

Welcome back now that you understand the architecture of DNS and have seen how our domain is registered and after that domain is registered it's added into the gear DNS system. Now I want to talk about **zones**. Remember, **zones are actually the databases of DNS. They store the records for a particular part of DNS.** So linuxacademy.com will be a zone and the domain that I registered in the previous lesson so associatecats.com that will also be a zone and it's been added to Route 53 as part of that registration process.

Now zones contain records, so if I go inside associatecats.com it won't have many records because we've not created any but **every zone contains at least these records**. So **the names of records and the SOA or star of authority records.** Now **these zones are hosted by a name server and these same servers delegated to be authoritative for that domain and that happens at a zone in a level above in the DNS hierarchy.** So when we registered the domain associatecats.com the operator of the .com domain added a record into the .com zone file, which delegated the service that we chose so Route 53 to be authoritative for associatecats.com and **that is how a zone and the servers that that zone lives on become authoritative** and I talked about that in the previous lesson.

This lesson I want to focus on these actual zones. **These are the databases inside DNS and Route 53 supports two different types of zones: public zones and private zones.** Now public zones at the default type. **These are the type that get created when you register a domain directly inside Route 53 or you migrate a domain into Route 53. A public hosted zone in Route 53 has the same name as the domain it relates to.** So when we registered associatecats.com as a domain, so if go to register domains this list the actual domains. So associatecats.com there is a zone created with that same name that's hosted on the Route 53 name servers. **Now public zone is accessible globally**. So because the .com zone delegates to these name servers and because DNS is a publicly globally accessible platform then a public zone that's hosted in Route 53 and is delegated to be authoritative for that domain by definition, that's publicly accessible. So any records that I create inside associatecats.com are going to be public and available to everyone and I'm going to demonstrate that now with a quick demo.

So I'll move across to EC2. I'm going to launch an EC2 instance. It's going to be a T3.micro. I'm going to put it inside the VPC that I've been using throughout this section of the course so VPC demo and it's going to be in a public subnet. So I may as well pick public A I'll expand advanced details and I'm going to paste in some user data. Now, this is available inside the folder for this lesson in the course GitHub repository. It's inside 04\_networking topic for DNS fundamentals, private public zones and then public cats. So inside there is a file called userdata.txt and inside there is the copy of this user data. So I'll make sure I'll link that in the lesson description, but I'm just going to paste that in here on the move to next storage I'll add tags. I'm going to add the key name and for the value I'm going to pick public cat. I'll configure security groups and I'll call it web and SHH I'll put that into the description as well. I'll add another rule allowing HTTP through. I'll change both of these to my IP only, go to review and launch, click Launch. I'll pick the VPC demo key pair that I've used earlier in the course and I'll launch this instance. Now, this will take a couple of minutes to create, but this is just going to be a simple public website. So I'm going to open this instance. Get the public IP and then open that in a new tab and there we go. That's a simple public cat website. That's Larry the Cat who's the official mouser of number 10 Downing Street, which is the official residence of the UK Prime Minister. So that's just a simple demo website, and that's publicly accessible. Now that we've got this available, I'm going to copy the IP address into my clipboard and move back across to the Route 53 console. I'm going to open up the hosted zone area of the console and go into associate cats and I'm going to create an A record. So I click on create record set. It's going to be an A record, and I'm going to use www. I'm going to paste in the IP address at that EC2 instance, and I'll create the record. So now we've got the fully qualified domain name www.associatecats.com. If I open that in a new tab that also opens the same public website. So this is a publicly hosted zone. It's available from the public internet, but it's also available from inside a VPC and I'm going to demonstrate that so I'll go back to the AWS console. I'm going to open a new tab this time to EC2 and I'm going to launch another instance, but it's going to be a windows instance. So, launch instance this time I'm going to search for windows, which is something I've not done so far in this course. This is only going to be online for a short period. So I'll select window server 2019 base and that's a data center edition. So I'll select that I'm going to pick a T3.large just to ensure that we get some decent performance. Again, I'll pick VPC demo and I'll put it in the public subnet A and I'll go to our storage. The volume needs to be encrypted so I'm going to select this dropdown. Pick the default EBS key. Click to add tags. This time I'll add a tag. The key is going to be name. The value is going to be Windows server. I'll go to security groups. I only want to allow port 3389 into this Windows machine, which is the port for Windows remote desktop and again, I'll change it to my IP address. Go to review and launch, launch, and I'll pick the VPC demo key pair. So I acknowledge that and launch the instance. So I'm going to give it a chance to create and then after a couple of minutes, I'm going to select it, right click, and put connect. Now this is a Windows machine so I'll need to get the administrator password. So I click on get password and I'll need to provide the PEM key as authentications are provide that and then it will give me the administrator password for the instance. So I'll click choose file and provide that key. So once I provided that key I'll be given access to the administrator password for that instance and I'll need to go ahead and use my remote desktop application to connect. So that's what I'll do. I'll click on download remote desktop file and that'll download a configuration file that I can use to connect to this instance. I'm going to need to get the admin password copied out into my clipboard, and then I'll go ahead and start remote desktop. Once I've done that I'll need to enter the username and the admin password, which I've done, and it will log me in to the Windows server desktop. Now, I've already gone ahead and installed the Chrome browser inside this window server but if I try to open that website, I'm going to get an error and that's because if you remember the security group that I created on the public cats EC2 instance, only allowed connections from my IP. So I'm going to move back to the console and change that. So I'll go to the EC2 dashboard running instances. I'll select public cat, select the web and SSH security group, inbound rules, edit, and then for HTTP, I'm going to change it to anywhere. I'll go ahead and click on Save and then move back to the Windows instance. Then if I refresh the website at this point, I get the same public cat website that I was browsing for my local machine. **So that demonstrates that the public hosted zone that we've got inside Route 53 is available both from the public internet and inside a VPC.**

