AWS® Certified Cloud Practitioner

STUDY GUIDE

FOUNDATIONAL (CLF-C01) EXAM

Includes interactive online learning environment and study tools:

Two custom practice exams

100 electronic flashcards

Searchable key term glossary

BEN PIPER
DAVID CLINTON

SYBEX®
A Wiley Brand

Route 53

Route 53 is Amazon's global Domain Name System (DNS) service. The primary purpose of DNS is to translate human-readable domain names (such as `example.com`) into IP addresses. Here's a simplified version of how it works: when you enter the domain name `example.com` into your web browser, your computer sends out a query to its configured DNS server asking for the IP address of that domain. The DNS server then sends the query to the domain's authoritative DNS server—the one that's in charge of the `example.com` domain name. The authoritative DNS server responds with the IP address for `example.com`. This process of translating a domain name to an IP address is called *name resolution*.

Resource Records

Name resolution goes beyond just mapping domain names to IP addresses. DNS can store mappings for different types of data, including IPv6 addresses, mail servers, and even arbitrary text. When you send an email to someone, DNS provides the lookup mechanism to ensure it gets routed to the correct mail server for that domain.

For DNS to work, someone must first define some resource records for a domain. A resource record consists of several fields, but the most important are the name, type, and value. Refer to Table 10.1 for some example resource records.

TABLE 10.1 Resource Records for the benpiper.com Domain

Name	Type	Value
`benpiper.com`	A - IPv4 address	93.184.216.34
`www.benpiper.com`	A - IPv4 address	93.184.216.34
`benpiper.com`	MX - Mail exchange	10 in1-smtp.messagingengine.com

Domain Name Registration

A public domain name is one that anyone on the internet can resolve. To ensure that no two entities try to use the same domain name, anyone who wants to have a public domain name must register it with a domain registrar. When you register a domain name, you must do so under a top-level domain (TLD) such as `.com`, `.net`, or `.org`. For example, you might register the name `example.com` or `example.org`. Route 53 is a domain registrar for hundreds of TLDs.

Registering a domain gives you control of it for the duration of the lease, which can be in yearly increments between 1 year and 10 years. Regardless of how long you initially register a domain for, you can renew it in yearly increments indefinitely. If you have an

existing domain name with another registrar, you can transfer it to Route 53. Transferring a domain entails extending the registration by at least one year.

It's important to understand that domain name registration and DNS hosting are two different functions. Registering a domain name gives you control over it for the duration of the lease, including the right to specify the service you want to provide DNS hosting for the domain. This means the domain registrar and DNS hosting provider don't have to be the same company, but they often are. Route 53 is both a registrar and a DNS hosting provider.

Hosted Zones

To have Route 53 host the DNS for a public domain name, you create a public hosted zone and specify the domain name. You can then define the resource records for that domain. If you use Route 53 to register a domain name, it automatically takes care of creating a public hosted zone for the domain.

Route 53 can also provide name resolution for private domain names. A private domain name is one used on a network other than the internet. Route 53 private hosted zones provide DNS resolution for a single domain name within multiple VPCs. This is useful for assigning user-friendly domain names to VPC resources such as EC2 instances or application load balancers. For example, instead of hardcoding a database server's IP in an application, you can define a record in a private hosted zone with the name db.`example.com` that points to the database server's IP address. Because private domain names aren't accessible from the internet, there are no registrars, so you can pick any domain name you want. Name resolution for private hosted zones is not available outside of the VPC you select.

Routing Policies

In some cases, you just need a domain name to resolve to a particular IP address. But there are other times when you want the value of a resource record to change dynamically to work around failures or ensure users get pointed to the least busy server. Route 53 lets you accomplish this with a variety of routing policies.

Simple The Simple routing policy is the default for new resource records. It simply lets you map a domain name to a single static value, such as an IP address. It doesn't check whether the resource the record points to is available.

Weighted A Weighted policy distributes traffic across multiple resources according to a ratio. For example, when introducing a new web server, you may want to route only 10 percent of the traffic to the new server while evenly distributing the load across the rest.

Latency A Latency policy sends users to resources in the AWS Region that's closest to them. This is useful if, for instance, you want to send European users to the eu-west-1 region while sending users in the United States to the us-east-1 region.

Failover A Failover policy lets you route traffic to a primary resource unless it's unavailable. In that case, traffic will be redirected to a secondary resource.

Geolocation A Geolocation policy lets you route users based on their specific continent, country, or state.

Multivalue Answer A Multivalue Answer policy allows you to evenly distribute traffic across multiple resources. Unlike Weighted policies that return a single record, a Multivalue Answer policy returns all records, sorted in a random order.

Health Checks

All routing policies with the exception of Simple can use health checks to determine whether they should route users to a given resource. A health check can check one of three things: an endpoint, a CloudWatch alarm, or another health check. All health checks occur every 10 seconds or 30 seconds.

Endpoint Endpoint health checks work by connecting to the endpoint you want to monitor via HTTP, HTTPS, or TCP. Route 53 has health checkers in several AWS Regions, and you can choose which health checkers a health check uses. This lets you ensure that an endpoint is reachable from various locations around the world.

