# AWS Security Incident Response Guide AWS Technical Guide

This version has been archived.

For the latest version of this document, visit:



#### **AWS Security Incident Response Guide: AWS Technical Guide**

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.



For the latest version of this document, visit:

#### **Table of Contents**

1
2
2
2
3
4
4
$\epsilon$
6
6
-
-
8
ç
ç
1
1
12
12
12
3
3
14
16
16
7
7
7
17
8
18
8
8
9
13
9
2(
20
1
2
22
22
22
22
2
2 [
26
26
26
27
27
)

#### AWS Security Incident Response Guide AWS Technical Guide

Event-Driven Response	31
Incident Response Examples	33
Service Domain Incidents	33
Identities	33
Resources	33
Infrastructure Domain Incidents	34
Investigation Decisions	35
Capturing Volatile Data	35
Using AWS Systems Manager	36
Automating the Capture	36
Conclusion	37
Additional Resources	38
Media	38
Third-Party Tools	38
Industry References	39
Document Revisions	40
Appendix A: Cloud Capability Definitions	41
Logging and Events	41
Visibility and Alerting	42
Automation	43
Secure Storage	44
Custom	44
Appendix B: Sample Code	45
Example AWS CloudTrail Event	45
Example AWS CloudWatch Event	45
Example Infrastructure Domain CLI Activities	
Appendix C: Example Runbook	
Incident Response Runbook – Root Usage	48
Objective	48
Assumptions	48
Indicators of Compromise	48
Steps to Remediate – Establish Control	49
Further Action Items - Determine Impact	49
Notices	E (

#### This version has been archived.

For the latest version of this document, visit:

# AWS Security Incident Response Guide

Publication date: November 23, 2020 (Document Revisions (p. 40))

This guide presents an overview of the fundamentals of responding to security incidents within a customer's AWS Cloud environment. It focuses on an overview of cloud security and incident response concepts, and identifies cloud capabilities, services, and mechanisms that are available to customers who are responding to security issues.

This paper is intended for those in technical roles and assumes that you are familiar with the general principles of information security, have a basic understanding of incident response in your current onpremises environments, and have some familiarity with cloud services.

This version has been archived.

For the latest version of this document, visit:

# Introduction

Security is the highest priority at AWS. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations. The AWS Cloud has a *shared responsibility model*. AWS manages security *of* the cloud. You are responsible for security *in* the cloud. This means that you retain control of the security you choose to implement. You have access to hundreds of tools and services to help you meet your security objectives. These capabilities help you establish a security baseline that meets your objectives for your applications running in the cloud.

When a deviation from your baseline does occur (such as by a misconfiguration), you may need to respond and investigate. To successfully do so, you must understand the basic concepts of security incident response within your AWS environment, as well as the issues you need to consider to prepare, educate, and train your cloud teams before security issues occur. It is important to know which controls and capabilities you can use, to review topical examples for resolving potential concerns, and to identify remediation methods that you can use to leverage automation and improve your response speed.

Because security incident response can be a complex topic, we encourage you to start small, develop runbooks, leverage basic capabilities, and create an initial library of incident response mechanisms to iterate from and improve upon. This initial work should include your legal department as well as teams that are not involved with security, so that you are better able to understand the impact that incident response (IR), and the choices you have made, have on your corporate goals.

#### **Topics**

- Before You Begin (p. 2)
- AWS CAF Security Perspective (p. 2)
- Foundation of Incident Response (p. 3)

#### Before You Begin

In addition to this denisal version gaps theen tarted iverses for Security, Identity, & Compliance and the Security Perspective of the AWS Cloud Adoption Framework (CAF) whitepaper. The AWS CAF provides guidance that supports coordinating between the different parts of organizations that are moving to the cloud. The CAF guidance is divided into several areas of focus that are relevant to implementing cloud-based IT systems, which we refer to as perspectives. The Security Perspective describes for refine the security properties on incident response. This document details some of our experiences in helping customers to assess and implement successful mechanisms in that workstream.

#### AWS CAntipse (dutistay Ranapactin Avhitepapers/latest/

aws-security-incident-response-guide/
The Security Perspective includes four components:
welcome.html

- **Directive controls** establish the governance, risk, and compliance models within which the environment operates.
- Preventive controls protect your workloads and mitigate threats and vulnerabilities.
- **Detective controls** provide full visibility and transparency over the operation of your deployments in
- Responsive controls drive remediation of potential deviations from your security baselines.

Although IR is generally viewed under the responsive controls component, these are dependent and influenced by the other components. For example, directive and preventative security controls help establish a baseline, so you can monitor and investigate any deviations from this baseline. This approach not only eliminates noise, but it also contributes to a defensive security design.

#### Foundation of Incident Response

All AWS users within an organization should have a basic understanding of security incident response processes, and security staff must deeply understand how to react to security issues. Experience and education are vital to a cloud incident response program, before you handle a security event. The foundation of a successful incident response program in the cloud is to *Educate*, *Prepare*, *Simulate*, and *Iterate*.

To understand each of these aspects, consider the following descriptions:

- **Educate** your security operations and incident response staff about cloud technologies and how your organization intends to use them.
- Prepare your incident response team to detect and respond to incidents in the cloud by enabling
  detective capabilities, and ensuring appropriate access to the necessary tools and cloud services.
  Additionally, prepare the necessary runbooks, both manual and automated, to ensure reliable and
  consistent responses. Work with other teams to establish expected baseline operations, and use that
  knowledge to identify deviations from those normal operations.
- **Simulate** both expected and unexpected security events within your cloud environment to understand the effectiveness of your preparation.
- **Iterate** on the outcome of your simulation to improve the scale of your response posture, reduce time to value, and further reduce risk.

This version has been archived.

For the latest version of this document, visit:

#### Educate

#### **Topics**

- Shared Responsibility (p. 4)
- Incident Response in the Cloud (p. 6)
- Cloud Security Incidents (p. 6)
- Understanding Cloud Capabilities (p. 8)

#### **Shared Responsibility**

The responsibility for security and compliance is shared between AWS and you. This shared model relieves some of your operational burden because AWS operates, manages, and controls the components from the host operating system and virtualization layer, down to the physical security of the facilities in which the service operates.

You are responsible for managing the guest operating systems (including updates and security patches) and application software, as well as configuring the AWS provided security controls, such as security groups, network access control lists, and identity and access management. You should carefully consider which services you use, because your responsibilities vary depending on the services you choose, the integration of those services in your IT environment, and applicable laws and regulations. Figure 2 (p. 5) shows a typical representation of the shared responsibility model as it applies to infrastructure services, such as Amazon Elastic Compute Cloud (Amazon EC2). It separates most responsibilities into two categories: security of the cloud (managed by AWS) and security in the cloud (managed by the customer). Responsibilities can change, depending on which services you use. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and apply the appropriate permissions.

However, the shared responsibility model changes with the addition of containers and other services that movering prelations model, the service profider is we may to the left of the poperating model, away from laas and data centers and towards Paas, the responsibility of the service provider increases. A customer has fewer responsibilities in the cloud and an easier time operating when migrating to the left of the graph. Note the following figures and the differences in the ability to operate or function in the cloud. As your shared responsibility in the cloud changes, your options for incident response or forensics change also. As the customer, while you plan your incident response, you'll also need to make sure that you plantage in the additional the possible interactions before they accurring model that you have chosen. Planning for and understanding these tradeoffs and matching them with your governance needs is a crucial step in incident response.

Welcome.html

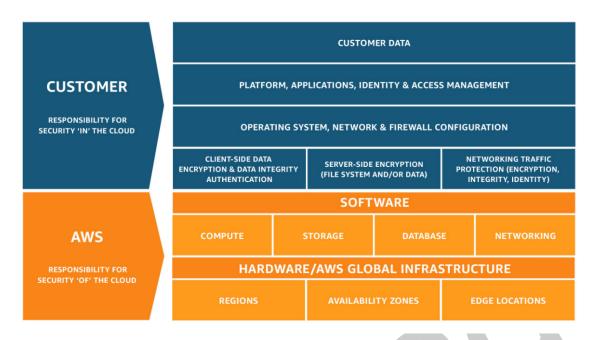
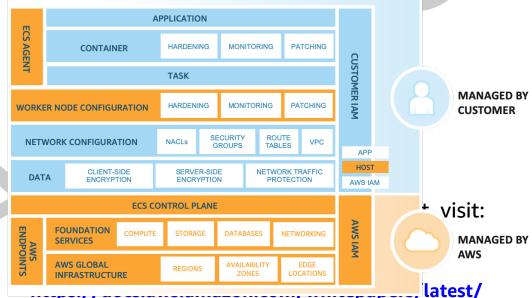


Figure 1: Shared Responsibility Model

# AWS ECS with Fargate Shared Responsibility Model



#### aws-security-incident-response-guide/ welcome.html

Figure 2: Amazon Elastic Container Service (Amazon ECS) with AWS Fargate Type Shared Responsibility Model

In addition to the direct relationship you have with AWS, there may be other entities that have responsibilities in your particular responsibility model. For example, you may have internal organizational units that take responsibility for some aspects of your operations. You may also have partners or other third parties that develop, manage, or operate some of your cloud technology.

Creating an appropriate incident response and forensics runbook that matches your operating model is extremely important. Your success hinges on your understanding of the types of tools that you need to create, or the tools you need to purchase, for the operating model that you have selected. The better your organization understands the tools available, the better prepared you will be to meet the needs of your enterprise's governance risk and compliance (GRC) model.

#### Incident Response in the Cloud

#### **Design Goals of Cloud Response**

Although the general processes and mechanisms of incident response, such as those defined in the NIST SP 800-61 Computer Security Incident Handling Guide, remain true, we encourage you to consider these specific design goals that are relevant to responding to security incidents in a cloud environment:

- Establish response objectives Work with your stakeholders, legal counsel, and organizational leadership to determine the goal of responding to an incident. Some common goals include containing and mitigating the issue, recovering the affected resources, preserving data for forensics, and attribution.
- Respond using the cloud Implement your response patterns where the event and data occurs.
- Know what you have and what you need Preserve logs, snapshots, and other evidence by copying them to a centralized security cloud account. Use tags, metadata, and mechanisms that enforce retention policies. For example, you may choose to use Linux dd command or a Windows equivalent to make a complete copy of data for investigative purposes.
- Use redeployment mechanisms If a security anomaly can be attributed to a misconfiguration, the remediation might be as simple as removing the variance by redeploying the resources with the proper configuration. When possible, make your response mechanisms safe to execute more than once and on unknown states.
- Automate where possible As you see issues or incidents repeat, build mechanisms that
  programmatically triage and respond to common situations. Use human responses for unique, new,
  and sensitive incidents.
- Choose scalable splutions, String to mutch the scalability of your organization's approach to cloud computing, and reduce the time between detection and response.
- Learn and improve your process When you identify gaps in your process, tools, or people, plan to fix them. Simulations are safe methods to find gaps and improve processes.

