COPYRIGHT

Copyright © 2016 by Anitian Corporation

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the Anitian Corporation, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

For permission requests, write to the publisher, at the address below:

Anitian Corporation
9780 SW Shady Ln, Suite 100
Portland OR, 97223
info@anitian.com
www.anitian.com
# TABLE OF CONTENTS

1. EXECUTIVE SUMMARY ........................................................................................................... 4
   1.1. Intended Audience ........................................................................................................... 4
   1.2. Premises .......................................................................................................................... 4
       1.2.1. As Is Disclaimer ..................................................................................................... 4
       1.2.2. Intent .................................................................................................................... 4
       1.2.3. Prerequisite Knowledge ......................................................................................... 5
       1.2.4. PCI Scoping ........................................................................................................... 5
       1.2.5. Compensating Controls ........................................................................................ 5

2. AWS PCI COMPLIANCE OVERVIEW .............................................................................. 6
   2.1. AWS PCI Compliance Status ........................................................................................ 6
   2.2. AWS PCI Compliance Scope ......................................................................................... 6
       2.2.1. Out of Scope AWS Services .................................................................................. 7
   2.3. AWS PCI Compliance Responsibility ......................................................................... 8
       2.3.1. Amazon Responsibility - Security of the Cloud ....................................................... 8
       2.3.2. Customer Reasonability - Security in the Cloud .................................................... 9

3. GENERAL PCI DSS GUIDANCE ...................................................................................... 10
   3.1. Requirement 1: Install and maintain a firewall configuration to protect cardholder data... 10
   3.2. Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters .................................................................................................................. 11
   3.3. Requirement 3: Protect stored cardholder data .............................................................. 12
   3.4. Requirement 4: Encrypt transmission of cardholder data across open, public networks ... 14
   3.5. Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs .............................................................................................................. 15
   3.6. Requirement 6: Develop and maintain secure systems and applications ................... 15
   3.7. Requirement 7: Restrict access to cardholder data by business need to know ............... 16
   3.8. Requirement 8: Identify and authenticate access to system components ...................... 17
   3.9. Requirement 9: Restrict Physical Access to Cardholder Data ........................................ 17
   3.10. Requirement 10: Track and monitor all access to network resources and cardholder data ... 18
   3.11. Requirement 11: Regularly test security systems and processes ................................. 19
   3.12. Requirement 12: Maintain a policy that addresses information security for all personnel... 19
   3.13. Requirement A.1: Shared hosting providers must protect the cardholder data environment... 19

4. REFERENCE ARCHITECTURES ..................................................................................... 20
   4.1. Architecture 1: Dedicated ............................................................................................. 20
       4.1.1. Overview ............................................................................................................... 21
       4.1.2. PCI Scope .............................................................................................................. 21
       4.1.3. Applicable AWS Services ...................................................................................... 22
       4.1.4. Build Out .............................................................................................................. 22
   4.2. Architecture 2: Segmented .......................................................................................... 36
       4.2.1. Overview ............................................................................................................... 36
       4.2.2. PCI Scope .............................................................................................................. 37
       4.2.3. Applicable AWS Services ...................................................................................... 37
       4.2.4. Build Out .............................................................................................................. 37
   4.3. Architecture 3: Connected ........................................................................................... 41
       4.3.1. Overview ............................................................................................................... 41
       4.3.2. PCI Scope .............................................................................................................. 42
       4.3.3. Applicable AWS Services ...................................................................................... 42
5. CONCLUSION .................................................................................................................................. 50

5.1. Support ................................................................................................................................................. 50

APPENDIX A. ADDITIONAL GUIDANCE FOR DESV ......................................................................... 51
A.1. What is DESV? ...................................................................................................................................... 51
A.2. DESV Requirements .............................................................................................................................. 51

APPENDIX B. AWS PCI DSS RESPONSIBILITY MATRIX SUMMARY .................................................. 53

APPENDIX C. CITATIONS ................................................................................................................ 59
1. EXECUTIVE SUMMARY

This workbook provides guidance on building an environment in Amazon Web Services that is compliant with the Payment Card Industry Data Security Standard (PCI DSS).

1.1. Intended Audience

The intended audience for this workbook includes:

- Organizations looking to build a PCI DSS-compliant environment in AWS.
- PCI Qualified Security Assessors (QSA) and others assessing Cardholder Data Environments (CDEs) running in AWS.

This workbook provides guidance for a customer building a compliant AWS environment.

1.2. Premises

This section lists Anitian’s assumptions and premises that influence the content of this workbook.

1.2.1. As Is Disclaimer

Anitian is a Qualified Assessor Company (QSAC) and the author of this workbook. The content in this workbook is based upon Anitian’s interpretations of the PCI. This content is provided “as is” with no guarantees expressed or implied. The content of this document is subject to change without notice. Likewise, future changes to the AWS environment may alter some of the guidance in this document.

Your PCI assessor may have different interpretations than Anitian and the guidance in this workbook.

None of the content in this workbook is intended to replace or supersede the requirements of the PCI DSS.

1.2.2. Intent

The purpose of this workbook is to provide guidance on deploying a PCI-compliant environment in AWS. The sections below outline how different AWS services can help support compliance with various PCI requirements.

While this workbook discusses AWS aspects useful for validating PCI compliance readiness as well as formal compliance, it does not offer step-by-step instructions on conducting an assessment of an AWS environment. However, it should assist QSAs in understanding how an AWS environment can be PCI-compliant.
1.2.3. Prerequisite Knowledge

Readers are expected to have an understanding of the following:

- The [PCI DSS](#), currently at version 3.2
- How to manage an AWS environment
- The PCI Standards Council’s [Cloud Computing Guidelines](#)

1.2.4. PCI Scoping

While this workbook discusses PCI scope reduction and segmentation within AWS, it is not a comprehensive guide on these issues in regards to overall PCI DSS compliance. Consult with your PCI Qualified Security Assessor (QSA) or the PCI Standards Council for more information on scope reduction strategies.

1.2.5. Compensating Controls

This workbook does not address compensating controls for AWS implementations. However, you may use compensating controls within AWS, provided your assessor has validated them according to PCI rules.
2. AWS PCI COMPLIANCE OVERVIEW

This section provides a general overview of AWS PCI compliance. For additional details, see Amazon’s AWS PCI Level 1 FAQ.

2.1. AWS PCI Compliance Status

AWS is currently a PCI DSS-compliant Level 1 Service Provider. Merchants and other service providers can use AWS to establish their own PCI-compliant environments. However, AWS operates on a shared responsibility model. Just because AWS is PCI DSS compliant, compliance does not automatically extend compliance to the hosted customer’s environment.

AWS customers are responsible for all aspects of PCI compliance related to their environment within AWS. This includes AWS service configurations, guest operating systems, and requisite security controls (IDS, anti-virus, etc.).

Because AWS is a PCI-compliant service provider, it is not necessary for organizations hosting at AWS to assess the AWS infrastructure as part of the organization’s PCI compliance. An assessor only needs to review AWS’s Attestation of Compliance (AOC) and Responsibility Matrix documents to validate the compliance of the infrastructure.

2.2. AWS PCI Compliance Scope

Amazon’s AWS Service Provider validation assessment for PCI compliance includes the AWS Management Environment and underlying infrastructure, including the AWS GovCloud (US) region.