Now the other type of hosted zone that's available inside Route 53 is a **private hosted zone and a private hosted zone is created in much the same way as a public hosted zone, except that it's done explicitly. These don't get created when you register a domain or migrate a domain in to Route 53 you have to go create hosted zone and explicitly set it to a private hosted zone for Amazon VPC**. Now private hosted zones can have the same naming formats as public hosted zones, except that you have to associate them with individual VPCs. **So generally you create these manually and associate them with only the VPCs that you want to be able to access them and at that point, you can attempt to do resolution inside that VPC and it works fine.**

Now I'm going to go ahead and create a private hosted zone, and I'm going to call it associatecatsprivate.com. I'm going to do this to differentiate it from the public one and of course, I'll need to select the VPC that I want this to be accessible from. So I'll scroll down to North Virginia, I'll select VPC demo, and I'll hit Create. So that's created the private hosted zone and I'll go ahead and create a new record set it's going to be www and then I'll need the IP address of the EC2 instance for public cat. So I'm going to get that. That's 3.88.211.34 in my case. Copy that into my clipboard. Paste it into the value. Just delete the URL components of it. So I've just got the IP address and then hit Create. So now I've got this private hosted zone which has a record inside it. So the fully qualified domain name of this private record is www.associatecatsprivate.com. Now if I copy this into my clipboard and attempt to open it in a new tab I'll get an error because **it's not a publicly accessible zone. It isn't accessible from the public internet but if I move back over to my window server instance, open a new tab on this one, and attempt to open this private zone from here. In this case, it will work because the private hosted zone is associated with this VPC. So this server has been allocated the Route 53 resolver, which is the network plus two address in the VPC and this has been configured because of this association between this private hosted zone, and the VPC. It's been configured so only inside this VPC It'll resolve to the public cat website, but it won't resolve from the public internet, so that's one of the advantages of private hosted zones.**

Now, **in order for private zones to work, you do need to have the enable DNS hostnames on enabled DNS support on the VPC.** So if you recall from an early lesson there are two options that do need to be enabled on custom VPCs. So if I go to the VPC console, click on your VPCs select the VPC demo, and then go to actions and enable DNS resolution, this is where those two options are set. So this is one of those boxes, and the other one is if I go to enable the DNS hostnames. That's the order. So both of those need to be enabled on the VPC if you want to utilize Route 53 private zones.