NIST design goals remind you to review architecture for the ability to conduct both incident response and threat detection. As you plan your cloud implementation, think about responding to an incident or a forensics event. In some cases, this means you may have multiple organizations, accounts, and tools specifically set up for these response tasks. These tools and functions should be made available to the incident responder by deployment pipeline and should not be static, as this would cause a larger risk. <a href="https://docs.aws.amazon.com/whitepapers/latest/">https://docs.aws.amazon.com/whitepapers/latest/</a>

aws-security-incident-response-guide/Cloud Security Incidentcome.html

#### **Topics**

- Incident Domains (p. 7)
- Indicators of Cloud Security Events (p. 7)

#### **Incident Domains**

There are three domains within the customer's responsibility where security incidents might occur: service, infrastructure, and application. The difference between the domains is related to the tools you use when you respond. Consider these domains:

- Service Domain Incidents in the service domain affect a customer's AWS account, IAM permissions, resource metadata, billing, and other areas. A service domain event is one that you respond to exclusively with AWS API mechanisms, or where you have root causes associated with your configuration or resource permissions, and might have related service-oriented logging.
- Infrastructure Domain Incidents in the infrastructure domain include data or network-related activity, such as the traffic to your Amazon EC2 instances within the VPC, processes and data on your Amazon EC2 instances, and other areas, like containers or other future services. Your response to infrastructure domain events often involves retrieval, restoration, or acquisition of incident-related data for forensics. It likely includes interaction with the operating system of an instance, and in some cases, might also involve AWS API mechanisms.
- Application Domain Incidents in the application domain occur in the application code or in software deployed to the services or infrastructure. This domain should be included in your cloud threat detection and response runbooks, and might incorporate similar responses to those in the infrastructure domain. With appropriate and thoughtful application architecture, you can manage this domain with cloud tools, using automated forensics, recovery, and deployment.

In these domains, you must consider the actors who might act against your account, resources, or data. Whether internal or external, use a risk framework to determine what the specific risks are to your organization and prepare accordingly.

In the service domain, you work to achieve your goals exclusively with AWS APIs. For example, handling a data disclosure incident from an Amazon S3 bucket involves API calls to retrieve the bucket's policy, analyzing the S3 access logs, and possibly looking at AWS CloudTrail logs. In this example, your investigation is unlikely to involve data forensic tools or network traffic analysis tools.

In the infrastructure domain, you can use a combination of AWS APIs and familiar digital forensics/incident response (DFIR) software within the operating system of a workstation, such as an Amazon EC2 instance that you've prepared for IR work. Infrastructure domain incidents might involve analyzing network packet captures, disk blocks on an Amazon Elastic Block Store (Amazon EBS) volume, or volatile memory acquired from an instance.

# Indicators of Cloud Security Events For the latest version of this document, visit:

There are many security events that you might not classify as incidents, but it might still be prudent to investigate them. To detect security-related events in your AWS Cloud environment, you can use these mechanisms. Though not an exhaustive list, consider the following examples of some potential indicators:

- https://docs.aws.amazon.com/whitepapers/latest/
  Logs and Monitors Review AWS logs (such as Amazon Cloud rail, Amazon S3 access logs, and VPC Flow Logs) and Wesnite ability in the literature gitch as pointed, mazon Detective, AWS Security Hub, and Amazon Maciel, haddition use monitors like Amazon Route 53 health checks and Amazon CloudWatch alarms. Similarly, use Windows Events, Linux syslog logs, and other application-specific logs that you can generate in your applications, and log to Amazon CloudWatch, using CloudWatch agents.
- Billing Activity A sudden change in billing activity can indicate a security event.
- Threat Intelligence If you subscribe to a third-party threat intelligence feed, you can correlate that information with other logging and monitoring tools to identify potential indicators of events.

#### AWS Security Incident Response Guide AWS Technical Guide Understanding Cloud Capabilities

- Partner Tools Partners in the AWS Partner Network (APN) offer hundreds of industry-leading
  products that can help you meet your security objectives. For more information, see Security Partner
  Solutions and Security Solutions in the AWS Marketplace.
- AWS Outreach AWS Support might contact you if we identify abusive or malicious activity. For more information, see the AWS Response to Abuse and Compromise (p. 9) section.
- One-Time Contact Because it can be your customers, your developers, or other staff in your organization who notice something unusual, it is important to have a well-known, well-publicized method of contacting your security team. Popular choices include ticketing systems, contact email addresses, and web forms. If your organization works with the general public, you may also need a public-facing security contact mechanism.

One of the tools that AWS offers for automation and detection is AWS Security Hub. Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts in one place, enabling better visibility to these indicators. AWS Security Hub is not Security Information and Event Management (SIEM) software and does not store log data, but instead aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services. Security Hub also gives you the ability to create custom insights that can stem from multiple sources. This gives the Security Operations team options and insight into more information when an event occurs. Security Hub continuously monitors your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows.

You can also take action on these security and compliance findings by investigating them in Amazon Detective or Amazon Athena, or by using Amazon CloudWatch Events or Event Bus rules to send the findings to ticketing, chat, SIEM, Security Orchestration Automation and Response (SOAR), and incident management tools or to custom remediation playbooks. Event-based automation allows you to automatically respond to incidents or events that occur. This approach changes security and the way you handle events in the cloud when compared to on-premises environments.

#### **Understanding Cloud Capabilities**

AWS offers a wide range of security capabilities that you can use to investigate security events across the domains. For example, AWS provides a number of logging mechanisms, such as AWS CloudTrail logs, Amazon CloudWatch This Metal Gardan Sgrade Hoal Gardan Sgrade Consider the services that you're using, and make sure you have enabled the logs that pertain to those services. AWS also offers a Centralized Logging Solution, which can help you to understand how to centralize and store the common types of cloud logs. After you have enabled these logging sources, you must decide how you want to analyze them, such as by using Amazon Athena to query logs held in your Amazon S3 buckets. For the latest version of this document, visit:

Additionally, there are a number of APN Partner products that can simplify your process when analyzing these logs, such as those described in the APN Security Competency program. There are also several AWS services that can help you get valuable insights into this data, such as Amazon GuardDuty (a threat detection service) and AWS Security Hub, which can give you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts Additionally Amazon Detective collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to help you identify the adviscus of bightial scountification of the properties of the production of the prod

#### Topics

- Data Privacy (p. 9)
- AWS Response to Abuse and Compromise (p. 9)

#### **Data Privacy**

We know customers care deeply about privacy and data security, and so we implement responsible and sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of customer content. Maintaining customer trust is an ongoing commitment. You can learn more about AWS data privacy commitments on our Data Privacy FAQ page.

These intentional, self-imposed controls limit the ability of AWS to assist in responding within a customer's environment. Because of this, focusing on understanding and building capabilities within the Shared Responsibility Model is key to success in the AWS Cloud. Although enabling logging and monitoring capabilities in your AWS accounts before an incident occurs is important, there are additional aspects to incident response that are imperative to a successful program.

#### California Consumer Data Privacy

The California Consumer Privacy Act of 2018 (CCPA) grants "consumer[s] various rights with regard to personal information relating to the consumer that is held by a business" that is subject to the CCPA. For information on AWS privacy and data security policies in relation to customers subject to CCPA, refer to the Preparing for the California Consumer Privacy Act whitepaper for guidance.

#### **General Data Protection Regulation**

The General Data Protection Regulation (GDPR) is a European privacy law (Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016) that became enforceable on May 25, 2018. The GDPR replaces the EU Data Protection Directive (Directive 95/46/EC), and is intended to harmonize data protection laws throughout the European Union (EU) by applying a single data protection law that is binding throughout each EU member state. For information on AWS compliance in relation GDPR, refer to the Navigating GDPR Guidance on AWS whitepaper.

#### **AWS Response to Abuse and Compromise**

Abuse activities are observed behaviors of AWS customers' instances or other resources that are malicious, offensive, illegal, or could harm other internet sites. AWS works with you to detect and address suspicious arthralicious civities from your resources can indicate that your AWS resources have been compromised, which signals potential risks to your business. Remember that you have alternate methods of contact in your AWS account. Be sure to use best practices when adding contacts, both for security and billing. Although your root account email is the primary target of communication from AWS, AWS also communicates security issues and billing is ues to the secondary email addresses. Adding an email address that goes to only one person, means that you have added a single point of failure to your AWS account. Make sure that you've added at least one distribution list to your contacts.

AWS detects abuse activities in your resources using mechanisms, such as:

- · <sup>AW</sup>ክittមួច:///የ៨៦៤១:ដូសម្មែងamazon.com/whitepapers/latest/
- External security intelligence against AW network address space guide/
- Internet abuse complaints against AWS resources.
   Welcome.html

Although the AWS abuse response team aggressively monitors and shuts down unauthorized activity running on AWS, the majority of abuse complaints refer to customers who have legitimate business on AWS. Some examples of common causes of unintentional abuse activities include:

 Compromised resource – An unpatched Amazon EC2 instance could be infected and become a botnet agent.

#### AWS Security Incident Response Guide AWS Technical Guide AWS Response to Abuse and Compromise

- Unintentional abuse An overly aggressive web crawler might be classified as a denial-of-service attack by some internet sites.
- Secondary abuse An end user of the service provided by an AWS customer might post malware files on a public Amazon S3 bucket.
- False complaints Sometimes internet users mistakenly report legitimate activities as abuse.

AWS is committed to working with AWS customers to prevent, detect, and mitigate abuse, and to defend against future recurrences. We encourage you to review the AWS Acceptable Use Policy, which describes prohibited uses of the web services offered by Amazon Web Services and its affiliates. To support a timely response to abuse notifications from AWS, make sure that your AWS account contact information is accurate. When you receive an AWS abuse warning, your security and operational staff should immediately investigate the matter. A delay can prolong the reputation impact and legal implications to yourself and others. More importantly, the implicated abuse resource might be compromised by malicious users, and ignoring the compromise could magnify damages to your business.

#### This version has been archived.

For the latest version of this document, visit:

# Prepare – People

Automated processes enable organizations to spend more time focusing on measures to increase the security of their cloud environment and applications. Automated incident response also makes humans available to correlate events, practice simulations, devise new response procedures, perform research, develop new skills, and test or build new tools. Despite increased automation, analysts and responders within a security organization still have much to do. Homogeneous teams can create blind spots, so it is essential to build a diverse team that offers different systems of thought, cultural perspectives, and work and life experience in complex fluid situations. One of the most impactful things that we can do as we plan for events, is to make sure that we have diversity built into our teams and response plans. A team comprising of diverse perspectives can potentially identify blind spots that may not have been caught and identify solutions that may not have otherwise been thought of.

#### **Topics**

- Define Roles and Responsibilities (p. 11)
- Define Response Mechanisms (p. 12)
- Create a Receptive and Adaptive Security Culture (p. 12)
- Predicting Response (p. 13)

#### Define Roles and Responsibilities

The skills and mechanisms of incident response are most important when handling new or large-scale events. These events rely on the written standards your team has developed and the practice that your team has had. Because we cannot predict or codify all potential directions an event will take, we rely on automation for simple, repetitive tasks, such as collecting instance memory or diagnostic logs, and let humans make hard decisions. Handling unclear security events requires cross-organizational discipline, bias for druging action and the hability is deliver results. Within your organizational structure, there should be many people who are responsible, accountable, consulted, or kept informed during an incident, such as representatives from human resources (HR), your executive team, and legal. Consider these roles and responsibilities, and whether any third parties must be involved. Note that in many geographies, there are local laws that govern what can and cannot be done. Although it may seem bureaucratic to build a responsible accountable, consulted, and informed (RACI) chart for an incident, doing so enables quick and direct communication and clearly outlines the leadership across different stages of the event.

