that they will not fall victim to a Man-In-The-Middle attack.

Well what is this CN?

The Common Name (CN), also known as the Fully Qualified Domain Name (FQDN), is the characteristic value within a Distinguished Name (DN). Typically, it is composed of Host Domain Name and looks like, "www.digicert.com" or "digicert.com".

INSTRUCTIONS

1. Under the Server Certificates, select an authentication server you created before
2. Then select usage of this authN server as certificate as ‘RADIUS / EAP (Extensible AuthN Protocol) Server Certificate’

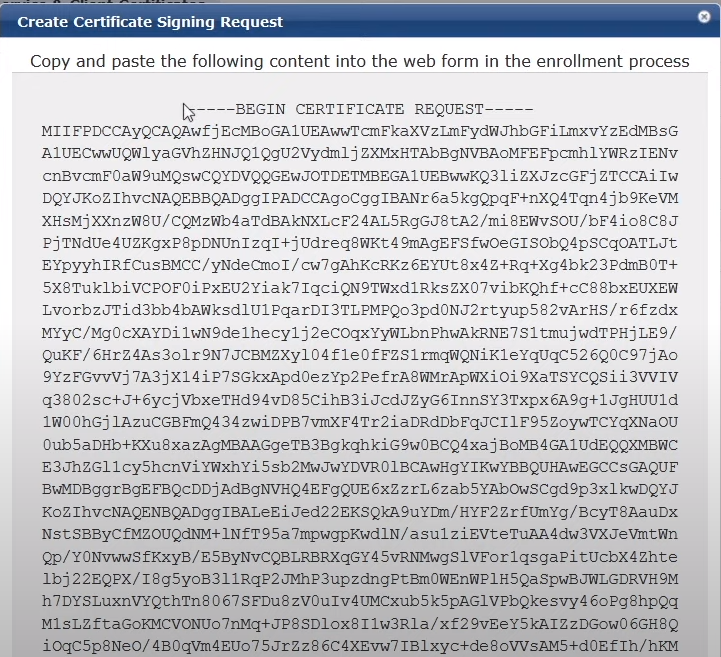
NOTE: For the RADIUS certificate, the details are in the Certificate 101 Technote, but it’s strongly recommended to have that issued a private certificate authority.

So not a sell-signed, but you need a private certificate authority. If you have that, and issue the certificate from there, so you have control over the issuing CA (Certificate Authority). As well you can make certificates with slightly longer running times. You can make sure that if you want to renew your certificate that your certificate authority is still available. There are multiple reasons to have the private certificate authority to issue your RADIUS certificate for ClearPass. So, there are no big benefits of having a public certificate authority. Because compared to the HTTPS certificate (we are comparing to HTTPS certificate just because its certificate is recommended to be a public certificate) where you can check the content in the certificate (for example the cppm1.lab.airheads.eu); if you are connecting to the Airheads-Corp SSID which you specified before in the beginning configurations, there’s no way of validating if you are connecting to the right SSID and if you’re using the right certificate server. So, there is not so much a use-to-use public certificates for RADIUS.

So for the RADIUS certificate, you could use the same approach as for the public certificate and import it, but instead you’ll do it the other way here!

1. Create a certificate signing request then go into your AD Certificate Services and issue that certificate and import it in the ClearPass server.
2. In the request box, the first thing you need to do is to change the common name to another name (radius.arubalab.loc i.e.)
3. Change the IP address entered with the same name you typed the above in the the subject alternative name (SAN) section.

NOTE: By the way this RADIUS certificate is the same type of certificate as a web server certificate. So, you could use your web server certificate as well! But as mentioned, it’s not recommended to use a public certificate for RADIUS!

1. Then enter your Private Key Password which you created before and verify it.
2. Select the private key type as 4096-bit RSA.
3. The digest algorithm should be SHA-512.
4. Click submit.
5.  Then you’ll encounter such as thing in the following figure:

11. You have your certificate signing request (which is for the RADIUS certificate) now! Copy it and go to your primary domain controller (In this sample, the dc01.arubalab.loc) in other words your certificate authority. (To go exactly, type the browser for example: dc01.arubalab.loc/certsrv as url)

12. Then it’ll prompt an authentication by requesting your username and password, enter them and click ok.

Inside, under the ‘Select a task’, click on ‘Request a certificate’ link. Instead of the user certificate, choose the advanced certificate request option. Then it’ll prompt you to enter a certificate signing request, paste here the certificate signing request that you copied before.