The majority of the AWS Services were included in the most recent AWS PCI DSS assessment. The list below shows those compliant services as well as a description of their function:

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Scaling</td>
<td>Automated, event-based instance provisioning</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>Creates and deploys templates of AWS resources</td>
</tr>
<tr>
<td>Amazon CloudFront</td>
<td>Content delivery web service</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>Cloud access to hardware security modules</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>Reporting on AWS API calls</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>Direct, private, dedicated connection to AWS</td>
</tr>
<tr>
<td>Amazon DynamoDB (DDB)</td>
<td>Scalable and highly available NoSQL data store</td>
</tr>
<tr>
<td>Amazon Elastic Beanstalk</td>
<td>Web application deployment and provisioning</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (EBS)</td>
<td>Block-level storage for EC2 instances</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (EC2)</td>
<td>Scalable cloud machine instances</td>
</tr>
<tr>
<td>Elastic Load Balancing (ELB)</td>
<td>Application fault tolerance and load balancing</td>
</tr>
<tr>
<td>Elastic MapReduce (EMR)</td>
<td>Big data services</td>
</tr>
<tr>
<td>Amazon Glacier</td>
<td>Data archival storage</td>
</tr>
<tr>
<td>AWS Management Console</td>
<td>Web interface for managing all AWS services</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>AWS Identity and Access Management (IAM)</td>
<td>Access controls and key management</td>
</tr>
<tr>
<td>AWS Key Management Services (KMS)</td>
<td>Data encryption key management</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>High-capacity data warehousing</td>
</tr>
<tr>
<td>Amazon Relational Database Service (RDS)</td>
<td>Database as a service</td>
</tr>
<tr>
<td>Amazon Route 53</td>
<td>Scalable and highly available Domain Name System</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (S3)</td>
<td>Store and retrieve any amount of data</td>
</tr>
<tr>
<td>Amazon SimpleDB (SDB)</td>
<td>Highly available and flexible non-relational data store</td>
</tr>
<tr>
<td>Amazon Simple Queuing Service (SQS)</td>
<td>Message queuing service</td>
</tr>
<tr>
<td>Amazon Simple Work Flow (SWF)</td>
<td>Service for coordinating application components</td>
</tr>
<tr>
<td>Amazon Virtual Private Cloud (VPC)</td>
<td>A logically isolated portion of the AWS network, functioning as a private network.</td>
</tr>
<tr>
<td>Amazon EC2 Container Services (Amazon ECS)</td>
<td>Scalable, hosted Docker container instances</td>
</tr>
<tr>
<td>AWS Config</td>
<td>AWS resource inventory, change history, and change notifications</td>
</tr>
<tr>
<td>AWS Web Application Firewall (AWS WAF)</td>
<td>Protection for CloudFront-accelerated web sites from web-based attacks</td>
</tr>
</tbody>
</table>

PCI compliance for AWS applies to the following regions, availability zones and edge locations (as of July 2016):
- US East (Northern Virginia)
- US West (Oregon)
- US West (Northern California)
- AWS GovCloud (US) (Oregon)
- EU (Ireland)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- South America (Sao Paulo)

2.2.1. Out of Scope AWS Services

AWS is constantly developing and deploying new services. While, not all new services are covered under AWS’s current PCI attestation, you can still use those services in your environment. If you do use them, your assessor must review their configuration to ensure they are PCI-compliant.
For example, AWS Certificate Manager is not in scope as of the most recent AWS Service Provider Assessment. If you use AWS Certificate Manager for your in-scope web applications, you must demonstrate that your usage meets the relevant PCI requirements. However, AWS Certificate Manager does run on AWS’s compliant infrastructure. Therefore, while the service itself might not be certified as compliant, the infrastructure it runs on is compliant.

2.3. AWS PCI Compliance Responsibility

Determining which party is responsible for PCI requirements is one of the more complex aspects of cloud hosting. This section outlines how to define and organize a PCI compliance assessment for an AWS hosted environment.

This workbook outlines the areas where AWS can cover compliance requirements, and where you must cover them yourself. It is important that you consult the AWS PCI DSS “Responsibility Matrix,” which defines exactly what AWS covers. Appendix B contains a summary of this matrix. If AWS does not cover a requirement, or if there is shared coverage, then your organization has responsibility to ensure the requirement is met.

Furthermore, you cannot arbitrarily choose to ignore a PCI requirement; you must meet all the requirements. However, it is possible that not all requirements are relevant to your organization. Your PCI assessor can clarify those that apply and those that do not.

![Figure 1 – Overview of AWS Shared Responsibility](image)

2.3.1. Amazon Responsibility - Security of the Cloud

Amazon is responsible for maintaining a PCI-compliant environment that you can use to aid in your compliance. This is referred to as “security of the cloud.” AWS validates compliance annually and documents the results in AWS’s Attestation of Compliance (AOC) document. As an AWS customer, you may request a copy (with a signed non-disclosure agreement).
2.3.2. **Customer Reasonability - Security in the Cloud**

You are responsible for designing, building, and maintaining a compliant environment in AWS. This is referred to “security in the cloud.”

When you build your environment in AWS, part of that environment will be compliant because it uses AWS’s compliant infrastructure. However, the final responsibility for PCI compliance rests with your organization (not AWS). The specifics are defined in the “Responsibility Matrix” as shown in Appendix B.
3. GENERAL PCI DSS GUIDANCE

This section contains general guidance and strategies for meeting the twelve top-level PCI requirements using AWS services.

3.1. Requirement 1: Install and maintain a firewall configuration to protect cardholder data

The following AWS services can help support the firewall and network segmentation requirements of PCI:

- Amazon Virtual Private Clouds (Amazon VPCs)
- Amazon EC2 Security Groups
- VPC Network ACLs

The topics below describe the strategies and considerations for utilizing these services for compliance with Requirement 1.

Amazon VPCs

VPCs are logically isolated portions of the AWS network that create private networks within a customer’s AWS account. VPCs allow for customers to have multiple environments with no connectivity between them, as if they were air-gapped physical networks. The AWS network includes features designed to prevent packets with malformed or modified addresses from hopping across VPC boundaries.

It is possible to purposely connect VPCs to other networks. For example, Internet Gateways combined with NAT instances, Elastic IPs, and other resources can provide Internet access. VPC Peering and properly configured routing tables can connect VPCs to each other. And, as we will see in Section 4 below, it is also possible to use VPNs or AWS Direct Connect to extend on-premise networks into the cloud.

NOTE: All subnets within the same VPC have a default route between them that cannot be removed.

EC2 Security Groups

Security Groups are stateful firewall components in AWS EC2, which track established connections and only allow return traffic associated with the session. Security Group access control lists (ACLs) can be used to restrict traffic to and from instances at the IP address, port, and protocol level, for compliance with Requirement 1.3.6.

VPC Network ACLs

VPC Network ACLs apply at the subnet level, but are not stateful and (on their own) cannot be used to meet Requirement 1.3.6.

Other Strategies and Considerations

For simple environments, like those described by the reference architectures in Section 4, Anitian recommends using a dedicated cloud firewall AMI. Not only are these clearly stateful firewalls, but they can also offer many additional (and important) security functions, like intrusion prevention (Requirement 11.4 specifies the need for IDS/IPS).
There are several firewall Amazon Machine Images (AMIs) in the AWS Marketplace from companies such as Fortinet, Palo Alto, and CheckPoint. These firewall instances may require specific licensing from the vendor, but can provide familiar management interfaces and advanced capabilities.

For more complex or dynamic AWS architectures, like those employing Auto Scaling to ensure sufficient application capacity to meet demand, traditional firewalls can complicate managing the environment. For these setups, Security Groups and host-based firewalls can be used to achieve segmentation for the CDE.

3.2. Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

The following AWS service can help support the host hardening requirements of PCI:

- Amazon Elastic Compute Cloud (Amazon EC2)

The strategies and considerations for utilizing Amazon EC2 for compliance with Requirement 3 are discussed below.

**Amazon EC2**

When you use an Amazon-provided AMI to create an EC2 instance, AWS generates unique administrator and root passwords that are encrypted with uniquely generated private keys. This helps support compliance with Requirement 2.1.

Furthermore, there are no default user accounts, since you must explicitly create them.

**Other Strategies and Considerations**

If you use non-Amazon images, then you are responsible for ensuring that the defaults are changed. Consult with the relevant documentation for those images.

The AWS AOC covers the underlying security configuration management for the AWS services. However, it is your responsibility to create and implement security configuration standards for your EC2 instances. There are various solutions in the AWS marketplace that may assist with this requirement.

**NOTE:** Anitian has created hardened AMIs for all available OSes, as both base servers and with a hardened web server. They include a supporting Security Configuration Standard documenting the hardening steps performed, as required by PCI DSS Requirement 2.2.
3.3. **Requirement 3: Protect stored cardholder data**

The following AWS services can help support the encryption and key management requirements of PCI for cardholder data (CHD) at rest:

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Services (KMS)
- Amazon Relational Database Service (Amazon RDS)

The strategies and considerations for utilizing these services for compliance with Requirement 3 are described below.

**Amazon EBS**

AWS supports several different ways to store information securely. EBS non-root volumes and S3 buckets support volume-level encryption using AES-256. For EBS volumes, EBS manages encryption keys using a FIPS 140-2 compliant infrastructure.

If you store CHD (such as DB files on the file system of a dedicated DB server instance) on an instance’s encrypted volume, additional encryption is required for the CHD in order to comply with Requirement 3.4.1. This is not unique to AWS, but is cited for completeness and clarification.

**NOTE:** Not all EC2 instance types support encrypted EBS volumes. See [EBS encryption](#).

**Amazon S3**

Amazon S3 is a simple data storage service. It can encrypt stored objects with AES-256, and supports three different mechanisms for key management (see [Server Side Encryption](#)).