Trusted partners may be involved in the investigation or response and they provide additional expertise and valuable scrutiny. When you do not have these skills on your own team, you may want to hire an external parties work with your internal developers and operators, they can extend the skills of your team members and that new expertise carbor valuable to your IR program in the future.

Welcome.html

During an incident, including the owners and developers of impacted applications and resources is key because they are subject matter experts (SMEs) that can provide information and context. Make sure to practice with and build relationships with the developers and application owners prior to relying upon their expertise for incident response. Application owners or SMEs may be required to act in situations where the environment is unfamiliar, has unanticipated complexity, or where the responders do not have access. Application SMEs should practice and become comfortable working with the IR team.

#### **Provide Training**

To reduce dependencies and decrease response time, make sure that your security teams and responders are educated about cloud services and have opportunities for hands-on practice with the specific cloud platforms that your organization uses. Some of this training comes from the team building and runbook creation that occurs at the beginning of the process. By including as many people as possible in the initial step of forming runbooks, you provide better understanding to your internal teams. This training becomes more real as these teams begin to follow these runbooks in tabletop exercises.

AWS and other third parties also provide online security workshops (AWS Security Workshops) that you can download and work through. Your organization can benefit by providing additional training to your staff to learn programming skills, development processes (including version control systems and deployment practices), and infrastructure automation.

AWS provides a number of training options and learning paths through digital training, classroom training, APN partners, and certifications. To learn more, see AWS Training & Certification.

#### **Define Response Mechanisms**

Your response mechanism depends on your governance, risk, and compliance (GRC) model. Ideally, your GRC model is built before you plan for incident response. If you have not started building a GRC, it is a necessary first step to building out a good incident response mechanism. When you consider your approach to incident response in the cloud, in unison with other teams (such as your legal counsel, leadership, business stakeholders, and others), you must understand what you have and what you need. Identify stakeholders and relevant contacts, and make sure you have appropriate access to perform the necessary response.

Although the cloud can provide you with greater visibility and capabilities through service APIs, your GRC model shows you how to use these in your response. Identify your team's AWS account numbers, the IP ranges of your Virtual Private Clouds (VPCs), corresponding network diagrams, logs, data locations, and data classifications. Many of these technological processes are included in the Prepare – Technology (p. 16) section. Then, begin documenting your incident response procedures, often referred to as procedures or runbooks, that define the steps to investigate and remediate an incident.

# This version has been archived. Create a Receptive and Adaptive Security Culture

At AWS, we have learned that our customers' and our own internal teams are most successful when security teams are learned that our customers' and our own internal teams are most successful when security teams are learned that makes sure all stakeholders cooperate and escalate to maintain an agile, highly responsive security posture. Although improving your organization's security culture is not the subject of this paper, you can get relevant intelligence from your non-security staff if they see the security team is receptive. When your security team is open and accessible, with support from leadership, they are more likely to get additional, timely notifications, cooperation, and responses to security events.

https://docs.aws.amazon.com/whitepapers/latest/

In some organizations, staff may fear retribution if they report a security problem. Sometimes they simply don't know how to report an issue. In other cases, they may not want to waste time, or may be embarrassed to report something awasecurity iecitlent that is later discovered to not be a problem. From the leadership team down, it is important to promote a culture of acceptance and to invite everyone to be a part of the organization's security. Provide a clear channel for anyone to open a high-severity ticket, whenever they believe there could be a potential risk or threat. Welcome these notifications with an eager and open mind, but more importantly, make it clear to non-security staff that you welcome these notifications. Emphasize that you would rather be over-notified of potential issues, than to receive no notifications at all. It is far better for a developer to call out his or her own mistake, then for a researcher to point out the issue in a public article.

#### AWS Security Incident Response Guide AWS Technical Guide Predicting Response

These notifications offer valuable opportunities to practice responsive investigations under stress. They can serve as an important feedback loop while you develop your response procedures.

#### **Predicting Response**

Because it is impossible to predict all potential events, you must continue to rely on human analysis. Taking the time to carefully train your staff and prepare your organization helps you to anticipate the unexpected; however, your organization does not have to prepare in isolation. Collaborating with trusted security partners to identify unexpected security events gives organizations the benefit of additional visibility and insight.

#### Partners and the Window of Response

The journey to the cloud is unique for every organization. However, there are patterns and practices that other organizations have already encountered that a trusted security partner can bring to your attention. We encourage you to identify external AWS security APN Partners that can provide you with outside expertise and a different perspective to augment your response capabilities. Your trusted security partners can help you identify potential risks or threats that you might not be familiar with.

In 1955, Joseph Luft and Harrington Ingham created the Johari window, an exercise for mapping traits to categories. The window is depicted as a grid that consists of four quadrants, similar to the following diagram.

	Known to You	Not Known to You
Known to Others	Obvious	Blind Spot
Not Known to Others	Internally Known	Unknown

Figure 3: Johari Window modified for incident response <a href="https://docs.aws.amazon.com/whitepapers/latest/">https://docs.aws.amazon.com/whitepapers/latest/</a>

Although the Johani window was not intended for information security; we can adjust the concept to use it as a simple mental model to consider the difficulty in assessing an organization's threats. In our modified concept, the four quadranty accome. html

- Obvious Risk of which both your team and your APN Partner are aware.
- Internally Known Risk that your team is familiar with, but that your APN Partner isn't. This could mean that you have internal expertise or tribal knowledge.
- Blind Spot Risk that your APN Partner is familiar with, but that your team is not.
- **Unknown** Risk which neither you or your APN Partner are familiar with.

#### **AWS Security Incident Response** Guide AWS Technical Guide Unknown Risk

Although this diagram is simple, it represents the value that having trusted APN Partners can achieve. Most critically, there might be blind spot items that you are unaware of, but an APN Partner with the right expertise can bring to your attention. Although you might both be familiar with those risks in the obvious quadrant, your APN Partner could recommend controls and solutions that you are unfamiliar with. Additionally, although you might bring those risks in the internally known quadrant to your APN Partner's attention, your APN Partner might also be able to identify optimized controls for mitigating that risk. As you measure yourself for improvement, contact your APN Partner to provide expert advice.

#### **Unknown Risk**

If you've been focused on tailoring alerts, improving your incident response procedures with automation, and improving your security defenses, you might be wondering what to improve next. You might be curious about your unknown risk, as represented in the unknown category in Figure 3. You can reduce unknown risk through the following methods:

- **Define security assertions** What are some truths that you can assert? What are the security primitives that should absolutely be true in your environment? Clearly defining these allows you to search for the inverse. This is something that's easier to do early in your cloud journey, rather than by attempting to reverse engineer your security assertions later.
- Education, communication, and research Create cloud security experts on your staff or include expert partners to help scrutinize your environment. Challenge your assumptions, and be wary of subtle reasoning. Create feedback loops in your processes and offer mechanisms for your engineering teams to communicate with security teams. You can also expand your approach to monitor relevant security mailing lists and information security disclosures.
- Reducing attack surface Improve your defense to avoid risk and give yourself more time against unknown attacks. Block and slow down attackers, and force them to be noisy.
- Threat intelligence Subscribe to a continuous feed of current and relevant threats, risk, and indicators from around the world.
- Alerts Generate notifications that alert you to unusual, malicious, or expensive activities. For example, you might create a notification for activities that occur in Regions or services that you do not
- Machine learning Use machine learning to identify complex anomalies for a specific organization or individual personas. To help you identify unusual behaviors, you can also profile the normal characteristics of your networks, users, and systems. This version has been archived.

Threat intelligence becomes the primary topic as you consider blind spots and unknown unknowns. The Johari window shows how to categorize what you know and do not know, but threat intelligence shows how to account for what you don't yet know. Threat intelligence is a discipline that helps companies to see around the configs of the stream engine in front the pist the pour paranty naistit yet know exist.

Generally, threat intelligence comprises:

- 1. Finding new threats.

- Defining new patterns. https://docs.aws.amazon.com/whitepapers/latest/
   Defining new automated acquisitions techniques.
   Repeating these processes. welcome.html

Although this type of practice can be helpful, the care and maintenance of a threat intelligence team can over burden many enterprises, even large enterprises. In the end, the question becomes one of matching your threat model, size, and risk adversity. Consider these questions:

- Is your threat model significantly different enough from the standard vertical the enterprise is in?
- Is your risk appetite low enough that such a team is required?

#### AWS Security Incident Response Guide AWS Technical Guide Unknown Risk

- Is it fiscally sound to run a team for your enterprise?
- Is your risk profile interesting enough to attract reasonable talent to your cause?

If you respond to any of these questions with *no*, you should most likely find a threat intelligence partner. This service is offered competitively by many large and well-known companies.

AWS provides you with the tools and services to manage these issues yourself. Using machine learning to identify malicious patterns is a well-researched field of study, with patterns that are implemented by customers, AWS Professional Services, APN Partners, and through AWS services such as Amazon GuardDuty and Amazon Macie. Some of these patterns have been discussed at AWS re:Invent conference sessions. For more information, see the Media (p. 38) section of this whitepaper.

Customers are also expanding their traditionally business-centric data lakes to leverage similar architecture patterns when they develop security data lakes. Security operations teams are also expanding their use of traditional logging and monitoring tools, such as Amazon OpenSearch Service and OpenSearch Dashboards, to big data architectures.

Those customers are collecting internal data from AWS CloudTrail event logs, VPC Flow Logs, Amazon CloudFront access logs, database logs, and application logs, and then combining this data with public data and threat intelligence. With this valuable data, customers have expanded to include data science and data engineering skills on their security operations teams to leverage tools such as Amazon EMR, Amazon Kinesis Data Analytics, Amazon Redshift, Amazon QuickSight, AWS Glue, Amazon SageMaker, and Apache MXNet on AWS to build custom solutions that identify and predict anomalies that are unique to their business.

Finally, see Security Partner Solutions for hundreds of industry-leading products from APN Partners that are equivalent, identical to, or integrated with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across the cloud and on premises.

This version has been archived.

For the latest version of this document, visit:

# Prepare – Technology

#### **Topics**

- Prepare Access to AWS Accounts (p. 16)
- Prepare Processes (p. 18)
- Cloud Provider Support (p. 22)

#### Prepare Access to AWS Accounts

During an incident, your incident response teams must have access to the environments and resources involved in the incident. Make sure that your teams have appropriate access to perform their duties before an event occurs. To do that, you must know what level of access your team members require (for example, what kinds of actions they are likely to take) and you must provision access in advance. This access is derived from your company's governance, risk management, and compliance (GRC) policies. Your team members' authentication and authorization should be documented and tested well before an event occurs to make sure they can perform a timely response without delays. To respond to an incident correctly, part of your preparation should be a review of how the AWS accounts are laid out and how the cross-account roles are allowed and organized.

At this stage, you must work closely with your developers, architects, partners, governance teams, and compliance teams to understand what level of access is necessary for responders. Identify and discuss the AWS account strategy and cloud identity strategy with your organization's cloud architects to understand what authentication and authorization methods are configured, for example:

- Federation A user assumes an IAM role in an AWS account from an Identity Provider.
- Cross-account access A user assumes an IAM role between multiple AWS accounts.
- Authentication A user authenticates as an AWS IAM user created within a single AWS account.