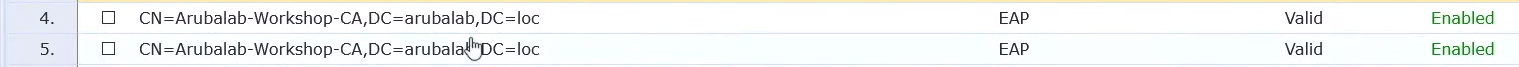
13. As last, select the certificate type as Web Server, then click submit. Download it in Base-64. So, here is your new certificate!

1. As well, you need to download also the CA certificate. To do that, go back the previous main page and click the ‘Download a CA certificate, certificate chain or CRL’ link then and the encoding method as Base-64 then download the both CA certificates in order. (Like first the current and then the previous).
2. Go back to the ClearPass Policy Manager to import your CA root.

In this context, go to the Trust List where is placed under the Certificate Store section.

Note: Remember, the first certificate file that you downloaded was the certificate which is the primary certificate (the certificate for the RADIUS), but the second one was the current CA root certificate which is needed to import the primary (the first) certificate as permission! The third one was the previous CA root certificate!

So, to do this click to the Add button, and in the Pop-Up upload your private CA root certificate file you downloaded before. In this context, click the browse button and select your second .cer file. And then the use-type will be EAP as you’ll use the root for RAIUS!

Then click Add Certificate.

The difference between two is that the expiration date! The bottom one is the previous, so the one below has expired!

16. Go back to the certificate store, and import your RADIUS certificate (the first certificate downloaded).

17. Click Import Certificate, then follow the following instructions:

1. Select the certificate type as ‘Server certificate’.
2. Select the Upload Method as ‘Upload Certificate and use saved private key’ option
3. Browse the first file to upload it
4. Then click import button.

Now you can see that you have the certificate!

18. Now put his certificate on the other subscriber node as well. In order to do that export this certificate here. (That’s the easiest way!)

NOTE: If we take a look at the Publisher – Subscriber Model, then first we know what does a cluster mean:

A cluster is a logical connection of any combination of ClearPass hardware or virtual appliances.

This chapter provides guidance on how to design and deploy ClearPass Policy Manager clusters, how to complete major tasks such as adding a Subscriber node and deploying a standby Publisher, as well as how to rejoin a down node to the cluster. Finally, the set of cluster-specific CLI commands is included.

Authentication Requests in a Cluster

The typical use case for Policy Manager is to process authentication requests using the policy framework. The policy framework is a selection of services that work to process authentication requests, but the policy framework also determines authentication, authorization, posture, enforcement, role, etc. of the endpoint/end-user.

In the context of cluster operations, authentication typically involves a read-only operation from the configuration database. A cluster node receives an authentication request, determines the appropriate policies to apply, and responds appropriately. This does not require a configuration change, and can therefore be scaled across the entire cluster.

NOTE: Authentication is performed from the node itself to the configured identity store, whether locally (as synchronized by the Publisher; for example, a Guest account) or externally, such as with Microsoft Active Directory.

Logs relevant to each authentication request are recorded separately on each node, using that node’s log database. Centralized reporting is handled by generating a Netevent from the node, which is sent to all Insight nodes and recorded in the Insight database.

ClearPass Databases

Each ClearPass server makes use of the following databases:

**Configuration database**. Contains most of the editable entries that can be seen in the ClearPass user interface. This includes, but is not limited to:

|  |  |  |
| --- | --- | --- |
|  |  | * Administrative user accounts |

|  |  |  |
| --- | --- | --- |
|  |  | * Local user accounts |

|  |  |  |
| --- | --- | --- |
|  |  | * Service definitions |

|  |  |  |
| --- | --- | --- |
|  |  | * Role definitions |

|  |  |  |
| --- | --- | --- |
|  |  | * Enforcement policies and profiles |

|  |  |  |
| --- | --- | --- |
|  |  | * Network access devices |

|  |  |  |
| --- | --- | --- |
|  |  | * Guest accounts |

|  |  |  |
| --- | --- | --- |
|  |  | * Onboard certificates |

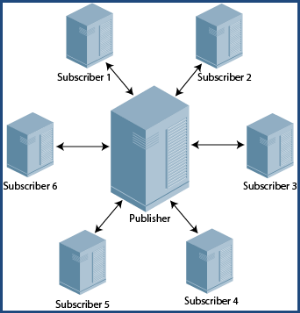
|  |  |  |
| --- | --- | --- |
|  |  | * Most of the configuration shown within Guest and Onboard |

**Log database**. Contains activity logs generated by typical usage of the system. This includes information shown in Access Tracker and the Event Viewer.