- **Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)**
  When SSE-S3 is enabled for an object in an S3 bucket (in the Management Console), S3 encrypts the object with a unique data encryption key. This data encryption key is itself encrypted with a master key that the S3 service rotates annually.

- **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)**
  SSE-KMS uses an envelope key to encrypt each object’s data encryption key. This allows greater control of who can decrypt data, and provides an audit log of key usage. KMS is discussed in the next section.

- **Server-Side Encryption with Customer-Provided Keys (SSE-C)**
  SSE-C allows you to use your own key and manage yourself. S3 never stores this key, only a message authentication hash of it to validate later use of the key when attempting to retrieve data.

By default, S3 is configured to use the SSE-S3. To use KMS or customer-supplied keys, you must specify the key management type when uploading the object via the console or the REST API. For further details, refer to [S3 Upload Objects](#).
AWS KMS

KMS is AWS’s encryption key management service. KMS provides automatic key rotation on an annual basis through the Management Console. See Amazon’s KMS Cryptographic Details document for additional information.

AWS KMS also has a documented API for programmatic or third-party vendor support.

KMS uses a customer master key (CMK) as the key encrypting key (KEK), and a backing key as the data encryption key. Enabling key rotation rotates the backing key.

When you enable key rotation, a new CMK and associated backing key (HBK) are generated annually. These new keys are used going forward, and the old CMK/HBKs remain available for decryption only. You can also manually create a new CMK/HBK at any time and set it as the currently active key.

NOTE: If you disable a CMK/HBK, it is no longer available to use, but attached EBS volumes that rely on the now-disabled key will continue to work. If that volume is detached from an Instance, you will have to re-enable the key to use the volume again.

CloudTrail logs all of the AWS KMS actions (key creation, data encryption, key rotation, etc.) to the CloudTrail log files in the user-specified S3 bucket.

Amazon RDS

In addition to encrypted storage, Amazon RDS also supports two different methods of database encryption. RDS encrypts the underlying storage using Amazon KMS managed keys. This protects the data at rest. RDS also supports Transparent Data Encryption (TDE) for Microsoft SQL and Oracle instances.

IAM policies control who can access RDS instances, and what actions they can perform. The databases within an RDS instance, however, rely on their own internal platform-specific mechanisms to manage access to data. Make sure to configure PCI-relevant account and password policies within CDE databases in RDS.

Other Strategies and Considerations

If you run your own DB on an EC2 instance, you are fully responsible for managing the encryption of any CHD within the DB. This encryption should be performed using the standard strategies appropriate for the particular DB in use. Common examples are programmatic encryption of CHD at the field or column level, or encryption at the DB instance level, such as TDE for MS SQL.
3.4. Requirement 4: Encrypt transmission of cardholder data across open, public networks

The following AWS components can help support the transit encryption requirements of PCI:

- Elastic load balancers
- Network ACLs
- Security Groups
- Customer Gateways
- Virtual Private Gateways
- VPN Connections
- AWS Direct Connect

The strategies and considerations for utilizing these services for compliance with Requirement 4 are discussed below.

**Elastic Load Balancers**

Elastic load balancers support SSL/TLS and can offload processing encryption for secure communications for both internal and external connections. SSL/TLS negotiation is configured using security policies. AWS provides a number of predefined security policies (see the ELB Security Policies Table for further information). You can also create your own. Security policies allow you to define the SSL protocols and ciphers, as well as the order preference for the client server negotiation during the SSL handshake.

**NOTE:** PCI DSS 3.1 states that “SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016.”

**Security Groups and Network ACLs**

Security Groups and Network ACLs can block the use of insecure protocols based on network port.

**Customer Gateways, Virtual Private Gateways, and VPN Connections**

Customer Gateways, Virtual Private Gateways, and VPN Connections enable you to set up encrypted VPN tunnels into an AWS VPC. AWS supports a wide range of common VPN solutions (see the VPC FAQ), as well as a generic text configuration file. The VPN settings are automatically created by AWS, so that you can configure your endpoint to match. After creating a VPN connection (in the VPN Connections section of the VPC dashboard), you can download the configuration file needed to set up the customer end point. You can view the configuration file to validate the encryption used (SHA1/AES 128); see Section 4.3.4.5 below for implementation details.

**AWS Direct Connect**

Direct Connect provides a dedicated high-speed connection between customer environments and AWS, similar to MPLS. Direct Connect itself is not an encrypted connection, so you will need to verify the privacy of the circuit. Depending on implementation, additional controls might be needed to comply with Requirement 4.1.
Other Strategies and Considerations

It is your responsibility to configure secure transit encryption for Internet-facing services running on EC2 instances, such as web servers. This should be included as part of the host hardening for Requirement 2.

Additionally, VPNs can be implemented on commercial firewalls or VPN AMIs running in the environment. You are responsible for configuring the device to ensure alignment with Requirement 4.

3.5. Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

AWS does not provide anti-virus protection for EC2 instances. You are responsible for ensuring that all instances run appropriate anti-virus scans as well as log and report, as defined in PCI Requirement 5.

There are numerous anti-virus solutions available in the AWS Marketplace.

3.6. Requirement 6: Develop and maintain secure systems and applications

AWS does not provide vulnerability and patch management of EC2 instances. While the AMIs are updated periodically, launched and running instances must be managed like any other host. For example, for the list of updates to the Amazon Linux AMI see the AWS Linux Security Center.

There are vulnerability and patch management solutions available in the AWS Marketplace that can assist with complying with Requirement 6.1 and 6.2.

Additionally, there are no AWS services that directly address the PCI requirements for secure software development (Req. 6.3) and change control (Req. 6.4). While not directly related to the PCI requirements, CodeDeploy and CodeCommit can assist with general source code management and deployment.

However, network segmentation technologies (discussed in Requirement 1 above) can separate production and development environments (Req. 6.4.1).

NOTE:  AWS Config records changes to resources within AWS itself, but not to applications and within EC2 instances.
AWS WAF and Amazon CloudFront
The AWS Web Application Firewall (WAF) is a PCI DSS-validated automated technical solution that can help meet PCI DSS Requirement 6.6. The WAF service helps protect publicly-facing web sites that use Amazon CloudFront for content delivery acceleration from web-based attacks.

NOTE: While Amazon CloudFront itself is not listed in Section 2.2 above as a PCI-compliant AWS service, the AWS WAF will only protect CloudFront-accelerated web applications.

Requirement 6.6 can be met either with a WAF or web application security testing. Anitian always recommends that web application security testing be performed in conjunction with any WAF deployment, so that the WAF can be tuned to explicitly address any known vulnerabilities with the web application.

3.7. Requirement 7: Restrict access to cardholder data by business need to know
The following AWS components can help support the access control requirements of PCI:

- AWS Identity and Access Management (IAM)
- AWS Directory Service

IAM
IAM service supports role-based access control within AWS. However, it is your responsibility to manage user roles and rights within the IAM service.

IAM supports users, groups and roles, as well as management of encryption keys.

Directory Service
Directory Service is a Microsoft Active Directory (AD) compatible directory service that allows you to create one (or more) instances called Simple AD. It can be deployed as a stand-alone Simple AD or can connect to an on premise Microsoft AD infrastructure.

Directory Service can manage access to AWS resources as well Microsoft AD-compatible systems and applications.

You must use a third-party tool to administer the AWS Directory Service, such as the Microsoft Active Directory Administration tools included with Windows Server. For more information, see the Admin Guide Directory Management.

NOTE: Simple AD directories do not support Microsoft Active Directory Web Services interfaces.

Other Strategies and Considerations
It is your responsibility to ensure all user roles and rights are documented with least privilege rights clearly explained.
3.8. Requirement 8: Identify and authenticate access to system components

The following AWS services can help support the account management requirements of PCI:

- IAM
- Directory Service

IAM

IAM supports password policies in accordance with Requirement 8, with the exception of account lockouts for invalid login attempts (Req. 8.1.6), minimum lockout durations (Req. 8.1.7), and idle session timeouts (Req. 8.1.8). Meeting these requirements with IAM requires using a PCI compliant external identity provider that can enforce these requirements, or Directory Service.

**NOTE:** IAM is only used for identity and access management to AWS resources, not authentication to EC2 instances and applications.

Directory Service

Simple AD supports all of the password and account policy settings that Microsoft AD uses, which fully supports Requirement 8 (Create a Directory).

Other Strategies and Considerations

For any directory services running on an EC2 instance, it is the customer’s responsibility to ensure that all password policies are configured to meet Requirement 8.