This version has been archived. These options define the technical choices for authentication to AWS, and how you can gain access during a response, but some organizations might rely on another team or a partner to assist in the response. User accounts that are created specifically to respond to a security incident are often privileged in order to provide sufficient access. Therefore, use of these user accounts should be restricted, and they should not be used for faily activities should not be used for faily activities.

Before you create new access mechanisms, work with your cloud teams to understand how your AWS accounts are organized and governed. Many customers use AWS Organizations to help centrally manage billing, share resources across their AWS accounts, and control access, compliance, and security. A core feature of Organizations is that it can be leveraged to apply Service Control Policies to groups of accounts solve the property of the following generalized response patterns to assist in identifying which expressing are right for your organization.

#### Topics

- Indirect Access (p. 17)
- Direct Access (p. 17)
- Alternative Access (p. 17)
- Automation Access (p. 17)

• Managed Services Access (p. 18)

#### **Indirect Access**

If you use *indirect access*, your account owners or application teams are required to perform authorized remediations in their AWS accounts with tactical guidance from the incident response team who are your security experts. This method is a slower and more complex way to execute tasks, but it can be successful when the responders are unfamiliar with the account or cloud environment.

#### **Direct Access**

To give incident responders *direct access*, deploy an AWS IAM role into the AWS accounts that your security engineers or incident responders can assume during a security event. The incident responder authenticates either through a normal federated process, or through a special emergency process, if the incident impacts your normal authentication process. The permissions you give the incident response IAM role depend on the actions you anticipate the responders to perform.

#### **Alternative Access**

If you believe a security event is impacting your security, identity, or communication systems, you might need to seek alternative mechanisms and access to investigate and remediate the impact. By using a new, purpose-built AWS account, your responders can collaborate and work from an alternate, secure infrastructure.

For example, responders can leverage new infrastructure launched in the cloud, such as remote workstations using Amazon WorkSpaces and email services provided by Amazon WorkMail. You must prepare appropriate access controls (using IAM policies) to delegate access so that your secure, alternative AWS account can assume permissions for the impacted AWS account.

After you have delegated appropriate access, you can use the AWS APIs in the affected account to share relevant data, such as logs and volume snapshots, to perform investigative work in the isolated environment. For more information about this cross-account access, see Tutorial: Delegate Access Across AWS Accounts Using IAM Roles.

#### This version has been archived.

#### **Automation Access**

As you migrate to using automation to respond to security events, you must create IAM roles specifically for your automatical respures to use (such as Amagon EC2 instances or AWS) Lambda functions). These resources can then assume the IAM roles and inherit the permissions assigned to the role. Instead of creating and distributing AWS credentials, you delegate permission to your AWS Lambda function or Amazon EC2 instance. The AWS resource automatically receives a set of temporary credentials and uses them to sign API requests.

You cantage of the common that the control of the c

The AWS Systems Manager Agent (SSM Agent) is installed by default on some Amazon EC2 Amazon Machine Images (AMIs), such as for Microsoft Windows Server and Amazon Linux. However, you might need to manually install the agent on other versions of Linux and hybrid instances. Whether you use the Run Command or another tool, complete any prerequisite setup and configuration before you receive your first security-related alert to investigate.

#### Managed Services Access

Your organization may already be partnered with an information technology provider that manages services and solutions on your behalf. These partners have a shared responsibility in supporting the security of your organization, and it's important to clearly understand this relationship before an anomaly occurs. Whether you already work with an AWS Managed Service Provider (MSP) Partner, or AWS Managed Services (p. 22), or a managed security services partner, you must identify the responsibilities of each partner as they relate to your cloud environments, what access the providers already have to your cloud services, what access they need, and points-of-contact or escalation paths for when you need their assistance. Finally, you should practice this with your partner to make sure that your response plans are predictable and successful.

#### **Prepare Processes**

Once appropriate access has been provisioned and tested, your incident response team must define and prepare the related processes necessary for investigation and remediation. This stage is effort intensive because you must sufficiently plan the appropriate response to security events within your cloud environments.

Work closely with your internal cloud services teams and partners to identify the tasks required to ensure that these processes are possible. Collaborate or assign each other response activity tasks and ensure necessary account configurations are in place. We recommend preparing processes and prerequisite configurations in advance to give your organization the following response capabilities.

#### **Topics**

- Decision Trees (p. 18)
- Use Alternative Accounts (p. 18)
- View or Copy Data (p. 19)
- Sharing Amazon EBS Snapshots (p. 19)
- Sharing Amazon CloudWatch Logs (p. 19)
- Use Immutable Storage (p. 20)
- Launch Resources Near the Event (p. 20)
   Isolate Resources (p. 21) version has been archived.
- Launch Forensic Workstations (p. 21)

#### Decision the latest version of this document, visit:

Sometimes, different conditions can require different actions or steps. For example, you might take different actions based on the type of AWS account (development versus production), the tags of the resources, the AWS Config rules compliance status of those resources, or other inputs.

To supptings:///thecearawana anazonarion of these decisions we reclaiment to decisions and decisions are reclaiment to the suppting of the contract of the suppting of the contract of the suppting of the sup decision tree with your other reints and clare significant configuration of the second configuration of the second

#### Use Alternative Accounts

Although responding to an event in the impacted account might be required, it is ideal to investigate data outside of the affected account. Some customers have a process for creating separate, isolated AWS account environments, using templates that preconfigure the resources they must provision. These

#### AWS Security Incident Response Guide AWS Technical Guide View or Copy Data

templates are deployed through a service, such as AWS CloudFormation or Terraform, which provides an easy method to create a collection of related AWS resources and provision them in an orderly and predictable fashion.

Preconfiguring these accounts using templated mechanisms helps to remove human interactions during the initial stages of an incident and ensure that the environment and resources are prepared in a repeatable and predictable manner, which can be verified by an audit. In addition, this mechanism also increases the ability to maintain security and containment of data in the forensics environment.

This approach requires you to work with your cloud services and architect teams to determine an appropriate AWS account process that can be used for investigations. For example, your cloud services teams could use AWS Organizations to generate new accounts and assist you in preconfiguring those accounts using a templated or scripted method.

This method of segmentation is best when you need to keep a larger organization removed from a potential threat. This segmentation, using a new and largely unconnected AWS account, means that a user from the Organization, labeled in multi-account documentation as the security Organizational Unit (OU), is able to move into the account, perform the needed forensics activities, and potentially hand off the account as a whole to a legal entity, if needed. This method of forensics and attribution requires significant review and planning and should align with the enterprise's GRC policies. Although this work is not easy, it is far easier to do prior to building a large account base.

#### View or Copy Data

Responders require access to logs or other evidence to analyze, and must ensure that they have the ability to view or copy data. At a minimum, the IAM permission policy for the responders should provide read-only access so that they can investigate. To enable appropriate access, you might consider some pre-built AWS Managed Policies, such as SecurityAudit or ViewOnlyAccess.

For example, responders might want to make a point-in-time copy of data, such as the AWS CloudTrail logs, from an Amazon S3 bucket in one account to an Amazon S3 bucket in another account. The permissions provided by the ReadOnlyAccess managed policy, for example, enable the responder to perform these actions. To understand how to use the AWS Command Line Interface (CLI) to perform this, see How can I copy all objects from one Amazon S3 bucket to another bucket?.

# Sharing Amazon EBS Snapshots This version has been archived.

Many customers use Amazon Elastic Block Store (Amazon EBS) snapshots as part of their investigation for security events that involve their Amazon EC2 instances. Snapshots of Amazon EBS volumes are incremental backups. For more information about Amazon EBS incremental snapshots, see Amazon EBS snapshots.

For the latest version of this document, visit:

To perform an investigation of an Amazon EBS volume in a separate, isolated account, you must modify the permissions of the snapshot to share it with the other specified AWS accounts. Users that you have authorized can use the snapshots you share as the basis to create their own EBS volumes, while your original snapshot remains unaffected. For more information, see Share an Amazon EBS snapshot.

If your shapshot is encrypted, your must also share the custom takes key management service (AWS KMS) Customer Managed/Keys/EMK) rised tipe reinfluctiffs rises both you can share a later time. Snapshots are constrained to the Region in which they were created, but you can share a snapshot with another Region by copying the snapshot to that Region. For more information, see Copy an Amazon EBS snapshot.

#### Sharing Amazon CloudWatch Logs

Logs that are recorded in Amazon CloudWatch Logs, such as Amazon VPC flow logs, can be shared with another account (such as your centralized security account) through a CloudWatch Logs subscription. For

#### AWS Security Incident Response Guide AWS Technical Guide Use Immutable Storage

example, the log event data can be read from a centralized Amazon Kinesis stream to perform custom processing and analysis. Custom processing is especially useful when you collect logging data from across many accounts. Ideally, create this configuration early in your cloud journey, before a security-related event occurs. For more information, see Cross-Account Log Data Sharing with Subscriptions.

#### Use Immutable Storage

When copying logs and other evidence to an alternative account, make sure that the replicated data is protected. In addition to protecting the secondary evidence, you also must protect the integrity of the data at the source. Known as *immutable* storage, these mechanisms protect the integrity of your data by preventing the data from being tampered with or deleted.

Using the native features of Amazon S3, you can configure an Amazon S3 bucket to protect the integrity of your data. For example, by using S3 Object Lock, you can prevent an object from being deleted or overwritten for a fixed amount of time or indefinitely. Managing access permissions with S3 bucket policies, configuring S3 versioning, and enabling MFA Delete are other ways to restrict how data can be written or read. This type of configuration is useful for storing investigation logs and evidence, and is often referred to as write once, read many (WORM). You can also protect the data by using server-side encryption with AWS Key Management Service (AWS KMS) and verifying that only appropriate IAM principals are authorized to decrypt the data.

Moreover, you can protect the data in Amazon S3 Glacier by using the Amazon S3 Glacier Vault Lock, which allows you to easily deploy and enforce compliance controls for individual Amazon S3 Glacier vaults with a vault lock policy. You can specify security controls, such as WORM, in a vault lock policy and lock the policy from future edits. Once locked, the policy can not be changed. Amazon S3 Glacier enforces the controls set in the vault lock policy to help achieve your compliance objectives, such as for data retention. You can deploy a variety of compliance controls in a vault lock policy using the AWS Identity and Access Management (IAM) policy language.

#### Launch Repoils reasion at a she Eyarchived.

For responders who are new to the cloud, it can be tempting to try to conduct cloud investigations on premises where your existing tools are located. In our experience, AWS customers who respond to incidents using cloud technologies achieve better results—isolations can be automated, copies can be made mor point property properties of religious technologies.

The best practice is to perform investigations and forensics in the cloud, where the data is, rather than attempting to transfer the data to a data center before you investigate. You can use the secure compute and storage capabilities of the cloud practically anywhere in the world to perform the secure response operations. Many customers choose to pre-build a separate AWS account that is ready to perform an investigation is expected to retain records for compliance and legal reasons, it might be prudent to maintain separate accounts for long-term storage and legal activities.

welcome.html

It is also a best practice to perform the investigation in the same AWS Region where the event occurred, rather than replicating the data to another Region. We recommend this practice primarily because of the additional time required to transfer the data between Regions. For each AWS Region that you operate in, make sure that both your incident response process and the responders abide by the relevant data privacy laws. If you do need to move data between Regions, consider the legal implications of moving data between jurisdictions. It is generally a best practice to keep the data within the same national jurisdiction.