**Insight database**. Records historical information generated by the Netevents framework. This database is used to generate reports (for related information, see [Deploying ClearPass Insight in a Cluster](https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/Cluster%20Deployment/Insight_enabling.htm)).

**Publisher/Subscriber Model**

ClearPass uses a Publisher/Subscriber model to provide multiple-box clustering. Another term for this model is *hub and spoke*, where the hub corresponds to the Publisher, and the spokes correspond to the Subscribers.

[](https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/Resources/Images/Cluster_spoke_hub.png)**Figure 1***Publisher and Subscribers in Hub and Spoke Configuration*

The **Publisher node** functions as the master controllerin a cluster. The Publisher is your central point of configuration, monitoring, and reporting. It is also the central point of database replication. All the databases are managed through the Publisher.

|  |  |  |
| --- | --- | --- |
|  |  | There is at most one active Publisher in this model, and a potentially unlimited number of Subscribers. |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | The Publisher node has full read/write access to the configuration database. All configuration changes must be made on the Publisher. The Publisher node sends configuration changes to each Subscriber node. |

The **Subscriber nodes**are worker nodes. All the AAA load, all RADIUS requests, and the node where policy decisions are being made are on the Subscriber nodes.

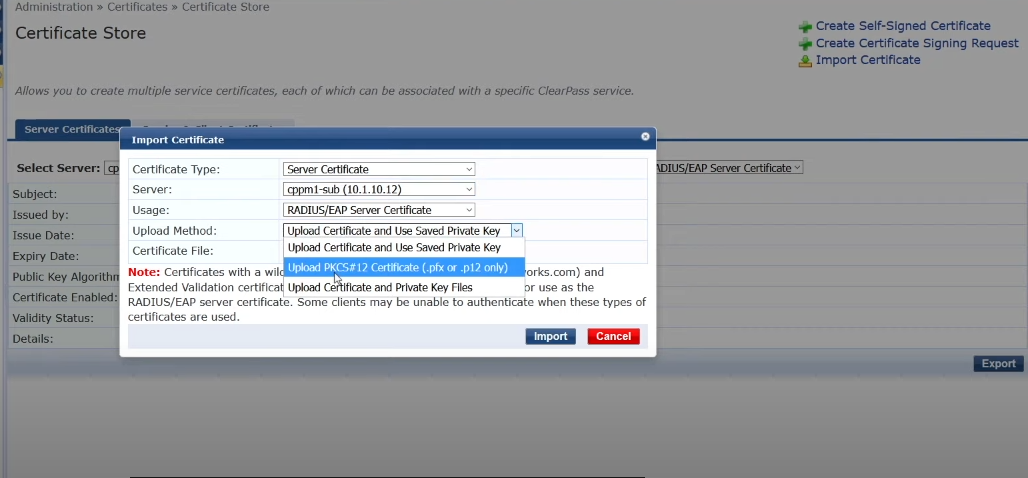
|  |  |  |
| --- | --- | --- |
|  |  | Subscriber nodes maintain a local copy of the configuration database, and each  Subscriber has read-only access to a local copy of the configuration database. |
|  |  |  |