3.9. Requirement 9: Restrict Physical Access to Cardholder Data

AWS’s AOC fully covers the physical security of AWS for Requirement 9. As long as you host your entire PCI environment in AWS, this requirement is covered.

AWS’s AOC does not cover any in-scope assets hosted outside of AWS.
3.10. Requirement 10: Track and monitor all access to network resources and cardholder data

The following AWS services can help support the log management requirements of PCI:

- AWS CloudTrail
- S3

**CloudTrail**

The AWS CloudTrail service can assist with tracking and monitoring access to a resources within an AWS account. The primary components supported by CloudTrail are log aggregation, alerting, and retention (Req. 10.5 to 10.7).

It is your responsibility to create an S3 bucket to receive and store the log files, and ensure that Cloud Trail is enabled to capture the required security events (Req. 10.2).

The CloudTrail Event Record Body supports all specific elements in Requirement 10.3. For more information, see the Event Reference Record.

**S3**

Retention policies for CloudTrail data are configured in S3. By default, the retention period is infinite, but is fully configurable (see Lifecycle Configuration).

**NOTE:** *For a cost-effective way to comply with Requirement 10.7, you can use S3 Lifecycle Configuration to set the retention period to 90 days and automatically archive older data to the Amazon Glacier storage service for long-term retention (required to be at least one year).*

Additionally, you must enable access control on the S3 bucket storing the CloudTrail logs. This must include limiting bucket write access to CloudTrail and bucket read access to authorized users.

**Other Strategies and Considerations**

Amazon’s CloudTrail is a basic logging service that can fulfill the PCI requirements for logging. While CloudTrail provides audit logging for access to AWS resources, it does not log events and activity for the applications you run on AWS. There are several Amazon Machine Images (AMIs) in the AWS Marketplace from companies such as Splunk, HP (ArcSight), and Alert Logic that can help you manage logs from your applications.

If you already use a Security Information and Event Management (SIEM) product, CloudTrail supports an API that your SIEM product may be able to use to collect its logs, or for advanced data correlation. Check with your SIEM vendor for additional information.

You must configure EC2 instances for network time protocol (NTP) to comply with Requirement 10.4.
3.11. Requirement 11: Regularly test security systems and processes

AWS’s AOC fully covers detection of rogue wireless access points (Req. 11.1). AWS does not provide vulnerability scanning, (Req. 11.2), penetration testing (Req. 11.3), intrusion prevention (Req. 11.4) or file change detection (Req. 11.5) within EC2 instances. However, there are numerous solutions in the AWS marketplace supporting many of these requirements. Anitian provides network penetration testing and web application security testing.

**NOTE:** *Penetration testing must be scheduled and approved through AWS. See [AWS Penetration Testing](#) for further details*

3.12. Requirement 12: Maintain a policy that addresses information security for all personnel

AWS does not provide any of the policy documentation as defined in Requirement 12 (and other PCI requirements). You will need to write this material on your own.

3.13. Requirement A.1: Shared hosting providers must protect the cardholder data environment

If you provide shared hosting as part of your EC2 instances, you are fully responsible for protecting your customers’ CHD. You will need to segment and isolate the CDE correctly to comply with Requirement A.1. The following services can assist with this:

- Requirement 1 – VPCs, Security Groups
- Requirements 7 and 8 – IAM and Directory Service
4. **REFERENCE ARCHITECTURES**

This section defines three common AWS reference architectures to help you build or assess a PCI-compliant environment.

1. **Dedicated**: An AWS PCI environment that is not connected to anything else
2. **Segmented**: A CDE and in-scope systems within a larger AWS environment
3. **Connected**: An environment that has both AWS and on-premise items

These reference architectures use Microsoft Windows platforms for the web and application tiers, and Amazon RDS for the database tier. While other OS platforms may have slightly different configurations, the architectures are generally the same.

**NOTE:** Determining the scope of compliance in an AWS hosted environment is largely the same as scoping an on-premise environment. The scope of compliance is dependent upon the cardholder data flows and segmentation strategies in use.

### 4.1. Architecture 1: Dedicated

This architecture demonstrates an e-commerce website hosted in a dedicated Amazon AWS account and contained in a single, private network.

*Figure 2 - Stand-alone e-commerce website architecture*
4.1.1. Overview

In the Dedicated reference architecture, there are three subnets in the default VPC:

- DMZ CDE
- Internal CDE
- Internal Management

The DMZ is an Internet-facing network containing the web server EC2 instance.

The In-scope internal subnet contains a Jumpbox, used to manage and provide support, security, patching, and other required services to the CDE Instances.

The Internal subnet is only accessible by the DMZ and in-scope instances via Security Groups (described in detail below), and contains an application server instance and RDS.

NOTE: Anitian has created a CloudFormation script using hardened AMIs for implementing the reference architectures.

4.1.2. PCI Scope

The CDE is comprised of the systems in the two CDE subnets:

- Web Server
- Application Server
- RDS DB instance

For this scope, the web server accepts CHD, which then flows through the application tier to the DB for storage.

The Jumpbox does not transmit, process, store, or otherwise handle cardholder data in this architecture. Placing it in a dedicated management network segregates it from the CDE, but does not remove it from the PCI assessment scope because it directly connects to, and can impact their security of, hosts in the CDE.
4.1.3. Applicable AWS Services

The following AWS services help support compliance with PCI 3.2 requirements for this architecture:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>PCI Requirements Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>2.2.4, 3.4, 3.5, 3.5.2-3, 3.6, 3.6.1-5, 3.6.7, 6.4.1-2, 7.1, 7.1.1-3, 7.2, 7.2.1-3, 8.1, 8.1.1-2, 8.2, 8.2.1, 8.2.3-6, 8.3, 8.3.1, A.1.2</td>
</tr>
<tr>
<td>KMS</td>
<td>3.1, 3.4, 10.5, 10.5.1-5, 10.7</td>
</tr>
<tr>
<td>S3</td>
<td>3.1, 3.4, 10.5, 10.5.1-5, 10.7</td>
</tr>
<tr>
<td>CloudTrail</td>
<td>10.1, 10.2, 10.2.2-7, 10.3, 10.3.1-6, 10.5, 10.5.1-5, 10.7, A.1.3</td>
</tr>
<tr>
<td>CloudWatch</td>
<td>10.1, 10.2, 10.2.2-7, 10.3, 10.3.1-6, 10.5, 10.5.1-5, 10.7, A.1.3</td>
</tr>
<tr>
<td>EC2</td>
<td>1.1, 1.1.4, 1.2, 1.2.1, 1.3, 1.3.1-7, 2.1, 4.1, 6.4.1</td>
</tr>
<tr>
<td>Security Groups</td>
<td></td>
</tr>
<tr>
<td>AMIs</td>
<td></td>
</tr>
<tr>
<td>EBS</td>
<td></td>
</tr>
<tr>
<td>RDS</td>
<td>3.4</td>
</tr>
<tr>
<td>Config</td>
<td>2.4, 11.5</td>
</tr>
<tr>
<td>VPC</td>
<td>1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7</td>
</tr>
</tbody>
</table>

4.1.4. Build Out

This section describes the primary steps for building out the reference architecture.

4.1.4.1. Create IAM Groups and Assign Permissions

First, define who can access and who can manage the environment. AWS requires you to explicitly define all your accounts and passwords, which ensures there are no shared defaults.

Figure 3 – Create users
4.1.4.2. Create Storage Encryption Keys

Use KMS to create keys for encrypting data storage locations. In this architecture, there will need to be at least one key created for the database instance that will contain cardholder data (CHD).

![Create Alias and Description](image)

_Figure 4 – KMS configuration_

In AWS, you can separately assign permissions to manage an encryption key and to use the key for encryption, which allows for enforcing least-privilege.

**NOTE:** While non-root volumes attached to AWS instances can also be encrypted using KMS keys, the disk encryption is transparent to the operating system running in the instance. Management of access to the data on encrypted disk is not separate and independent from the operating system, as required by PCI Requirement 3.4.1.

It is best practice, and a PCI requirement (Req. 3.6.4), to change encryption keys used to protect data on a regular basis. This limits how long a compromised key is usable.

After creating the key, click on its URL in the Encryption Keys section of the Identity and Access Management AWS service. The Key Rotation setting is in the listed properties for the selected key. This allows you to automate key rotation within a designated cryptoperiod in alignment with Requirement 3.6.4.