#### AWS Security Incident Response Guide AWS Technical Guide Isolate Resources

If you believe a security event is impacting your security, identity, or communication systems, you might need to seek alternative mechanisms and access to investigate and remediate the impact. AWS offers you the ability to quickly launch new infrastructure that can be used for secure, alternate work environments. For example, while you investigate the potential severity of the situation, you might want to create a new AWS account with the secure tools needed by your legal counsel, public relations, and security teams to communicate and continue working. Services such as AWS WorkSpaces (for virtual desktops), AWS WorkMail (for email), and Amazon Chime (for communication) can provide your response teams, leadership, and other participants with the capabilities and connectivity they need to communicate, investigate, and remediate an issue.

#### **Isolate Resources**

In the course of your investigation, you might need to isolate resources as part of your response to a security anomaly. The intention behind isolating resources is to limit the potential impact, prevent further propagation of affected resources, limit the unintended exposure of data, and prevent further unauthorized access.

As with any response, business, regulatory, legal, or other considerations can apply. Make sure to weigh your intended actions against expected and unexpected consequences. If your cloud teams use resource tags, these tags can help you identify the criticality of the resource or the owner to contact.

#### **Launch Forensic Workstations**

Some of your incident response activities might include analyzing disk images, file systems, RAM dumps, or other artifacts that are involved in an incident. Many customers build a customized forensic workstation that they can use to mount copies of any affected data volumes (known as EBS snapshots). To do so, follow these basic steps:

- 1. Choose a base Amazon Machine Image (AMI) (such as Linux or Microsoft Windows) that can be used as a forensic workstation.
- 2. Launch an Amazon EC2 instance from that base AMI.
- 3. Harden the operating system, remove unnecessary software packages, and configure relevant auditing and logging mechanisms.
- 4. Install your preferred suite of open source or private toolkits, as well as any vendor software and packages that you his version has been archived.
- 5. Stop the Amazon EC2 instance and create a new AMI from the stopped instance.
- 6. Create a weekly or monthly process to update and rebuild the AMI with the latest software patches.

After the forms it is the simple of the forensic workstation for each investigation. The process for launching the AMI as an Amazon EC2 instance can be preconfigured to simplify the deployment process. For example, you can create a template of the forensic infrastructure resources that you need in a text file and deploy it into your AWS account using AWS CloudFormation.

https://docs.aws.amazon.com/whitepapers/latest/ When your resources are available to be deployed quickly from a template, your well-trained forensic expertsawsbisecustity-incid watstatispanseshquidigation, instead of reusing infrastructure. With this process, you can make sure that there is no cross-contamination from other forensic examinations.

#### **Instance Types and Locations**

Amazon EC2 provides a wide selection of instance types that are optimized for different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Many instance

#### AWS Security Incident Response Guide AWS Technical Guide Cloud Provider Support

types include multiple instance sizes, which enables you to scale your resources to the requirements of your target workload. For incident response instances, follow your company's GRC policies for location and segmentation from the network that runs production instances.

AWS enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. There is no additional charge for using enhanced networking. For information about which instance types support 10 or 25 Gbps network speeds, and other advanced capabilities, see Amazon EC2 Instance Types.

#### **Cloud Provider Support**

#### **Topics**

- AWS Managed Services (p. 22)
- AWS Support (p. 22)
- DDoS Response Support (p. 22)

#### **AWS Managed Services**

AWS Managed Services (AMS) provides ongoing management of your AWS infrastructure so that you can focus on your applications. By implementing best practices to maintain your infrastructure, AMS helps to reduce your operational overhead and risk. AMS automates common activities such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support your infrastructure.

As an Infrastructure Operator, AMS takes responsibility for deploying a suite of security detective controls and provides a 24/7 first line of response to alerts, using a follow-the-sun model. When an alert is triggered, AMS follows a standard set of automated and manual runbooks to ensure a consistent response. These runbooks are shared with AMS customers during onboarding so they can develop and coordinate response with AMS. AMS encourages the joint execution of security response simulations with customers to develop operations and the provided and the customers to develop operations are all the customers.

#### AWS Support

AWS Suppropries and estawers in Moderces is to compenite this it is to compenite this item of your AWS solutions. All support plans provide 24/7 access to customer service, AWS documentation, whitepapers, and support forums. If you need technical support and more resources to help plan, deploy, and optimize your AWS environment, you can select a support plan that best aligns with your AWS use case.

You should she says a contact to get support favings we detail for the AWS Management of the support of the sup

Additionally, if you need to report abuse of Amazon EC2, contact the AWS Abuse team.

#### **DDoS Response Support**

A Denial of Service (DoS) attack makes your website or application unavailable to end users. Attackers use a variety of techniques that consume network bandwidth or other resources, disrupting access for

#### AWS Security Incident Response Guide AWS Technical Guide DDoS Response Support

legitimate end users. In its simplest form, a DoS attack against a target is executed by a lone attacker from a single source.

In a Distributed Denial of Service (DDoS) attack, an attacker uses multiple sources, which may be compromised or controlled by a group of collaborators, to orchestrate an attack against a target. In a DDoS attack, each of the collaborators or compromised hosts participates in the attack, generating a flood of packets or requests to overwhelm the intended target.

AWS offers customers AWS Shield, which provides a managed DDoS protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield: Standard and Advanced.

All AWS customers benefit from the no cost, automatic protections of AWS Shield Standard. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

For higher levels of protection against attacks targeting your web applications running on Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront, and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. Additionally, AWS Shield Advanced gives you 24/7 access to the AWS DDoS Response Team (DRT). For more information about AWS Shield Standard and AWS Shield Advanced, see AWS Shield.

#### This version has been archived.

For the latest version of this document, visit:

# Simulate

#### **Topics**

- Security Incident Response Simulations (p. 24)
- Simulation Steps (p. 24)
- Simulation Examples (p. 25)

#### Security Incident Response Simulations

Security Incident Response Simulations (SIRS) are internal events that provide a structured opportunity to practice your incident response plan and procedures during a realistic scenario. SIRS events are fundamentally about being prepared and iteratively improving your response capabilities. Some of the reasons customers find value in performing SIRS activities include:

- · Validating readiness.
- Developing confidence by learning from simulations and training staff.
- Following compliance or contractual obligations.
- Generating artifacts for accreditation.
- · Being agile and gaining incremental improvement with focus.
- · Improving speed and tools.
- Refining communication and escalation.
- Developing comfort with the rare and the unexpected.

For these reasons, the value derived from participating in a SIRS activity increases an organization's effectiveness during stressful events. Developing a SIRS activity that is both realistic and beneficial can be a difficult exercise. Although testing your procedures or automation that handles well-understood events has certain advantages, it is just as valuable to participate in creative SIRS activities to test yourself against the prespected residuals been archived.

### **Simulation Steps**

Regardles Forhthe Latest Wersion of this document, wisitine groundwork, simulations generally follow these steps:

- 1. Find an issue of importance Define the trigger that should cause a response.
- 2. Identify skilled security engineers A simulation requires a builder and a tester.
- 3. Build a party chose systems The small allow must be it as participants might not value the exercise is it is too minimal the exercise might not value the exercises and work towards a full event.
- 4. **Build and test the scenario elements** Called and test the scenario elements and alerts, and potential runbooks.
- 5. **Invite other security individuals and cross-organizational participants –** Invite everyone who needs to train and participate. If your general legal counsel, executives, and public relations have a part in the simulation, you should also invite them.
- 6. **Run the simulation** Choose if your staff should expect the SIRS event, or if the simulation should remain unannounced.

#### AWS Security Incident Response Guide AWS Technical Guide Simulation Examples

7. Celebrate, measure, improve, and repeat – The simulation has factors of stress, so it is important to encourage and celebrate the efforts of your participants. After encouragement comes the opportunity to measure, improve, and iterate for the next simulation. AWS encourages you to make a habit of these activities.

#### **Important**

If you are planning a Security Incident Response Simulation (SIRS), see Penetration Testing and review the *Other Simulated Events* section for the latest information on how to proceed.

#### Simulation Examples

Security simulations must be realistic to provide the expected value. When you or your partners work toward creating your own simulations, always consider past, real-world events as a valuable source for potential simulation exercises. Here are a few examples that AWS customers have found useful to use for their initial simulations:

- Unauthorized changes to network configuration or resources.
- Credentials that were mistakenly exposed publicly due to developer misconfiguration.
- Sensitive content that was mistakenly made publicly accessible by developer misconfiguration.
- Isolation of a web server that is communicating with suspected malicious IP addresses.

In addition to the valuable, experiential learning, performing SIRS activities generates outputs, such as lessons learned, that you can use as inputs into the next process of your program: iteration.

This version has been archived.

For the latest version of this document, visit:

#### **Iterate**

The previous section defined some of the benefits of SIRS activities. Among these advantages was gaining agility through incremental improvements. Simulations should generate valuable outcomes that you can leverage to improve your security response. They provide a feedback loop to the organization, about what is working and what is not working. With this knowledge, you can incrementally create new procedures or update existing ones to improve your response.

#### **Topics**

- Runbooks (p. 26)
- Automation (p. 27)

#### Runbooks

When a security anomaly is detected, containing the event and returning to a known good state are important elements of a response plan. As an example, if the anomaly occurred because of a security misconfiguration, the remediation might be as simple as removing the variance through a redeployment of the resources with the proper configuration. To do this, you will need to plan ahead and define your own security response procedures, which are often called runbooks.

A runbook is the documented form of an organization's procedures for conducting a task or series of tasks. This documentation is usually stored either in an internal digital system or on printed paper. You might currently have incident response runbooks, or you might need to create them to be compliant to a security assurance framework. However, when you manually follow written runbooks, you increase the potential that you will make mistakes. Instead, we recommend that you automate all of your repeatable tasks. Automation frees your response team from common tasks, and makes them available for more important tasks, surther correlating events practicing in simulations, devising new response procedures, performing research, developing new skills, and testing or building new tools. However, before you can decompose the tasks into programmable logic and iterate towards proper automation, you must start by writing a runbook.

#### Creating the latest kersion of this document, visit:

To create runbooks for the cloud, we recommend that you first focus on the alerts you currently generate. If you generate an alert, it is important to investigate it. Start by defining the descriptions of the manual processes that you perform. After this, test the processes and iterate on the runbook pattern to psychology a logic afrom the complete white what the exceptions are for those scenarios. For example, in a development environment, you might want to terminate a misconfigured Amazon EC2 instance. However, if the same event occurred in a production environment, instead of the himself instance, you might stop the instance and verify with stakeholders that critical data will not be lost and whether termination is acceptable.

After you determine the best solution, you can deconstruct the logic into a code-based solution, which can be used as a tool by many responders to automate the response and remove variance or guess-work by your responders. This speeds up the lifecycle of a response. The next goal is to enable this code to be fully automated by being invoked by the alerts or events themselves, rather than them being executed by a human responder.

#### **Getting Started**

If you're not sure where to start, consider beginning with the alerts that could be generated by AWS Trusted Advisor, AWS Security Hub's Foundational Security Best Practices, and AWS Config Rules (including the AWS Config Rules Github repository). Then, focus on events generated by services that will describe systems that you are concerned with.