Now, there is one other concept that I want to demonstrate and to do that, I'm going to need to create a new EC2 instance, I'm going to open up the EC2 console again and I'm going to create a new instance. It's also going to be a Linux instance. So I'm going to select Amazon Linux two once again I'm going to pick a T3.micro and I'll skip through this fairly quickly. I'm going to select VPC demo and again, I'm going to pick public A as the subnet. I'm going to expand the advanced details and this time, I'm going to paste in some other user data. Now for this there's also a private cats folder inside this lesson's folder in the GitHub repository for this course and I'm going to paste in the user data from this folder. So, private cats, this is slightly different. It's a different website just to illustrate these are two different servers, so I'm going to paste in that user data. I will make sure this is linked in the lesson description. If you need to test it out yourself, going to go to next add storage, I'll leave that as default I'll add some tags. The key will be name. The value will be private cat, configure security group, and then for security groups, I'm going to select an existing security group and I'll pick the web and SSH group created earlier in this lesson. Remember, this already has HTTP from anywhere as well as SSH from IP address, I'll go to review and launch, launch it, pick the VPC demo key pair and acknowledge that I've still got it and then launched the instance. Now the next concept I want to talk about is a concept known as **split view.**

Up until now I have created a public zone inside Route 53. So that's associatecats.com. I'll go back to the Route 53 console to illustrate this. We've got associatecats.com, which is a public zone, and associatecatsprivate.com, which is a private zone **but I can also create a private zone with the same name as a public zone.** So I'm going to go ahead and do that now I'll create a hosted zone, and I'll call it associatecats.com, just like the public one. I'll set it to private hosted zone and I'll select the VPC demo VPC and hit create. So now we've got two different zones. We've got a public zone called associatecats.com and a private zone called associatecats.com. **Now, at the moment, the private zone only has these two default DNS records. Whereas the public one has both of those as well as the www record for the public cat website.** So that's important right now I've got a private hosted zone which is available inside the VPC that I've got the Windows server running in and I've also got a public hosted zone. The concept that I want to talk about is **split view and split view is the concept of where you create a private zone and a public zone with the same name. What that allows you to do is actually set up the same records, but with different targets.** I'm going to give you an example of this. So now that we know that this EC2 instance will have finished, I'm going to look at this private cat instance. Copy the IP address and open it in a new tab and then we go, we got private cat. So this is Palmerston another cat that lives on Downing Street in the UK. Now I'm going to copy of the IP address for private cat and go back to the Route 53 console. What I'm going to do is I'm going to go into the associatecats.com private zone. I'm going to create a record set. I'm going to name the host www and I'm going to paste in the IP address of the private cat website. I'll just remove the URL components again and then I'll create that record. So now we've got two records with the same name www.associatecat.com. We've got one of them in a public zone, one of them in a private one. Now, if I open this from the public internet, I still get Larry the cat, so I still get the public cat website but if I go back to the window server instance and I open the original associatecats.com website, if I do refresh now, I get the private cat. This is what's known a split view. **Now split view allows you to have one website that's available on the public internet using one name so www.associatecats.com and then have a different website available using the same name on private networks. Now, why might you want this? Well, you might have two different versions of websites. You might have one version of the website that's accessible internally and maybe includes different information or an admin interface but you want that website to be accessible using the same DNS name as the public website and you do that using split view. The way that split view works is if you have two zones, a public and a private, and if in any of those zones you have a same named record so, www in this case, well, inside the VPC, the private zone overrides the public zone. If you have two zones and the private one doesn't have any records then there is no override. This public name would still work inside the VPC if I hadn't have created the same named record inside the private zone. So it doesn't impact the functionality of public zones unless you override them with same name record in a private zone and this is extremely powerful. It lets you test out new versions of applications, have internal view of applications, and you can do it without disrupting your public facing application.**

Now, you might need to know this for the exam. You might be asked how you'd present two different versions of your application one internal and one external and if you do face that scenario, **you need to use split view DNS, create a public zone inside Route 53 or another DNS provider and have that as normal, accessible from the public internet, but then create a private hosted zone, map it to whatever VPCs you need to view it from, and then you can access that same record but pointing at a different target.** Now that's everything I wanted to cover in this lesson about public zones, private zones, and split view DNS. It's a pretty simple set of concepts, but they're all concepts that you will need for the exam.