![Key Rotation](image)

_Figure 5 – Key rotation option_

4.1.4.3. Create Subnets

For this architecture, you need at least four separate subnets:
- A DMZ subnet for the web server
- A management subnet for the Jumpbox
- Two internal subnets for the application and database systems.
These internal subnets need be in different availability zones, so that we can setup RDS redundancy in a later step.

Figure 6 – Configuring a subnet

Use the VPC service management page in the AWS console to configure subnets, even for the Default VPC EC2 Classic uses.

Figure 7 - VPC Service Management page with three new subnets

4.1.4.4. Configure Routing

When creating a new subnet, it will use the main route table for the VPC that will include one route allowing internal traffic for that subnet only.
Only the DMZ and Management subnets need to have routes to the Internet Gateway. This ensures only instances in these subnets support direct inbound or outbound Internet connections.

**Figure 9 - Gateway route for DMZ**

4.1.4.5. **Create Security Groups**

Security groups function like an inbound firewall. They restrict incoming instance network access to predefined sources, IP protocols, and TCP or UDP ports.
Figure 10 - Security Group Rules
They can also reference other Security Group(s) in the same VPC as allowed sources. For example, you can reference the application servers Security Group to restrict access to a Microsoft SQL Server to only instances in that group.

Figure 11 - Security Groups are stateful and block all access not explicitly allowed
This architecture uses five Security Groups to accomplish the architecture depicted:
Figure 12 - Logical Firewall / Security Group Design

Web Server Security Group

This group allows inbound web client connections from anywhere and outbound web services connections to internal application servers.

Figure 13 - Web Server Security Group Inbound Rules
Figure 14 - Web Server Security Group Outbound Rules

**Application Server Security Group**

This Security Group allows incoming web service connections from the web servers to the application servers.

Figure 15 - App Server Security Group Inbound Rules

The group allows outbound MySQL connections to the RDS database instances.

Figure 16 - Application server security group outbound rules

**Database (RDS) Security Group**

Security Groups can secure network access to RDS instances, although RDS only uses the inbound rules.
These rules allow MySQL connections from the application servers, and from other RDS instances in the group to support database replication.

**Figure 17 - DB Server Security Group Inbound Rules**

**Management Security Group**

The Management Security Group is a special group that allows RDP and ICMP connections from the Jumpbox to all instances, for management purposes.

**Figure 18 - Management Server Security Group Inbound Rules**

**Jump Box Security Group**

The Jumpbox itself only needs to allow connections from the public IP address of your company’s network.
NOTE: You must implement two-factor authentication for remote access to meet Requirement 8.3. There are numerous third-party products that can support this for a Windows or Linux system. AWS does not natively support two-factor authentication for remote access to EC2 instances. However, AWS does support multi-factor authentication to AWS itself. For more information, see AWS MFA details and pricing at http://aws.amazon.com/iam/details/mfa/.

Figure 19 - Jumpbox Server Security Group Inbound Rules
The Jumpbox will need outbound communication to the web and application servers for management purposes.

Figure 20 - Jumpbox Server Security Group Outbound Rules

4.1.4.6. Create Hardened AMIs from secured instances

PCI requires the development of secure configuration standards for all system components. AWS allows for the creation of one secure instance that will serve as a template for the creation of pre-secured systems.

Launch a new instance for each of the types needed for deployment. For this architecture, a web server, an application server, and an application or base server instance for the Jumpbox are required (the database will use the AWS RDS service).
These instances are only going to live long enough to perform host hardening and configuration steps. Make sure each of these instances are part of the Jumpbox Security Group, is in the Management subnet, and has an Elastic IP or a Public IP, so that you can remotely connect to and manage them.

Public IPs are provisioned by AWS when an instance is launched. This is automatic in the Default VPC, but configurable by subnet in other VPCs (see the Amazon VPC User Guide for further information).

Elastic IPs (EIPs) are managed by a customer and associated with the AWS account, not a specific instance. You can reassign which instance uses a specific EIP without the address changing.

Connect to and harden your instance. Make sure you document all steps taken to secure the instance, as your assessor will need to review these.

**NOTE:** Alternately, you can use Anitian’s pre-hardened AMIs, which include a security configuration standard document. These are available in the AWS Marketplace.

Once you are finished, and the instance is ready, power it off and create a custom AMI from it.
4.1.4.7. **Launch Instances from Hardened AMI**

This architecture needs a minimum of three instances:

- **Jumpbox instance**
  - Used to manage the environment remotely
  - In the Management subnet, it will need an EIP or a public IP

- **Web server instance**
  - Front-end to the e-commerce application
  - In the DMZ subnet, it will need an EIP or a public IP

- **Application server instance**
  - App tier running middleware that brokers connectivity between web servers and DB (RDS in this example)
  - In the internal subnet. It is only accessible by the web server and Jumpbox, and is the only instance with access to the DB

Launch the EC2 instances from the newly created AMIs.
4.1.4.8. Create Subnet Group

Subnet Groups allow RDS to determine where redundant instances need to be located to survive the failure of the primary instance.

Manage Subnet Groups from the RDS service management page. Create one that contains the two Internal CDE subnets created earlier.

4.1.4.9. Create Encrypted RDS Instance

Using the KMS key and Subnet Group already created, launch the encrypted RDS instance that will store CHD.
When creating the RDS instance, a few settings need special attention in order to meet PCI requirements. The DB instance Class needs to be db.m3.medium or higher to support encryption.

**Figure 25 - Selecting instance class that supports encryption**

Additionally, ensure that you:

- Select the RDS Security Group created earlier, to ensure AWS does not create a new “default” Security Group.
- Select “Yes” for Enable Encryption, and choose the KMS key created earlier.
4.1.4.10. Install application software

Once the RDS DB instance is finished provisioning, the environment is ready.

**NOTE:** The steps in this build focus on leveraging the AWS services for compliance. Numerous additional PCI requirements will need to be addressed in order to ensure this environment is compliant, including (but not limited to) anti-virus, patch management, log management, vulnerability management, and file integrity monitoring.
4.2. Architecture 2: Segmented

This architecture builds upon the previous design. It demonstrates an e-commerce website segmented from other systems in an existing Amazon AWS environment.

Segmenting the CDE systems from the rest of an AWS account limits the scope of PCI compliance.

In the Segmented reference architecture, there are two private networks contained in separate VPCs:

- **CDE VPC**
  - Contains the DMZ CDE, the Management, and Internal CDE subnets.

- **Out-of-scope VPC**
  - Contains two subnets, in private networks segmented from the CDE.

The systems and subnets in the CDE VPC network are the same as those in the first architecture. The new VPC represents additional systems and subnets that do not require connectivity to any CDE systems. This architecture demonstrates how to remove the new VPC from the PCI assessment scope through segmentation.

To segment the out-of-scope networks, they must not connect to the CDE. In a traditional environment, this is typically accomplished using firewall policies, switch ACLs, VLANs, or other network segmentation and isolation technologies.

In AWS, Security Groups can control traffic into and out of CDE instances, but they do not meet the routing configuration requirements in PCI Requirement 1.2. Similarly, you cannot use the default VPC that EC2 creates, because within a single VPC all instances are part of the same supernet (this is partly why all the systems in the first architecture are in scope).
However, VPCs represent separate, private network spaces. They each use their own private address space, and are isolated from other networks and other resources in an AWS account. They provide the most direct way to implement true network segmentation for PCI scope reduction.

**NOTE:** In order to ensure that your CDE VPC is segmented from your out-of-scope VPC, you must not implement VPC peering between them. This could bring the non-CDE VPC into your assessment scope (which is an appropriate strategy in some circumstances, but not used in this example).

### 4.2.2. PCI Scope

The CDE is comprised of the following instances in this architecture, all contained within the private CDE VPC network:

- Web server
- App server
- RDS DB

The new VPC is out-of-scope for PCI due to network segmentation, as discussed below.