Amazon GuardDuty and Access Analyzer describe many of the domains that an application will use in AWS, which is why they are generally suggested; however, Amazon Inspector and Amazon Macie have specific uses for those that have data and end point concerns. Information about Amazon GuardDuty findings is available in the Amazon GuardDuty User Guide. Access Analyzer findings are available in the Amazon Access Analyzer User Guide. Macie findings are available in the Amazon Macie User Guide. Amazon Inspector findings are available in the Amazon Inspector User Guide. Security Hub gives you the ability to unify those findings into one place and react to them in concert with low latency, which is why it is suggested as a central location for remediation.

All of the above services send notifications through Amazon CloudWatch Events when any change in the findings or alerts occurs, including newly generated alerts and updates to existing alerts. You can set up the Amazon CloudWatch Events rules to trigger AWS Lambda functions to perform an event-driven response. However, the ability to build custom insights and add your own findings from the application domain adds to the weighty reasons to use Security Hub instead. For more information, see the Event-Driven Response (p. 31) section.

#### **Automation**

Automation is a force multiplier, which means it scales the efforts of your responders to match the speed of the organization. Moving from manual processes to automated processes enables you to spend more time increasing the security of your AWS Cloud environment.

#### **Topics**

- Automating Incident Response (p. 27)
- Event-Driven Response (p. 31)

# Automating incident Response

To automate security engineering and operations functions, you can use a comprehensive set of APIs and tools from AWS. You can fully automate identity management, network security, data protection, and monition of the lites were proventially according to the contraction of the c

If your incident response teams continue to respond to alerts in the same way, they risk alert fatigue. Over time, the team can become desensitized to alerts and can either make mistakes handling ordinary situations of sing functions that process the repetitive and ordinary alerts to be specifically and unique incidents.

You can improve manual processes **Wp logaring ancilly** automating steps in the process. After you define the remediation pattern to an event, you can decompose that pattern into actionable logic, and write the code to perform the logic. Responders can then execute that code to remediate the issue. Over time, you can automate more and more steps, and ultimately automatically handle whole classes of common incidents.

However, your objective should be to further reduce the time gap between detective mechanisms and responsive mechanisms. Historically, this time gap can take hours, days, or even months. An Incident

Response survey by SANS in 2016 found that 21% of respondents stated their time to detection took two to seven days, and only 29% of respondents were able to remediate events within the same time frame. In the cloud, you can reduce that response time gap to seconds by building event-driven response capabilities.

#### **Topics**

- Options for Automating Response (p. 28)
- Cost Comparisons in Scanning Methods (p. 30)

#### **Options for Automating Response**

It is important to make sure that you balance the enterprise implementation and organization structure. *Figure 4* illustrates the differences in technical attributes for each automated response option in your AWS implementation with a radar chart. In the chart, the further the technical attribute moves from the center of the chart, the greater the strength of that technical attribute for the corresponding automation response. For example, AWS Lambda offers more speed and requires a less technical skillset. AWS Fargate offers more flexibility and requires less maintenance and technical skillset. *Table 1* provides an overview of these automation options and a summary of the technical attributes of each.

#### **Technical Attributes**

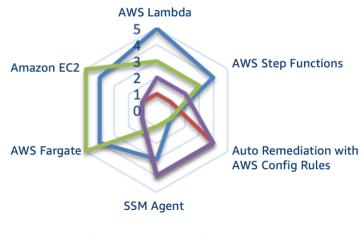




Figure 4: Differences in technical attributes or as of this document, visit:

Table 1: Options for automated response

AWS Service or Feature	Description	Attributes Summary*
aws-security	System using AWS Lambda THIS LEIGHT TO SPREAMED SOLVE WELLOW TO SUPPLY TO SU	Speed ide/ Flexibility
		Maintenance
		Skillset
AWS Step Functions	System using AWS Step Functions, Lambda, and SSM	Speed
	Agent.	Flexibility

#### AWS Security Incident Response Guide AWS Technical Guide Automating Incident Response

AWS Service or Feature	Description	Attributes Summary*
		Maintenance
		Skillset
Auto Remediation with AWS Config Rules	Set of AWS Config Rules and auto remediations that evaluate the environment and push it back into the approved specification.	Maintenance & Skillset Speed & Flexibility
SSM Agent	Set of automation rules and documents reviewing many pieces of the environments and internal systems and making corrections.	Maintenance & Skillset Speed Flexibility
AWS Fargate	AWS Fargate system using open source step function code and the events from Amazon CloudWatch, and other systems, to drive detection and remediation.	Flexibility Speed Maintenance & Skillset
Amazon EC2	A system running on a full instance, similar to the AWS Fargate option.	Flexibility Speed Maintenance Skillset

<sup>\*</sup> Attributes are listed in descending order for each service or feature. For example, AWS Lambda offers more speed and requires less technical skillset. AWS Fargate offers more flexibility, and requires less maintenance and technical skillset.

As you consider the **Tais** n**Version** s**has** in **Deen** variety **and** is o need to consider centralization and scan period (events per second [EPS]).

Centralization refers to a central account that drives all of the detection and remediation for an organization. This approach may seem like the best choice out-of-the-box, and it is the current best practice. However, spend gire most account that the property of the proof of the current best when depends on how you handle your subordinate accounts. We encourage you to get started by leveraging the approach of the Security Tooling account in the Multi-Account Framework in AWS Organizations or AWS Control Tower.

Table 2: Pros and cons of centralization

#### https://docs.aws.amazon.com/whitepapers/latest/

	Centralization	Decentralization
Pros	Wiffice Configuration management Unable to cancel or modify response	Simple architecture Faster initial setup
Cons	Increased complexity in architecture	More resources to manage

#### AWS Security Incident Response Guide AWS Technical Guide Automating Incident Response

Centralization	Decentralization
Onboarding/offboarding accounts and resources	Difficulty maintaining a software baseline

A cost comparison for these implementations may also drive your enterprise decision in determining the best option. Events per second (EPS) is the metric that you use to best estimate cost. It may, in the end, be far easier and cheaper to use centralized or decentralized approaches, but it is impossible for us to review how you will evaluate that cost specifically in your account. Make sure to consider EPS when sending those events to a central account to be responded to. The more EPS, the higher the cost of sending those events to a centralized account.

#### **Cost Comparisons in Scanning Methods**

Costs are further determined by the scanning method by which an anomaly is detected and the time frame between validations. For scanning methods, you can choose between *event based* or *periodic scan* review. *Table 3* shows the pros and cons of both approaches.

Table 3: Pros and cons of different scanning methods

	Event-Based	Periodic Scan
Pros	Less time from event to response  Limited need to query additional API calls	Full picture at a given point in time
Cons	Limited state context around the resource	Service limits against large accounts
This vers	Events triggered may be for a resource not readily available sion has been archiv	Can potentially run into throttling due to high volume of calls

In many cases, a combination of both scanning approaches is most likely the best choice in a fully mature organization. The AWS Security Hub and AWS Foundational Security Best Practices standard provide a combination of this document, visit:

Figure 5 provides a radar chart illustrating the cost comparison of events per second (EPS) for each of the automation approaches. For example, Amazon EC2 and AWS Fargate have the highest costs for running 0-10 EPS, whereas AWS Lambda and AWS Step Functions have the highest costs for running 76+ EPS.

# Amazon EC2 Aws Lambda Aws Step Functions Aws Fargate Auto Remediation with Aws Config Rules

Figure 5: Cost comparison of automation options scanning methods (events per second [EPS])

**—11-50 EPS** 

#### **Event-Driven Response**

■0-10 EPS

With an event-driven response system, a detective mechanism triggers a responsive mechanism to automatically remediate the event. You can use event-driven response capabilities to reduce the time-to-value between detective Mechanism and appeared had a serverless compute service that runs your code in response to events and automatically manages the underlying compute resources for you.

SSM Agent

•51-75 EPS —— 76+ EPS

For example, assume that you have an AWS account with the AWS CloudTrail service enabled. If AWS CloudTrail service enabled the service again and investigate the user that disabled the AWS CloudTrail logging. Instead of performing these steps manually in the AWS Management Console, you can programmatically enable the logging again (through the cloudtrail:StartLogging API). If you implement this with code, your response objective is to perform this task as quickly as possible and notify the responders that the response was performed

#### esponse was performed aws.amazon.com/whitepapers/latest/

You can decompose the legic intesimple totle torunin an AWS Lambda function to perform these tasks. You can then use Amazon CloudWatch Events monitor for the specific cloudtrail: StopLogging event, and invoke the function if it Weeks What Lambda responder function is invoked by Amazon CloudWatch Events, you can pass it the details of the specific event with the information of the principal that disabled AWS CloudTrail, when it was disabled, the specific resource that was affected, and other relevant information. You can use this information to enrich the finding from logs, and then generate a notification or alert with only the specific values that a response analyst would require.

Ideally, the goal of event-driven response is for the Lambda responder function to perform the response tasks and then notify the responder that the anomaly has been successfully resolved with any pertinent

#### AWS Security Incident Response Guide AWS Technical Guide Event-Driven Response

contextual information. It is then up to the human responder to decide how to determine why it occurred and how future reoccurrences might be prevented. This feedback loop drives further security improvement into your cloud environments. To achieve this objective, you must have a culture that enables your security team to work closer with your development and operations teams.



For the latest version of this document, visit:

# **Incident Response Examples**

#### **Topics**

- Service Domain Incidents (p. 33)
- Infrastructure Domain Incidents (p. 34)

### Service Domain Incidents

Service domain incidents are typically handled exclusively through AWS APIs.

### Identities

AWS provides APIs to our cloud services that are used by millions of customers to build new applications and drive business outcomes. These APIs can be invoked through many methods, such as by software development kits (SDKs), the AWS CLI, and the AWS Management Console. To interact with AWS through these methods, the IAM service helps you securely control access to AWS resources. You can use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources at the Account Level. For a list of AWS services that you can use with IAM, see AWS Services That Work with IAM.

When you first create an AWS account, you begin with a single sign-on (SSO) identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, and particularly not for administrative tasks. Instead, we recommend that you follow the best practice of using the root user only to create your first IAM user, securely store the root user credentials, and perform only a few account and service management tasks. For more information, see Create Individual IAM Users.

Although these API**Thris**le **Veirsiori**linas deep sare hived can be abused if the wrong individuals get access to your IAM account or root credentials. For example, you can use the APIs to enable logging within your account, such as AWS CloudTrail. However, if attackers get your credentials, they can also use the API to disable these logs. You can prevent this type of abuse by configuring appropriate IAM permissions that follow a least privilege model, and by properly protecting your IAM credentials for interesting your IAM credentials for interesting your IAM credentials. If this type of event does occur, there are multiple detective controls to identify that your AWS CloudTrail logging was disabled, including AWS CloudTrail, AWS Config, AWS Trusted Advisor, Amazon GuardDuty, and AWS CloudWatch Events.

# Resetps://docs.aws.amazon.com/whitepapers/latest/

Other features that can be abused or misconfigured vary from organization to organization, based on how each customer operates in the week correspondent organizations intend to make certain data or applications publicly accessible, while others keep their applications and data internal and confidential. Not all security events are malicious in nature; some events might result from unintentional or improper configurations. Consider which APIs or features have a high impact to your organization, and whether you use them frequently or infrequently.