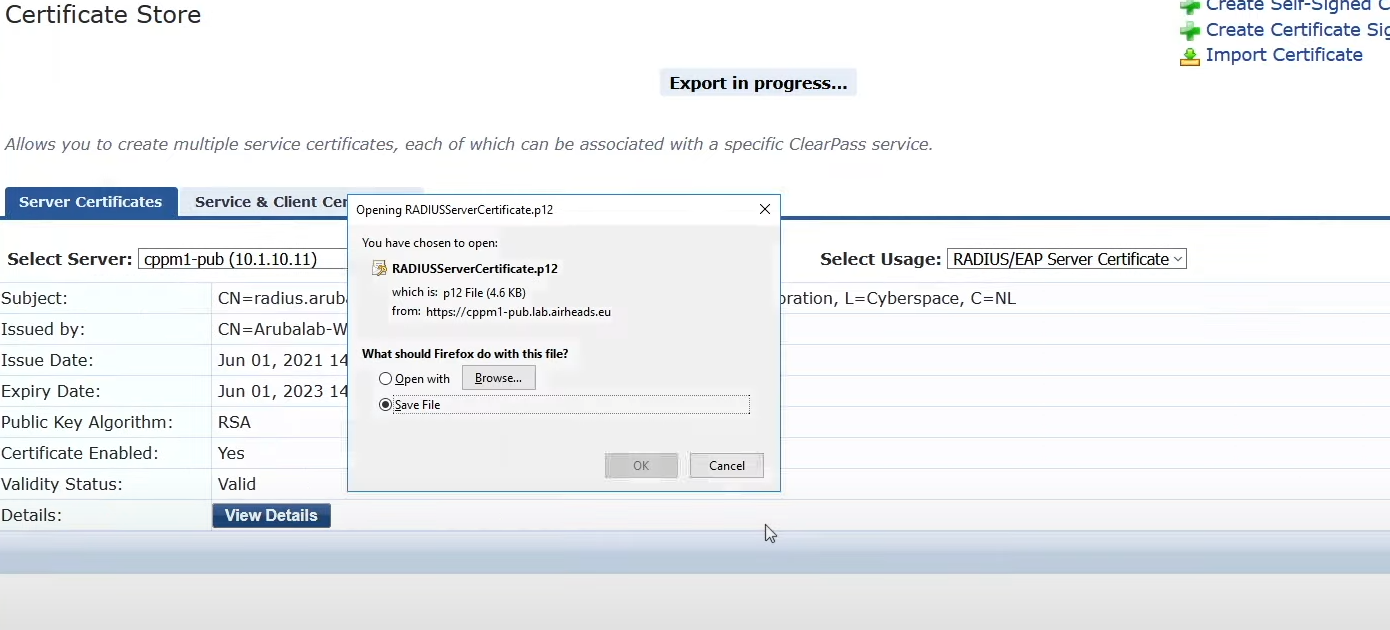
19. Click export button and select the ‘YES’ option to export the file with password protection and then specify a password / secret key then click export again. When you clicked, the RADIUSServerCetificate.p12 file will download.

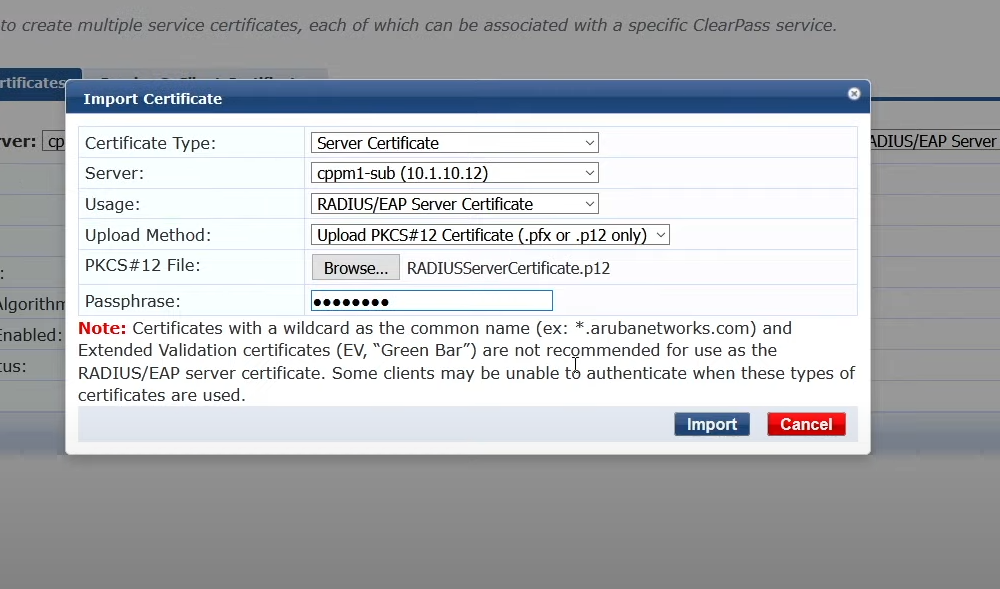
20. Now import the certificate that you exported before in the other subscriber node, to do this; click the Import Certificate link.

21. Select the other server [subscriber node – in the figure it’s cppm1-sub (10.1.10.12)].

Then select the upload method as Upload PKCS#12 Certificate (.pfx or .p12 only), and click the browse to upload the RADIUSServerCetificate.p12.







As last put in the passphrase, then click import! After that you have your certificate on the publisher.

E) Go to the client (it may be a vm) and try to connect to SSID that we created. And likely it’ll work.

F) Check the Access Tracker for everything is good or not.

1. Go to the Aruba ClearPass – Monitoring - Live Monitoring - Access Tracker
2. There you can see you are connected as the host (host-based authN)

You can see the all details in the Pop-Up window Summary.