### 4.2.3. Applicable AWS Services

The following AWS services helps to support compliance with PCI requirements for this architecture:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>PCI Requirements Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>2.2.4, 3.4, 3.5, 3.5.2-3, 3.6, 3.6.1-5, 3.6.7, 6.4.1-2, 7.1, 7.1.1-3, 7.2, 7.2.1-3, 8.1, 8.1.1-2, 8.2, 8.2.1, 8.2.3-6, 8.3, 8.3.1, A.1.2</td>
</tr>
<tr>
<td>KMS</td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>3.1, 3.4, 10.5, 10.5.1-5, 10.7</td>
</tr>
<tr>
<td>CloudTrail</td>
<td>10.1, 10.2, 10.2.2-7, 10.3, 10.3.1-6, 10.5, 10.5.1-5, 10.7, A.1.3</td>
</tr>
<tr>
<td>CloudWatch</td>
<td></td>
</tr>
<tr>
<td>EC2</td>
<td>1.1, 1.1.4, 1.2, 1.2.1, 1.3, 1.3.1-7, 2.1, 4.1, 6.4.1</td>
</tr>
<tr>
<td>Security Groups</td>
<td></td>
</tr>
<tr>
<td>AMIs</td>
<td></td>
</tr>
<tr>
<td>EBS</td>
<td></td>
</tr>
<tr>
<td>RDS</td>
<td>3.4</td>
</tr>
<tr>
<td>Config</td>
<td>2.4, 11.5</td>
</tr>
<tr>
<td>VPC</td>
<td>1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7</td>
</tr>
</tbody>
</table>

### 4.2.4. Build Out

This section describes the primary steps to build out the reference architecture.
4.2.4.1. Create a VPC

Create a new VPC network to contain and segregate the out-of-scope instances from the CDE instances created in the first architecture.

Figure 28 – Creating a new VPC

The new VPC includes a NAT instance designed to work like an Internet gateway router for the private subnet. Once the VPN is created, you can delete this NAT instance to prevent other instances in the new subnets from accessing the Internet.
Figure 29 – Configure the new VPC

4.2.4.2. Create IAM Users, Groups and KMS Keys

IAM resources are not region or VPC specific. All resources within an AWS account share the same IAM resources.

Create these as outlined above in Sections 4.1.4.1 and 4.1.4.2.

4.2.4.3. Create Resource in the VPC

When creating resources, be sure to select the newly created VPC in the “VPC” dropdown of each resource creation wizard.
NOTE: Not all AWS resources are specific to a single VPC or region. If a resource cannot be found on the VPC Dashboard, try looking in the EC2 service management console.

Figure 30 – Create VPC subnet

4.2.4.4. Internet Access

The VPC network will need its own Internet gateway. Create the gateway, and then attach it to the VPC.

Figure 31 – Attaching an Internet Gateway to a VPC
4.3. Architecture 3: Connected

This architecture represents connecting an on-premise CDE into an Amazon AWS environment.

Figure 32 – Connected on-premise systems into AWS CDE

4.3.1. Overview

In the Connected reference architecture, there are three private networks in AWS and two typical on-premise networks:

**AWS Networks**

1. **CDE VPC**
   - This is the VPC from Architecture 1, with a DMZ and internal CDE subnet.

2. **Out-of-scope VPC**
   - This is the new VPC from Architecture 2, fully segmented with no VPC peering.

3. **In-Scope VPC**
   - This is a new VPC. It is connected to the CDE via VPC peering.
On-premise Networks

1. In-Scope On-Premise Network
   This is a customer network segment connected to the AWS CDE via a VPN.

2. Out-of-scope On-Premise Network
   This is a customer network segmented from the in-scope customer network and AWS.

Extending an on-premise network into a VPC in AWS is no different than setting up other business-to-business VPN connections. In a typical VPN setup, IPsec tunnels provide private communication, for two or more trusted networks, across untrusted networks like the Internet. The same technology can be used to provide access to a private VPC network from other VPCs or even on-premise environments.

It is also possible to set up a direct, private, non-VPN connection into AWS using the Direct Connect service. Direct connect supports high bandwidth links and can be combined with 802.1q VLAN tagging to support logical segmentation. As Section 3.4 above notes, connections using Direct Connect are not encrypted. Additional controls, for example a VPN or use of TLS may still be necessary to comply with PCI 4.1, if that direct network connection is not private.

This architecture does not include its own Jumpbox as the on-premise in-scope management systems can administer the AWS CDE systems without changes to the assessment scope.

4.3.2. PCI Scope

The PCI assessment scope in this reference architecture consists of:

- The CDE VPC network (web, app, and database tiers)
- The In-Scope VPC network in AWS
- The In-Scope On-Premise network

The two in-scope networks do not have CHD, but are connected to the CDE. This architecture demonstrates two common uses cases for connected in-scope systems:

- The In-Scope VPC in AWS has systems that perform analytics on the CDE web application (without accessing CHD).
- The In-Scope On-Premise Network has systems that provide security controls for the CDE, such as anti-malware and patch management.

The two out-of-scope networks in this reference architecture have no network connectivity to the AWS CDE, as discussed in Section 4.3.1 above.

4.3.3. Applicable AWS Services

The following AWS services help support compliance with PCI requirements for this architecture:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>PCI Requirements Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>2.2.4, 3.4, 3.5, 3.5.2-3, 3.6, 3.6.1-5, 3.6.7, 6.4.1-2, 7.1, 7.1.1-3, 7.2, 7.2.1-3, 8.1, 8.1.1-2, 8.2, 8.2.1, 8.2.3-6, 8.3, 8.3.1, A.1.2</td>
</tr>
<tr>
<td>KMS</td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>3.1, 3.4, 10.5, 10.5.1-5, 10.7</td>
</tr>
<tr>
<td>CloudTrail</td>
<td>10.1, 10.2, 10.2.2-7, 10.3, 10.3.1-6, 10.5, 10.5.1-5, 10.7, A.1.3</td>
</tr>
</tbody>
</table>
4.3.4. Build Out

This section describes the primary steps for building out the reference architecture.

4.3.4.1. Create a VPC

Build the In-Scope VPC as per the steps in Architecture 2: Segmented CDE, described in Section 4.2 above.

4.3.4.2. Create a VPC Peering Connection

Create a VPC Peering connection between the CDE VPC and the newly created In-Scope VPC.

![Create VPC Peering Connection](image)

Figure 33 – Creating a VPC Peering Connection

4.3.4.3. Accept the VPC Peering Connection

After creating the VPC Peering connection, the peering request must be accepted. This is necessary as VPC Peering is supported between VPCs in different AWS accounts.
4.3.4.4. Add Routes through the VPC Peering Connection

Once the VPC Peering connection is accepted, you will be able to add routes to the peered VPC in the CDE VPC routing tables. Do not forget to add return routes from the In-Scope VPC.

4.3.4.5. Leverage In-Scope VPC Resources

After the routes are added, the In-Scope VPC systems, such as the analytic systems cited in this example, will be able to access the CDE.
NOTE: You will need to modify the CDE Security Groups, or create new ones, to allow connections from the In-Scope CDE to the appropriate CDE Instances.

4.3.4.6. Create a Customer Gateway

Within the CDE VPC, create a Customer Gateway. This resource in AWS represents a VPN concentrator at a client site.

![Create Customer Gateway](image)

FIGURE 36 – CREATING A CUSTOMER GATEWAY

NOTE: Customer Gateways also support dynamic IP routing using BGP. If dynamic is selected, the gateway will also need the ASN for the network of the remote IP address.

4.3.4.7. Create a Virtual Private Gateway

Within the VPC, create a Virtual Private Gateway (VPG). This resource in AWS represents an AWS routing target for a VPN connection.

Similar to an Internet Gateway, this a VPG is a specialized network interface used to send and receive external traffic. Attach the VPG to the VPC after creating it.
4.3.4.8. Create the VPN Connection

AWS supports industry-standard IPsec VPN connections. The VPN AWS resource provides the connection between the VPG and the Customer Gateway.

For the VPN, specify the VPG and the Customer Gateway created above.

The “Static IP Prefixes” item is the remote IP subnet to route through the VPN connection.

**NOTE:** The VPN connection includes two AWS side end-points for redundancy.
4.3.4.9. Download IPsec Configuration Details

Download the configuration needed for the On-Premise VPN concentrators. AWS supports native configuration files for a variety of firewall/VPN manufacturers such as Cisco and Fortinet.

Figure 39 – Downloading the VPN Configuration
There is a Generic option that allows the download of a text file containing the VPN connection details if you have a device not listed.

Figure 40 – Example Generic VPN Configuration File
4.3.4.10. Verify VPN Tunnel Status

After configuring the On-Premise Client VPN endpoints, verify that the VPN was able to come up. View the tunnel status from the “Tunnel Details” tab of the VPN resource details pane.

Viewing the VPN tunnels status

4.3.4.11. Leverage On-Premise Resources

After the VPN tunnels come up, the on-premise in-scope systems will be available for use within the AWS CDE, such as the AV and patch management consoles cited in this example.
5. CONCLUSION

AWS is a powerful cloud platform that offers numerous capabilities to support a fully PCI-compliant environment. However, it is important that you and your PCI assessor understand these capabilities.