You can identify many security misconfigurations using tools and services. For example, AWS Trusted Advisor provides a number of checks for best practices. APN Partners also offer hundreds of industry-

#### AWS Security Incident Response Guide AWS Technical Guide Infrastructure Domain Incidents

leading products that are equivalent, identical to, or integrate with existing controls in your on-premises environments. A number of these products and solutions have been prequalified by the AWS Partner Competency Program. We encourage you to visit the Configuration and Vulnerability Analysis section of the APN Security Competency program to browse these solutions and to determine if they can satisfy your requirements.

### Infrastructure Domain Incidents

The infrastructure domain typically includes your application's data or network-related activity, such as the traffic to your Amazon EC2 instances within the VPC and the processes running in your Amazon EC2 instance operating systems.

For example, assume that your monitoring solution notified you of a potential security anomaly on your Amazon EC2 instance. The following actions are common steps to address this issue:

- Capture the metadata from the Amazon EC2 instance, before you make any changes to your environment.
- Protect the Amazon EC2 instance from accidental termination by enabling termination protection for the instance.
- Isolate the Amazon EC2 instance by switching the VPC Security Group. However, be aware of VPC connection tracking and other containment techniques.
- 4. **Detach** the Amazon EC2 instance from any AWS Auto Scaling groups.
- 5. Deregister the Amazon EC2 instance from any related Elastic Load Balancing service.
- 6. **Snapshot** the Amazon EBS data volumes that are attached to the EC2 instance for preservation and follow-up investigations.
- 7. **Tag** the Amazon EC2 instance as quarantined for investigation, and add any pertinent metadata, such as the trouble ticket associated with the investigation.

You can perform all of the preceding steps using the AWS APIs, AWS SDKs, AWS CLI, and AWS Management Console. To interact with AWS using these methods, the IAM service helps you securely control access to AWS resources at the Account Level. The IAM service provides the authentication and authorization for you to perform these actions and interact with the service domain.

A snapshot of an Amazon EBS volume is a point-in-time, block-level copy of an EBS data volume, which occurs asymptoping and might take time to complete, but it is a delta of that data going forward. You can create new EBS volumes from these copies and mount them to the forensic EC2 instance for deep analysis offline by forensic investigators. The following diagram shows a simplified version of the outcome, and does not describe all of the network components (such as subnets, routing tables, and network access control lists).

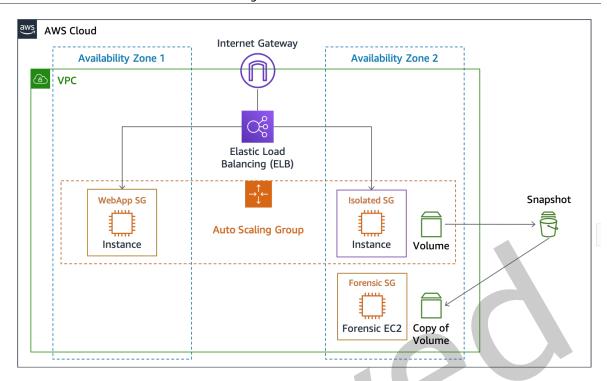


Figure 6: EC2 Instance Isolation and Snapshots

#### **Topics**

- Investigation Decisions (p. 35)
- Capturing Volatile Data (p. 35)
- Using AWS Systems Manager (p. 36)
- Automating the Capture (p. 36)

# Investigations Decision has been archived.

At this point, you can choose between an offline investigation (immediately shutting down the instance) or an online investigation (keeping the instance running). One advantage to the offline investigation is that after the instance is shut down, it can no longer affect the existing environment. Additionally, you can create a tage of the control of the standard of the control of the control

### Capttpsin/dowslawikenpagen.com/whitepapers/latest/ aws-security-incident-response-guide/

Although you might not choose to perform the entire investigation, it is important to understand the necessary mechanisms to capture volatile data from an instance. An online investigation requires interaction with the operating system that is running on the Amazon EC2 instance. In this scenario, you need more than the AWS IAM service to execute tasks on an Amazon EC2 instance. Although you could authenticate directly to the machine using a standard method (such as Linux secure shell (SSH) or Microsoft Windows remote desktop (RDP)), manual interaction with the operating system is not a best practice. We recommend that you programmatically use an automation tool to execute tasks on a host.

### **Using AWS Systems Manager**

The AWS Systems Manager Run Command helps you to remotely and securely perform on-demand changes running Linux shell scripts and Windows PowerShell commands on a targeted instance. Although you can invoke Run Command through permissions in the AWS IAM service, you must first activate your Amazon EC2 instances as managed instances, install the SSM Agent on your machines (if it's not installed by default), and configure the AWS IAM permissions. If you are interested in using Run Command for automation or response activities, make sure to complete the prerequisite activities before you have to perform an investigation.

AWS Systems Manager, which includes the Run Command, is integrated with AWS CloudTrail, a service that captures API calls made by or on behalf of a Systems Manager and delivers the log files to an Amazon S3 bucket that you specify. Using the information collected by AWS CloudTrail, you can determine what request was made, the source IP address that made the request, who made the request, when it was made, and more. CloudTrail creates logs of all Systems Manager API actions, including API requests to execute commands using Run Command or to create Systems Manager documents.

You can use the AWS Systems Manager Run Command service to invoke the SSM Agent that executes Linux shell scripts and Windows PowerShell commands. These scripts can load and execute specific tools to capture additional data from the host, such as the Linux Memory Extractor (LiME) kernel module. You can then transfer the memory capture to your forensic Amazon EC2 instance in the VPC network, or to an Amazon S3 bucket for durable storage.

### **Automating the Capture**

One method to invoke the SSM Agent is to target the Run Command through Amazon CloudWatch Events when the instance is tagged with a specific tag. For example, if you apply the Response=Isolate+MemoryCapture tag to an affected instance, you can configure Amazon CloudWatch Events to trigger two actions:

- A Lambda function that performs the isolation activities
- · A Run Command that executes a shell command to export the Linux memory through the SSM Agent

This tag-driven response is another method of event-driven response.

This version has been archived.

For the latest version of this document, visit:

# Conclusion

As you continue your cloud journey, it is important for you to consider the aforementioned fundamental security incident response concepts for your AWS environment. You can combine the available controls, cloud capabilities, and remediation options to help you improve the security of your cloud environment. You can also start small and iterate as you adopt automation capabilities that improve your response speed, so you are better prepared when security events occur.



This version has been archived.

For the latest version of this document, visit:

# **Additional Resources**

#### For additional information, see:

- · AWS Well-Architected
- AWS Cloud Adoption Framework page
- · AWS Centralized Logging Solution
- Visualize AWS CloudTrail Logs using AWS Glue and Amazon QuickSight
- · How to Monitor Host-Based Intrusion Detection System Alerts on Amazon EC2 Instances
- Store and Monitor OS & Application Log Files with Amazon CloudWatch
- Identity and Access Management in Amazon S3
- Using Versioning (Amazon S3)
- Using MFA Delete
- Protecting Data Using Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
- Incident Response with AWS Console and CLI
- Preparing for the California Consumer Privacy Act

### Media

- AWS re:Invent 2014 (SEC402): Intrusion Detection in the Cloud
- AWS re:Invent 2014 (SEC404): Incident Response in the Cloud
- AWS re:Invent 2015 (SEC308): Wrangling Security Events in The Cloud
- AWS re:Invent 2015 (SEC316): Harden Your Architecture with Security Incident Response Simulations
- AWS re:Invent 2016 (SEC313): Automating Security Event Response, from Idea to Code to Execution
- AWS re:Invent 2017 (SID302): Force Multiply Your Security Team with Automation and Alexa
- AWS re:Invent 2016/SAC316): Security Automation: Spend Less Time Securing Your Applications
   AWS re:Invent 2016 (SAC304): Predictive Security: Using Big Data to Fortify Your Defenses
- AWS re:Invent 2017 (SID325): Amazon Macie: Data Visibility Powered by Machine Learning for Security and Compliance Workloads
- AWS London Summit 2018: Automating Incident Response and Forensics in AWS For the latest version of this document, visit:

# **Third-Party Tools**

The following links to this capacity took are exterminant and interpretations of any kind about these tools or pages.

aws-security-incident-response-guide/

- AWS\_IR Python installable command line utility for mitigation of host and key compromises.
- MargaritaShotgun Remote Memory Acquisition Tool.
- ThreatPrep Python module for evaluation of AWS account best practices around incident handling readiness.
- ThreatResponse Web Web based analysis platform for use with the AWS\_IR command line tool.
- GRR Rapid Response Remote live forensics for incident response.
- Linux Write Blocker The kernel patch and user-space tools to enable Linux software write blocking.

# **Industry References**

• NIST SP 800-61R2: Computer Security Incident Handling Guide



This version has been archived.

For the latest version of this document, visit:

# **Document Revisions**

To be notified about updates to this whitepaper, subscribe to the RSS feed.

update-history-change	update-history-description	update-history-date
Minor updates (p. 40)	Bug fixes and numerous minor changes throughout.	April 1, 2022
Minor updates (p. 40)	Bug fixes and numerous minor changes throughout.	June 2, 2021
Minor update (p. 40)	Corrected broken links.	March 5, 2021
Whitepaper updated (p. 40)	Corrected broken links and numerous text changes to improve readability.	November 23, 2020
Minor update (p. 40)	Fixed link to "Incident Response with AWS Console and CLI".	June 30, 2020
Whitepaper updated (p. 40)	Updated for new security services, threat intelligence, shared responsibility for containers, automation, and CCPA. Added appendices with sample decision tree and runbook.	June 11, 2020
Initial publication (p. 40)	Whitepaper first published	June 1, 2019

# This version has been archived.

For the latest version of this document, visit:

# Appendix A: Cloud Capability Definitions

AWS offers over 150 cloud services and thousands of features. Many of these provide native detective, preventative, and responsive capabilities, and others can be used to architect custom security solutions. This section includes a subset of those services that are most relevant to incident response in the cloud.

#### **Topics**

- Logging and Events (p. 41)
- Visibility and Alerting (p. 42)
- Automation (p. 43)
- Secure Storage (p. 44)
- Custom (p. 44)

# **Logging and Events**

AWS CloudTrail – AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Validated log files are invaluable in security and forensic investigations. To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation. This feature is built-in using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files vincers.

By default, the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption. You can optionally use the AWS Key Management Service (AWS KMS) managed keys (SSE-KMS) for your CloudTrail log files.

Amazon cloudwatch Events – Amazon cloudwatch Events delivers a near real-time stream of system events that describe changes in AWS resources, or when API calls are published by AWS CloudTrail. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. CloudWatch Events becomes aware of operational changes as they occur. CloudWatch Events can respond to these operational changes and take corrective action as necessary, by sending these too spond to these operational changes and take corrective action as necessary, by sending these too spond to these operations. Some security services such as Amazon Guard Duty, produce their output in the form of CloudWatch Events.

#### welcome.html

AWS Config – AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and enables you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, manually or automatically. You can review detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

#### AWS Security Incident Response Guide AWS Technical Guide Visibility and Alerting

Amazon S3 Access Logs – If you store sensitive information in an Amazon S3 bucket, you can enable S3 access logs to record every upload, download, and modification to that data. This log is separate from, and in addition to, the CloudTrail logs that record changes to the bucket itself (such as changing access policies and lifecycle policies).