CloudWatch alarm A Route 53 health check can monitor the status of a CloudWatch alarm. This is useful if you want to consider a resource unhealthy if it's experiencing high latency or is servicing a high number of connections.

Calculated This type of health check monitors the status of other health checks. For example, if you want to consider the status of both an Endpoint health check and a CloudWatch alarm health check, you can create a Calculated health check to take both into account.

Traffic Flow and Traffic Policies

If you require complex routing scenarios for a public hosted zone, creating multiple resource records with a variety of different routing policies can become an administrative nightmare. As an alternative to manually engineering routing policies, you can use the Route 53 Traffic Flow visual editor to create a diagram to represent the desired routing.

The diagram you create represents a traffic policy that you can save and associate with a domain name by creating a policy record. Route 53 doesn't create the individual resource records but instead hides the routing behind the single policy record. The cost is currently $50 USD per month per policy record.

You can use the same routing policies that are available with normal resource records: Simple, Weighted, Latency, Failover, Geolocation, and Multivalue Answer. But in addition, Traffic Flow offers another routing policy that's not otherwise available: Geoproximity. The Geoproximity routing policy lets you direct users to a resource based on how close they are to a geographic location. This differs from the Geolocation routing policy that routes based on the user's specific continent, country, or state.

CloudFront

Amazon CloudFront is a content delivery network (CDN) that helps deliver static and dynamic web content to users faster than just serving it out of an AWS Region. For example, if you're hosting a website from a single AWS Region, as a general rule, the farther a user is away from that region, the more network latency they'll encounter when accessing it. CloudFront solves this problem by caching your content in a number of data centers called *edge locations*. There are more than 150 edge locations spread out around the world on six continents.

CloudFront works by sending users to the edge location that will give them the best performance. Typically, this is the edge location that's physically closest to them. CloudFront also increases the availability of your content because copies of it are stored in multiple edge locations.

The more edge locations you use, the more redundancy you have and the better performance you can expect. As you might expect, the price of CloudFront increases as you utilize more edge locations. You can't select individual edge locations. Rather, you must choose from the following three options:

- United States, Canada, and Europe
- United States, Canada, Europe, Asia, and Africa
- All edge locations

To make your content available via CloudFront, you must create a distribution. A distribution defines the type of content you want CloudFront to cache, as well as the content's origin—where CloudFront should retrieve the content from. There are two types of distributions: Web and Real-Time Messaging Protocol (RTMP).

Web A Web distribution is the most common type. It's used for static and dynamic content such as web pages, graphic files, and live or on-demand streaming video. Users can access Web distributions via HTTP or HTTPS. When creating a Web distribution, you must specify an origin to act as the authoritative source for your content. An origin can be a web server or a public S3 bucket. You can't use nonpublic S3 buckets.

RTMP The Real-Time Messaging Protocol (RTMP) delivers streaming video or audio content to end users. To set up an RTMP distribution, you must provide both a media player and media files to stream, and these must be stored in S3 buckets.

Summary

Virtual Private Cloud (VPC) provides the virtual network infrastructure for many AWS resources, most notably EC2. VPCs can connect to other networks, including the following:

- The internet via an internet gateway
- External, private networks via Direct Connect or a virtual private network (VPN)
- Other VPCs using VPC peering

The Route 53 service provides two distinct but related Domain Name System (DNS) services. Route 53 functions as a registrar for many top-level internet domain names (TLDs). You can register a new domain with Route 53 or transfer an existing one that you control. Route 53 also provides DNS hosting services. To use Route 53 with a public domain, you must create a public hosted zone. To use Route 53 for name resolution within a VPC, you must create a private hosted zone.

CloudFront is Amazon's content delivery network (CDN). It improves delivery of data to end users by storing content in edge locations around the world. When a user connects to a CloudFront distribution to retrieve content, CloudFront serves the content from the edge location that will give them the best performance.

Exam Essentials

Know the components of a VPC. The key components of a VPC include at least one subnet, security groups, network access control lists (NACLs), and internet gateways.

Understand the different options for connecting to resources in a VPC. You can connect to resources in a VPC over the internet, a Direct Connect link, a VPC peering connection, or a virtual private network (VPN) connection.

Understand the difference between a Route 53 public hosted zone and a private hosted zone. A public hosted zone allows anyone on the internet to resolve records for the associated domain name. A private hosted zone allows resolution only from resources within the associated VPCs.

Be able to select the best Route 53 routing policy for a given scenario. All routing policies except the Simple routing policy can use health checks to route around failures. If you want to direct traffic to any available resource, Failover, Weighted, and Multivalue Answer routing policies will suffice. If performance is a concern, choose a Latency routing policy. If you need to direct users based on their specific location, use a Geolocation routing policy.

Know how CloudFront improves the speed of content delivery. CloudFront caches objects in edge locations around the world and automatically directs users to the edge location that will give them the best performance at any given time.

Be able to identify scenarios where CloudFront would be appropriate. CloudFront is designed to give users the fastest possible access to content regardless of their physical location. By caching content in edge locations that are distributed around the world, CloudFront helps ensure that your content is always close to your users.