This workbook clarifies some of these issues. Ultimately, achieving PCI compliance is a function of how effectively you deploy, configure, manage, and document the environment. AWS offers an outstanding platform for PCI compliance, yet it requires understanding how the AWS natively supports the various PCI requirements so you can use them correctly.

5.1. Support

If you need support with AWS, you should contact Amazon’s AWS technical support.

If you require consulting or assessment services, Anitian can help. We offer a comprehensive suite of PCI compliance services including penetration testing, vulnerability scanning, technology integration, and QSA assessment.

Contact us at: 888-264-8456, email info@anitian.com, or visit our site www.anitian.com.
APPENDIX A. ADDITIONAL GUIDANCE FOR DESV

This section contains general guidance and strategies for meeting the five additional requirements for entities subject to additional validation of PCI DSS requirements, and who are using AWS services.

A.1. What is DESV?

For some organizations, a card brand or acquirer may require additional validation that all existing PCI DSS requirements have been met. Generally speaking, this may be required of firms that:

- Handle large volumes of CHD
- Aggregate CHD from multiple places or other companies
- Have had multiple or significant CHD breaches

The PCI DSS Designated Entity Supplemental Validation (DESV) outlines these additional validation steps.

A.2. DESV Requirements

A.2.1. DE.1 Implement a PCI DSS compliance program.

AWS does not provide any of the policy or procedure documentation as defined in DE.1 (and other PCI requirements). You will need to write this material on your own.

A.2.2. DE.2 Document and validate PCI DSS scope.

There are no AWS services that directly address the DE.2 requirements for validating PCI DSS scope, that the scope is accurate based on segmentation control testing and CHD discovery processes, and that it remains valid following organizational and technical changes.

However, there are some AWS services, like those noted in Section 3 above, which can help supply information in efforts to meet this additional validation requirement. For example:

- **AWS Config** can identify changes to AWS components, helping to determine if the AWS-hosted CDE network or segmentation has changed.
- **S3** supports programmatic and command-line access to stored objects, assisting in CHD discovery efforts.
- **CloudTrail** and **CloudWatch** can be used to detect changes to the environment that may affect your assessment scope or state of compliance.
- **IAM** can be used to assign read-only access to AWS components, allowing Governance, Risk, and Compliance (GRC) solutions or personnel to gather evidence.
**A.2.3. DE.3 Validate PCI DSS is incorporated into business-as-usual (BAU) activities.**

Specific AWS services are assessed annually against the current PCI DSS version. Those AWS services that are covered in the AWS assessment scope are documented in AWS’s Service Provider AOC. As mentioned above in Section 2, AWS customers may request a copy of that AOC (with a signed non-disclosure agreement).

Consulting AWS’s AOC and the AWS PCI DSS “Responsibility Matrix” will help you determine if all the technologies used in your CDE have been, currently are, and will continue to meet the applicable PCI requirements.

**A.2.4. DE.4 Control and manage logical access to the cardholder data environment.**

Like for DE.2 above, there are no AWS services that directly address the semi-annual access reviews DE.4 requires. However, there are some AWS services, like those noted in Section 3, which can help supply information in efforts to meet this additional validation requirement. For example:

**IAM**

IAM to inventory assigned access policies and determine what access users and groups have to AWS resources that are in the assessment scope.

---

**NOTE:** While access to most AWS resources is controlled via IAM policies, access can be directly assigned in some instances. S3, for example, can have bucket access policies that are difficult to enumerate per-user.

**Directory Service**

If you use Directory Service for identity and access management within your environment, access to the service itself within AWS will also need to be documented and reviewed at least every six months.

**A.2.5. DE.5 Identify and respond to suspicious events.**

AWS does not provide incident detection, response, or analysis methodologies as required in DE.5 (and other PCI requirements). You will need to write this material on your own. However, CloudTrail and CloudWatch can be used to detect suspicious events to support incident response program.
## APPENDIX B. AWS PCI DSS RESPONSIBILITY MATRIX

### SUMMARY

The following table summarizes the responsibilities for PCI compliance between AWS and customers.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>AWS Responsibility</th>
<th>Customer Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement 1:</strong> Install and maintain a firewall configuration to protect cardholder data.</td>
<td>• <strong>All In-Scope Services:</strong> AWS maintains instance isolation for host operating systems and the AWS Management Environment including host operating system, hypervisor, firewall configuration and baseline firewall rules. &lt;br&gt; • AWS meets all requirements for implementing and managing firewalls for the AWS management environment. &lt;br&gt; • <strong>Amazon EC2 and Amazon ECS:</strong> Amazon VPC Security Groups and network ACLs implement stateful inspection network access control and are suitable for compliant network segmentation.</td>
<td>• <strong>Amazon EC2 and Amazon ECS:</strong> AWS customers are responsible for security group definitions and network access control rules.</td>
</tr>
<tr>
<td><strong>Requirement 2:</strong> Do not use Supplier-supplied defaults for system passwords and other security parameters.</td>
<td>• <strong>All In-Scope Services:</strong> AWS develops and maintains configuration and hardening standards for the AWS Management</td>
<td>• <strong>Amazon EC2 and Amazon ECS:</strong> AWS customers are responsible for changing default vendor configurations, security controls, and vendor default passwords. &lt;br&gt; • <strong>All In-Scope Services:</strong> AWS customers are responsible for secure and compliant configuration for all customer-</td>
</tr>
</tbody>
</table>
| Requirement 3: Protect stored cardholder data. | **All In-Scope Services:** Amazon EC2 and Amazon ECS: AWS customers are responsible for changing default vendor configurations, security controls, and vendor default passwords.  
**All In-Scope Services:** AWS customers are responsible for implementing encryption on all applicable internal and external network connections. (This may require use of AWS optional API encryption).  
**AWS KMS and AWS CloudHSM:** AWS customers are responsible for the creation, usage, and management of encryption keys in accordance with PCI Data Security Standards. |
| --- | --- |
| Environment that provides the virtualization technologies and applications for providing the cloud services.  
- AWS maintains configuration and hardening standards for the underlying operating systems and platforms for these services.  
- Configurable items. This may include OS configuration for Amazon EC2 and Amazon ECS instances, logging and log retention for data base services, or permissions for AWS management functions. | **All In-Scope Services:** AWS encrypts access and manages encryption within the AWS Management Environment.  
**All In-Scope Services:** AWS customers are responsible for implementing encryption on all applicable internal and external network connections. (This may require use of AWS optional API encryption). |
| Requirement 4: Encrypt transmission of cardholder data across open, public networks. | **All In-Scope Services:** AWS manages anti-virus software for the AWS Management Environment and, where appropriate, for identified services.  
**Amazon EC2 and Amazon ECS:** AWS customers are responsible for implementing anti-virus software on customer-managed OS instances commonly subject to malware. |
### Requirement 6: Develop and maintain secure systems and applications.

- **All In-Scope Services:**
  - AWS maintains security patching, development, and change control of the applications that support the services included in the assessment including web interfaces, APIs, access controls, provisioning and deployment mechanisms.
  - AWS develops and manages changes to applications that support the services included in the assessment including web interfaces, APIs, access controls, provisioning and deployment mechanisms.
  - Amazon EC2 and Amazon ECS: AWS customers are responsible for monitoring published OS and application vulnerabilities and patching on instances.
  - Customers are required to use documented change control for all configurations and customer code.
  - Customers who develop custom code that is used to transmit, process, or store credit card data must comply with requirements for secure development and testing.
  - **AWS Web Application Firewall (AWS WAF):** Customers are responsible for protecting their web applications from common web exploits. This includes (but not limited to) configuring access control lists and web application firewall rules for filtering traffic to and from their web applications.

- **Amazon EC2 and Amazon ECS:** AWS customers are responsible for monitoring published OS and application vulnerabilities and patching on instances.
- Customers are required to use documented change control for all configurations and customer code.
- Customers who develop custom code that is used to transmit, process, or store credit card data must comply with requirements for secure development and testing.
- **AWS Web Application Firewall (AWS WAF):** Customers are responsible for protecting their web applications from common web exploits. This includes (but not limited to) configuring access control lists and web application firewall rules for filtering traffic to and from their web applications.

### Requirement 7: Restrict access to cardholder data by business need-to-know.

- **All In-Scope Services:**
  - AWS maintains the access controls related to underlying infrastructure systems and the AWS Management Environment.
  - Amazon EC2 and Amazon ECS: AWS customers are responsible for access control within all OS instances.
  - **All In-Scope Services:** AWS customers are responsible for configurable access controls within the services, such as database users within Amazon RDS.
  - **AWS IAM & AWS Credentials:** AWS customers are responsible for managing access to all AWS services that are included in their CDE. AWS IAM can be used to configure resource management and AWS configuration roles and permissions. Customers are responsible for configuring AWS account and session controls to meet PCI requirements. Customers must be aware of AWS guidelines for credentials and access control for AWS resource management.
### Requirement 8: Assign a unique ID to each person with computer access.