Amazon CloudWatch Logs – You can use Amazon CloudWatch Logs to monitor, store, and access your log files (such as your operating system, application, and custom log files) from your Amazon Elastic Compute Cloud (Amazon EC2) instances using the CloudWatch Logs agent. Additionally, Amazon CloudWatch Logs can capture logs from AWS CloudTrail, Amazon Route 53 DNS Queries, VPC Flow Logs, Lambda functions, and other sources. You can then retrieve the associated log data from CloudWatch Logs.

Amazon VPC Flow Logs – VPC flow logs enable you to capture information about the IP traffic going to and from network interfaces in your VPC. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs. VPC flow logs can help you with a number of tasks. For example, you can use flow logs to troubleshoot why specific traffic is not reaching an instance, which can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic to your instance.

**AWS WAF Logs** – AWS WAF now supports full logging of all web requests that are inspected by the service. You can store these logs in Amazon S3 for compliance and auditing needs, as well as to use them for debugging and additional forensics. These logs help you to understand why certain rules are triggered and why certain web requests are blocked. You can also integrate the logs with your SIEM and log analysis tools.

Other AWS Logs – With the pace of innovation, we continue to deploy new features and capabilities for customers practically every day, which means that there are dozens of AWS services that provide logging and monitoring capabilities. For information about the features available for each AWS service, see the AWS documentation for that service.

# Visibility and Alerting

AWS Security Hub – AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. With Security Hub, you have a single place that aggregates, organizes, and prioritizes your security alerts or findings from multiple AWS services, such as Amazon GuardDuty, AnisoMospello Inflass Deene, ar Call Lyedo. AWS Partner solutions. Your findings are visually summarized on integrated dashboards with actionable graphs and tables. You can also continuously monitor your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows.

Amazon Gundothy e Amazos Guay existic prograph is rediscreptive price is it ontinuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers.

Guard Dttps://ificuspedies.inanazono.gomegiatei topa pengenatest/and uses machine learning to detect anomalies in account and workload activity. When a patential threat is detected, the service delivers a detailed security alert to the Guard Duty console and AWS Cloud Watch Events. This makes alerts actionable and easy to weach a least a detailed security alert to the Guard Duty console and AWS Cloud Watch Events. This makes alerts actionable and easy to weach a least a lea

Amazon Macie – Amazon Macie is an Al-powered security service that helps you prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in AWS. Amazon Macie uses machine learning to recognize sensitive data such as personally identifiable information (PII) or intellectual property, assign a business value, and provide visibility into where this data is stored and how it is being used in your organization. Amazon Macie continuously monitors data access activity for anomalies, and delivers alerts when it detects a risk of unauthorized access or inadvertent data leaks.

#### AWS Security Incident Response Guide AWS Technical Guide Automation

**AWS Config Rules** – An AWS Config Rule represents the preferred configurations for a resource and is evaluated against configuration changes on the relevant resources, as recorded by AWS Config. You can see the results of evaluating a rule against the configuration of a resource on a dashboard. Using Config Rules, you can assess your overall compliance and risk status from a configuration perspective, view compliance trends over time, and find which configuration change caused a resource to be out of compliance with a rule.

**AWS Trusted Advisor** – AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real time guidance to help you provision your resources by following AWS best practices. The full set of Trusted Advisor checks, including CloudWatch Events integration, is available to Business and Enterprise support plan customers.

Amazon CloudWatch – Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources, such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to get system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react accordingly and keep your application running smoothly.

**AWS Inspector** – Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available through the Amazon Inspector console or API.

Amazon Detective – Amazon Detective is a security service that automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations. Amazon Detective can analyze trillions of events from multiple data sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty, and automatically creates a unified, interactive view of your resources, users, and the interactions between them over time. With this unified view, you can visualize all the details and context in one place to identify the underlying reasons for the findings, drill down into relevant mitroical activities and culcivities and context.

### **Automation**

For the latest version of this document, visit:

AWS Lambda – AWS Lambda is a serverless compute service that runs your code in response to events,

AWS Lambda - AWS Lambda is a serverless compute service that runs your code in response to events, and automatically manages the underlying compute resources for you. You can use Lambda to extend other AWS services with custom logic, or create your own back-end services that operate at AWS scale, performance, and security. Lambda runs your code on high-availability compute infrastructure and performs all the administration of the compute resources for you. This includes server and operating system that the compute resources for you. This includes server and operating system that the compute resources for you. This includes server and operating system that the compute resources for you. This includes server and operating system that the code of the compute resources for you. This includes server and operating system that the code of the compute resources for you.

**AWS Step Functions** – AWS Step Functionales it easy to coordinate the components of distributed applications and microservices using visual workflows. Step Functions provides a graphical console for you to arrange and visualize the components of your application as a series of steps. This makes it simple to build and run multistep applications. Step Functions automatically triggers and tracks each step, and retries when there are errors, so your application executes in order and as expected.

Step Functions logs the state of each step, so when things do go wrong, you can diagnose and debug problems quickly. You can change and add steps without writing code, so you can easily evolve your

#### AWS Security Incident Response Guide AWS Technical Guide Secure Storage

application and innovate faster. AWS Step Functions is part of the AWS Serverless Platform, and makes it simple to orchestrate AWS Lambda functions for serverless applications. You can also use Step Functions for microservices orchestration using compute resources such as Amazon EC2 and Amazon ECS.

**AWS Systems Manager** – AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services, and enables you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. Systems Manager can keep your instances in their defined state, perform on-demand changes, such as updating applications or running shell scripts, and perform other automation and patching tasks.

# Secure Storage

Amazon S3 Glacier – Amazon S3 Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. It is designed to deliver 99.99999999999 durability, provides comprehensive security, and is designed to meet your regulatory requirements. Amazon S3 Glacier provides query-in-place functionality, which enables you to run powerful analytics directly on your archive data at rest. To keep costs low yet suitable for varying retrieval needs, Amazon S3 Glacier provides three options for access to archives, from a few minutes to several hours.

### Custom

The aforementioned spigewers in a so beem using his wells continuously adding new capabilities. For more information, we encourage you to review the What's New at AWS and AWS Cloud Security pages. In addition to the security services that AWS offers as native cloud services, you might be interested in building your own capabilities on top of AWS services.

Although we recommend enabling a base set of security services within your accounts, such as AWS Cloud Trail, Amazon Guard Duty, and Amazon Macle, you might eventually want to extend these capabilities to derive additional value from your log assets. There are a number of partner tools available, such as those listed in our APN Security Competency program. You might also want to write your own queries to search your logs. With the extensive number of managed services that AWS offers, this has never been easier. There are many additional AWS services that can assist you with investigation that are to inside the GOSs and is paper a constant of the constant of the

welcome.html

# Appendix B: Sample Code

# Example AWS CloudTrail Event

The following example shows that an IAM user named Alice used the AWS CLI to call the Amazon EC2 StopInstancesaction by using ec2-stop-instances.

```
{"Records": [{
   "eventVersion": "1.0",
   "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
       "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
   "eventTime": "2014-03-06T21:01:59Z",
   "eventSource": "ec2.amazonaws.com",
   "eventName": "StopInstances",
   "awsRegion": "us-east-2",
   "sourceIPAddress": "205.251.233.176",
   "userAgent": "ec2-api-tools 1.6.12.2",
   "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
   "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        "previous Litts version has been archived."
            "name": "running
   }]}}
}]}
```

For the latest version of this document, visit:

# **Example AWS CloudWatch Event**

The following of acousting the state of the following of

```
"check-name": "Exposed Access Keys",
"check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
```

#### AWS Security Incident Response Guide AWS Technical Guide Example Infrastructure Domain CLI Activities

```
"Fraud Type": "Exposed",
  "Location": "www.github.com"
},
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

# **Example Infrastructure Domain CLI Activities**

The following AWS CLI commands show an example of responding to an event within the infrastructure domain. This example uses the AWS APIs to perform many of the initial incident response activities described in this paper.

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address, Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group > aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name web-
asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-balancer-
name web-load-balancer
```

# # Create an EBS Ships version has been archived.

> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-REFERENCE-ID"

# # Create Fow the latestroers of this document, visit: > aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e

```
# Create a new EBS volume copy from the EBS snapshot

> awsheft create a new EBS volume copy from the EBS snapshot

> awsheft create a new EBS volume copy from the EBS snapshot

> awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot

| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS snapshot
| awsheft create a new EBS volume copy from the EBS volume copy from the EBS volume copy fr
```

```
# Attach the volume to the for  COMPLATION | Auto-instance | i-new4n6x --device | dev/sdf |
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port 0-65535 --source-group sg-1a2b3c4d
```

#### AWS Security Incident Response Guide AWS Technical Guide Example Infrastructure Domain CLI Activities

# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
Key=Environment,Value=Quarantine:REFERENCE-ID



For the latest version of this document, visit:

# Appendix C: Example Runbook

This following example runbook represents a single entry of a larger runbook. This runbook is unofficial and provided only as an example. As you craft your runbooks, each of your scenarios may evolve into larger items that have different beginnings and indicators of compromise, but all have similar outcomes or actions that need to be taken. Realizing this change can also open up other situations to better or more insightful responses.

# Incident Response Runbook – Root Usage

## Objective

The objective of this runbook is to provide specific guidance on how to manage Root AWS account usage. This runbook is not a substitute for an in-depth Incident Response strategy. This runbook focuses on the IR lifecycle:

- · Establish control.
- Determine impact.
- · Recover as needed.
- Investigate the root cause.
- · Improve.

The Indicators of Compromise (IOC), initial steps (stop the bleeding), and the detailed CLI commands needed to execute those steps are listed below.

## Assumptions version has been archived.

- CLI configured and installed.
- Reporting process is already in place.
- · Trusted For the tatest version of this document, visit:
- · Security Hub is active.

Indicators of Compromise <a href="https://docs.aws.amazon.com/whitepapers/latest/">https://docs.aws.amazon.com/whitepapers/latest/</a>

- Activity that is abnormal for the account aws-security-incident-response-guide/
  - Creation of IAM users.
- welcome.html
- CloudTrail turned off.
- · Cloudwatch turned off.
- SNS paused.
- · Step Functions paused.
- Launching of new or unexpected AMIs.
- Changes to the contacts on the account.

### Steps to Remediate – Establish Control

AWS documentation for a possible compromised account calls out the specific tasks listed below. The documentation for a possible compromised account can be found at: What do I do if I notice unauthorized activity in my AWS account?

- 1. Contact AWS Support and TAM as soon as possible.
- 2. Change and rotate Root password and add an MFA device associated with Root.
- 3. Rotate passwords, access/secret keys, and CLI commands relevant to remediation steps.
- 4. Review actions taken by the root user.
- 5. Open the runbooks for those actions.
- 6. Close incident.
- 7. Review the incident and understand what happened.
- 8. Fix the underlying issues, implement improvements, and update the runbook as needed.

### Further Action Items – Determine Impact

Review created items and mutating calls. There are may be items that have been created to allow access in the future. Some things to look at:

- · IAM Cross account roles.
- · IAM Users.
- S3 buckets.
- · EC2 instances.
- [Your application and infrastructure will drive this list.]

This version has been archived.

For the latest version of this document, visit:

# **Notices**

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.



For the latest version of this document, visit: