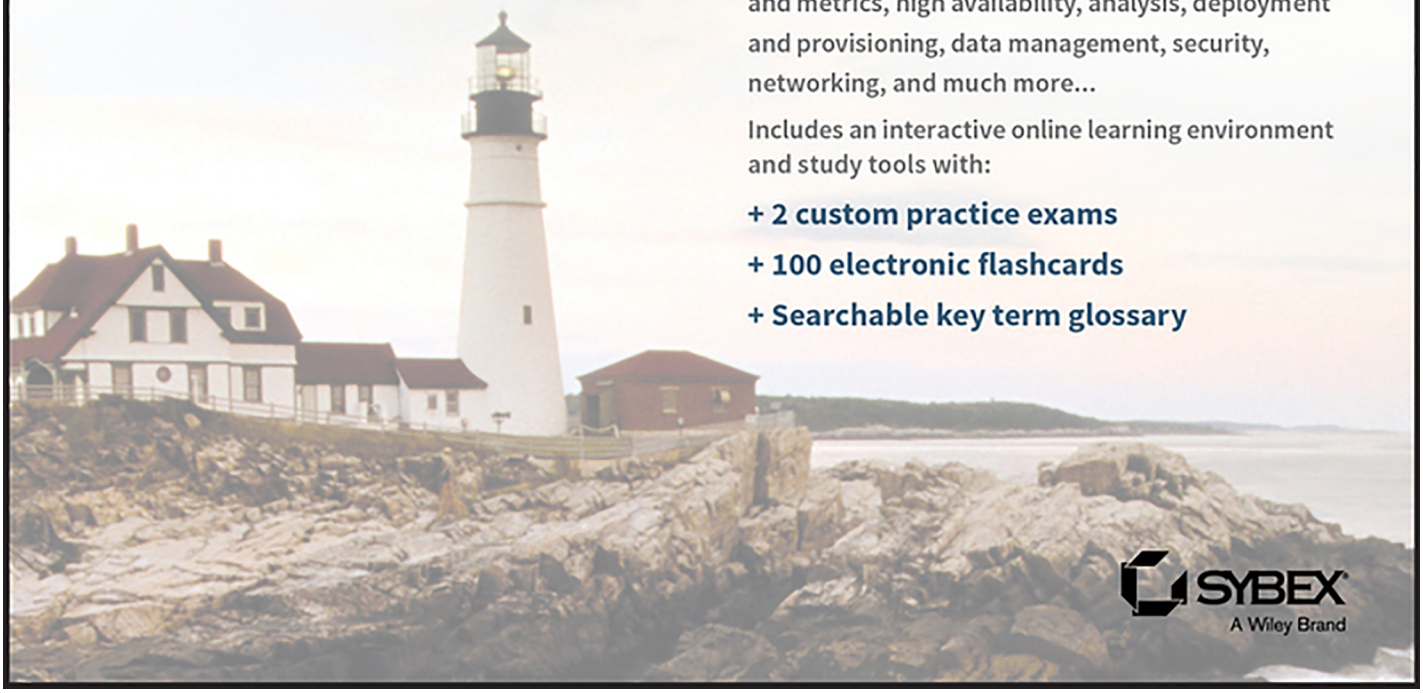
amazon web services

Stephen Cole, Gareth Digby, Chris Fitch,
Steve Friedberg, Shaun Qualheim, Jerry Rhoads,
Michael Roth, Blaine Sundrud

AWS Certified SysOps Administrator

OFFICIAL STUDY GUIDE

ASSOCIATE EXAM



Covers exam objectives, including monitoring and metrics, high availability, analysis, deployment and provisioning, data management, security, networking, and much more...

Includes an interactive online learning environment and study tools with:

+ 2 custom practice exams

+ 100 electronic flashcards

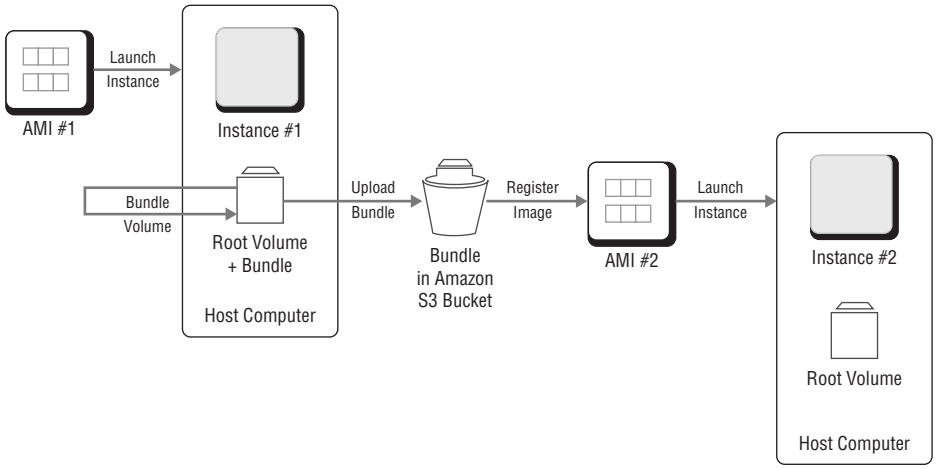
+ Searchable key term glossary

SYBEX
A Wiley Brand

AMIs on Instance Store

To create an instance store-backed AMI, start from an instance that you have launched from an existing instance store-backed Linux AMI. Customize the instance to suit your needs, then bundle the volume and register a new AMI. Figure 6.6 summarizes the process of creating an AMI from an instance store-backed instance.

FIGURE 6.6 Process to create an AMI from an instance store-backed instance



The bundling step is different compared to Amazon EBS, with which you can create an AMI directly from an instance or a snapshot.

Once an instance store AMI is created, all root volumes will be built on the instance store when using that AMI.

The bundling process is a multi-step function that we are not going to cover in this book, as it falls outside the scope of the exam. Nevertheless, you should look up the online documentation and practice making an instance store-backed AMI to understand the process.

Amazon Elastic File System (Amazon EFS)

Amazon EFS is not a true unformatted block service but rather a fully managed file storage service. Multiple Linux Amazon EC2 instances connect to Amazon EFS through standard operating system I/O APIs. Amazon EFS can also connect to on-premises Linux servers through AWS Direct Connect.

Amazon EFS is designed to be automatically flexible in sizing, growing from gigabytes of shared storage up to petabytes in a single logical volume.

Amazon EFS vs. Amazon EBS

When comparing the two options, it is important to look closely at the primary use cases. Amazon EFS is designed to provide regional, durable, multi-user file systems. Amazon EBS is designed for single Amazon EC2 volumes.

Because of its design, Amazon EBS is significantly cheaper when looking at per-GB cost of storage. If there is no need for multiple instances to attach to the storage, Amazon EBS will likely be a good place to start your operation.

Once you have multiple users, however, Amazon EFS will often be a much less expensive option. Cost savings are more apparent once you consider the regional redundancy and durability that is rolled into Amazon EFS, bypassing the need to build your own highly available, regionally redundant file system. This becomes even more important when you consider the maintenance overhead that you avoid when using Amazon EFS over a DIY solution.

Provisioning Amazon EFS

After creating Amazon EFS using the Create API, you create endpoints in your Amazon Virtual Private Cloud (Amazon VPC) called "mount targets." When mounting from an Amazon EC2 instance, you provide the Amazon EFS Domain Name System (DNS) name in your `mount` command. The DNS resolves to the mount target's IP address. If your instance has access to the mount target in the VPC, you will then be able to access the file system.

This will be the same mount target that peered Amazon VPC instances or on-premises instances will use. They are granted access to the host VPC through the networking methods, and that will complete their ability to connect to the file system as well.

Instances then connect to the system with an NFSv4.1 client. See Figure 6.7 for the AWS CLI command to create an Amazon EFS.

FIGURE 6.7 Amazon EFS create command

```
rhoadsg@chaos:~$ aws efs create-file-system --creation-token CertBook --region us-east-1
{
    "SizeInBytes": {
        "Value": 0
    },
    "CreationToken": "CertBook",
    "CreationTime": 1499132308.0,
    "PerformanceMode": "generalPurpose",
    "FileSystemId": "fs-6d41ce24",
    "NumberOfMountTargets": 0,
    "LifeCycleState": "creating",
    "OwnerId": "123456789abc"
}
rhoadsg@chaos:~$
```

Securing Amazon EFS

The mount target you created when you provisioned the file system can use Amazon VPC security groups (the same ones that you use to secure access to Amazon EC2). All of the same rules of ingress and egress control can then be managed in detail with that toolset.

The mount targets are also specifically assigned to subnets (which by extension means that you should include mount points in a subnet in each Availability Zone in which you intend to run connected instances). This means that network Access Control List (ACL) control would also apply at the subnet level, if needed, for additional controls over an instance connecting from outside the subnet where the mount targets exist.

Encryption is not yet available natively on Amazon EFS as of this writing.

File access inside the system is controlled with standard UNIX-style read/write/execute permissions based on the user and group ID asserted by the mounting NFSv4.1 client.