- **All In-Scope Services:**
  - AWS provides each user in the AWS Management Environment a unique ID.
  - AWS provides additional security options that enable AWS customers to further protect their AWS Account and control access: AWS Identity and Access Management (AWS IAM), Multi-Factor Authentication (MFA) and Key Rotation.

- **Amazon EC2 and Amazon ECS:** AWS customers are responsible for access control within all OS instances.
- **All In-Scope Services:** AWS customers are responsible for configurable access controls within the services, such as database users within Amazon RDS.
- **AWS IAM & AWS Credentials:** AWS customers are responsible for managing access to all AWS services that are included in their CDE. AWS IAM can be used to manage resource management and AWS configuration roles and permissions. Customers are responsible for configuring AWS account and session controls to meet requirements. Customers must be aware of AWS guidelines for credentials and access control for AWS resource management.

### Requirement 9: Restrict physical access to cardholder data.

- **All In-Scope Services:**
  - AWS maintains the physical security and media handling controls for the services included in the assessment.

- **All In-Scope Services:** Any media created outside of the AWS environment is the sole responsibility of the customer.

### Requirement 10: Track and monitor all access to network resources and cardholder data.

- **All In-Scope Services:**
  - AWS maintains and monitors audit logs for the AWS Management Environment and AWS service infrastructure.

- **Amazon EC2 and Amazon ECS:** AWS customers are responsible for logging within all OS instances.
- **AWS IAM & AWS Console:** User activity logs of resource management activities via the console and command line are available to users via Amazon AWS CloudTrail. Amazon AWS CloudTrail must be used to record and monitor AWS resource management activities.
- **Amazon S3:** Users are responsible for configuring bucket logging and monitoring logs.
- **Amazon RDS & Amazon Redshift:** Users are responsible for configuring database access logging and monitoring logs.
- **Amazon EMR:** Customers using Amazon EMR to store cardholder data are responsible for logging access.
| Requirement 11: Regularly test security systems and processes. | All In-Scope Services: AWS manages rogue wireless access point detection, vulnerability and penetration testing, intrusion detection and file integrity monitoring for the AWS Management Environment and the identified services. | Amazon EC2 and Amazon ECS: AWS customers are responsible for internal and external scanning and pen testing of their instances and virtual networks. Customers must follow AWS processes for scanning and pen testing: http://aws.amazon.com/security/penetration-testing/. | Amazon SimpleDB & Amazon DynamoDB: Customers using these databases are responsible for access logging. | AWS Config: Customers using AWS Config to store configuration data and resource inventory are responsible for access logging and monitoring logs. | AWS WAF: Customers using AWS WAF to protect public facing applications including application databases that store cardholder data are responsible for logging access and monitoring. | All In-Scope Services: AWS customers are responsible for configuration of logging within the services. AWS CloudTrail can be used to log all AWS API calls. | Customers are responsible for monitoring logs for security events. Log monitoring may be implemented with CloudWatch or 3rd party services. | AWS customers are responsible for implementing IDS functionality, typically using Host-based IDS (HIDS) on network segments they implement and manage. |
### Requirement 12: Maintain a policy that addresses information security for employees and contractors.

- **All In-Scope Services:** AWS maintains security policies and procedures, security awareness training, security incident response plan, and human resource processes that align with PCI requirements.

- **All In-Scope Services:** AWS customers are responsible for all policies and procedures. AWS customers should include AWS as an infrastructure provider for Req. 12.8. Alerts from AWS should be part of the IRP for Req. 12.10.

### Requirement A: Shared hosting providers must protect the cardholder data environment.

- **All In-Scope Services:** AWS customer instances and data are protected by instance isolation and other security measures in the AWS Management Environment.

- **All In-Scope Services:** AWS customers may also be considered a shared hosting provider, if they run applications or store data for their customers. In this case, customers are responsible for protecting their customers’ data within AWS services.

### Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS

- **All In-Scope Services:** AWS encrypts access and manages transmission encryption within the AWS Management Environment using TLS 1.1 or greater.

- **All In-Scope Services:** AWS customers are responsible for using TLS 1.1 or greater or work towards upgrading to TLS 1.1 or greater by June 30, 2018. If TLS 1.0 or SSLv3 are in place in the cardholder data environment, AWS customers are responsible for developing a formal Risk Mitigation and Migration Plan for migrating to TLS 1.1 or greater by the June 30th, 2018 deadline.
# APPENDIX C. CITATIONS

The following table summarizes all links referenced throughout this technical workbook.

<table>
<thead>
<tr>
<th>Section</th>
<th>Resource</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3</td>
<td>PCI DSS version 3.1</td>
<td><a href="https://www.pcisecuritystandards.org/security_standards/documents.php">https://www.pcisecuritystandards.org/security_standards/documents.php</a></td>
</tr>
<tr>
<td>1.2.3</td>
<td>Manage AWS Environments</td>
<td><a href="http://aws.amazon.com/getting-started/">http://aws.amazon.com/getting-started/</a></td>
</tr>
<tr>
<td>2</td>
<td>AWS PCI Level 1 FAQ</td>
<td><a href="http://aws.amazon.com/compliance/pci-dss-level-1-faqs">http://aws.amazon.com/compliance/pci-dss-level-1-faqs</a></td>
</tr>
<tr>
<td>2.3.1</td>
<td>Request copy of AWS AOC</td>
<td><a href="http://aws.amazon.com/compliance/contact/">http://aws.amazon.com/compliance/contact/</a></td>
</tr>
<tr>
<td>3.3</td>
<td>Amazon S3 Server Side Encryption</td>
<td><a href="http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html">http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html</a></td>
</tr>
<tr>
<td>3.3</td>
<td>Amazon S3 Upload Objects</td>
<td><a href="http://docs.aws.amazon.com/AmazonS3/latest/UG/UploadingObjectsintoAmazonS3.html">http://docs.aws.amazon.com/AmazonS3/latest/UG/UploadingObjectsintoAmazonS3.html</a></td>
</tr>
<tr>
<td>3.3</td>
<td>AWS KMS Cryptographic Details</td>
<td><a href="https://d0.aws%E9%9D%99%E6%80%81.com/whitepapers/KMS-Cryptographic-Details.pdf">https://d0.aws静态.com/whitepapers/KMS-Cryptographic-Details.pdf</a></td>
</tr>
<tr>
<td>3.3</td>
<td>AWS KMS API Key Rotation</td>
<td><a href="http://docs.aws.amazon.com/kms/latest/APIReference/API_EnableKeyRotation.html">http://docs.aws.amazon.com/kms/latest/APIReference/API_EnableKeyRotation.html</a></td>
</tr>
<tr>
<td>3.4</td>
<td>VPC FAQ</td>
<td><a href="http://aws.amazon.com/vpc/faqs/">http://aws.amazon.com/vpc/faqs/</a></td>
</tr>
<tr>
<td>3.6</td>
<td>AWS Linux Security Center</td>
<td><a href="https://alas.aws.amazon.com/">https://alas.aws.amazon.com/</a></td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>URL</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.8</td>
<td>Directory Service – Create a Directory</td>
<td><a href="http://docs.aws.amazon.com/directoryservice/latest/adminguide/create_directory.html">http://docs.aws.amazon.com/directoryservice/latest/adminguide/create_directory.html</a></td>
</tr>
<tr>
<td>3.10</td>
<td>Amazon S3 Lifecycle Configuration</td>
<td><a href="http://docs.aws.amazon.com/AmazonS3/latest/UG/LifecycleConfiguration.html">http://docs.aws.amazon.com/AmazonS3/latest/UG/LifecycleConfiguration.html</a></td>
</tr>
<tr>
<td>3.11</td>
<td>AWS Penetration Testing Information</td>
<td><a href="http://aws.amazon.com/security/penetration-testing">http://aws.amazon.com/security/penetration-testing</a></td>
</tr>
<tr>
<td>5.1</td>
<td>AWS Technical Support</td>
<td><a href="https://aws.amazon.com/premiumsupport/">https://aws.amazon.com/premiumsupport/</a></td>
</tr>
<tr>
<td>5.1</td>
<td>Anitian Website</td>
<td><a href="http://www.anitian.com">www.anitian.com</a></td>
</tr>
</tbody>
</table>