Konzepte und Verfahren von AMS Accelerate

AMS Accelerate-Benutzerhandbuch

Version October 3, 2025

AMS Accelerate-Benutzerhandbuch: Konzepte und Verfahren von AMS Accelerate

Table of Contents

Was ist AMS Accelerate?

Willkommen bei AMS Accelerate for Amazon Web Services (AWS). AMS Accelerate bietet eine Reihe von Betriebsdienstleistungen, die Sie dabei unterstützen, betriebliche Exzellenz zu erreichen AWS. Ganz gleich, ob Sie gerade erst mit der Cloud beginnen, Ihr derzeitiges Team erweitern möchten oder eine langfristige Betriebslösung benötigen, Accelerate kann Ihnen helfen, Ihre betrieblichen Ziele in der Cloud zu erreichen. Mithilfe einer AWS-Services Bibliothek von Automatisierungen, Konfigurationen und Runbooks bieten wir eine end-to-end betriebliche Lösung sowohl für neue als auch für bestehende Umgebungen. AWS

Der Accelerate-Service nutzt eine Reihe systemeigener Funktionen AWS-Services und bietet so umfassende Funktionen für das Infrastrukturmanagement. Im Rahmen dieser AWS-Services Funktionen erstellt und verwaltet Accelerate kuratierte Sätze von Überwachungskontrollen, Erkennungsleitplanken, Automatisierungen und Runbooks, um die Infrastruktur auf konforme und sichere Weise zu betreiben.

Themen

AMS-Betriebspläne

AWS Managed Services (AMS) ist mit zwei Betriebsplänen erhältlich: AMS Accelerate und AMS Advanced. Ein Betriebsplan bietet einen bestimmten Funktionsumfang und hat unterschiedliche Serviceniveaus, technische Fähigkeiten, Anforderungen, Preise und Einschränkungen. Unsere Betriebspläne bieten Ihnen die Flexibilität, für jede Ihrer AWS Workloads die Betriebskapazitäten auszuwählen, die am besten geeignet sind. In diesem Abschnitt werden die Funktionen und Unterschiede sowie die mit den einzelnen Plänen verbundenen Verantwortlichkeiten, Funktionen und Vorteile beschrieben, sodass Sie verstehen, welcher Betriebsplan für Ihre Kunden am besten geeignet ist.

Einen detaillierten Funktionsvergleich der beiden Betriebspläne finden Sie unter Funktionen von AWS Managed Services.

AMS Accelerate-Betriebsplan

AMS Accelerate ist der AMS-Betriebsplan, der Sie beim day-to-day Infrastrukturmanagement Ihrer neuen oder bestehenden AWS Umgebung unterstützt. AMS Accelerate bietet Betriebsdienstleistungen wie Überwachung, Vorfallmanagement und Sicherheit. AMS Accelerate bietet auch ein optionales Patch-Add-on für EC2 Amazon-basierte Workloads, die regelmäßig gepatcht werden müssen.

Mit AMS Accelerate entscheiden Sie, in welchen AWS-Konten AWS-Regionen AMS Accelerate betrieben werden soll, in welchen AWS-Regionen AMS Accelerate betrieben werden soll, welche Add-Ons Sie benötigen und welche Service Level Agreements (SLAs) Sie benötigen. Weitere Informationen finden Sie unter Verwenden des AMS Accelerate-Betriebsplans und in der Servicebeschreibung.

Erweiterter AMS-Betriebsplan

AMS Advanced bietet Services über den gesamten Lebenszyklus für die Bereitstellung, den Betrieb und den Support Ihrer Infrastruktur. Zusätzlich zu den von AMS Accelerate bereitgestellten Betriebsdiensten umfasst AMS Advanced auch zusätzliche Dienste wie Landezonenmanagement, Infrastrukturänderungen und -bereitstellung, Zugriffsmanagement und Endpunktsicherheit.

AMS Advanced stellt eine landing zone bereit, in die Sie Ihre AWS Workloads migrieren und AMS-Betriebsdienste in Anspruch nehmen können. Unsere verwalteten Landezonen mit mehreren Konten sind mit der Infrastruktur vorkonfiguriert, um Authentifizierung, Sicherheit, Vernetzung und Protokollierung zu erleichtern.

AMS Advanced umfasst auch ein Änderungs- und Zugriffsmanagementsystem, das Ihre Workloads schützt, indem es unbefugten Zugriff oder die Implementierung riskanter Änderungen an Ihrer Infrastruktur verhindert. AWS Kunden müssen mithilfe unseres Change-Management-Systems eine Änderungsanforderung (RFC) erstellen, um die meisten Änderungen in Ihren AMS Advanced-Konten zu implementieren. Sie erstellen RFCs aus einer Bibliothek automatisierter Änderungen, die von unseren Sicherheits- und Betriebsteams vorab geprüft wurden, oder fordern manuelle Änderungen an, die von unserem Betriebsteam geprüft und implementiert werden, wenn sie sowohl als sicher erachtet werden als auch von AMS Advanced unterstützt werden.

Verwenden des AMS Accelerate-Betriebsplans

AMS Accelerate ist der AMS-Betriebsplan, mit dem die AWS-Infrastruktur betrieben werden kann, die Workloads unterstützt. Unabhängig davon, ob sich Ihre Workloads bereits in einem AWS-Konto befinden oder Sie planen, neue zu migrieren, können Sie von den Betriebsservices von AMS Accelerate wie Überwachung und Warnung, Vorfallmanagement, Sicherheitsmanagement und Backup-Management profitieren, ohne eine neue Migration durchführen zu müssen, Ausfallzeiten zu haben oder Ihre AWS-Nutzung zu ändern. AMS Accelerate bietet auch ein optionales Patch-Add-on für EC2 basierte Workloads, die regelmäßig gepatcht werden müssen.

Mit AMS Accelerate haben Sie die Freiheit, alle AWS-Services nativ oder mit Ihren bevorzugten Tools zu verwenden, zu konfigurieren und bereitzustellen. Sie können Ihre bestehenden Zugriffs- und Änderungsmechanismen weiterhin nutzen, während AMS konsequent bewährte Verfahren anwendet, die Ihnen helfen, Ihr Team zu skalieren, Kosten zu optimieren, Sicherheit und Effizienz zu erhöhen und die Ausfallsicherheit zu verbessern.

AMS Accelerate kann Ihren Betrieb zwar vereinfachen, aber Sie sind weiterhin für Anwendungsentwicklung, Bereitstellung, Test und Tuning sowie Verwaltung verantwortlich. AMS Accelerate nimmt nur aufgrund von Vorfällen, Alarmen, Problembehebungen und einigen Serviceanfragen Änderungen an Ihrem Konto vor. AMS Accelerate stellt in Ihrem Namen keine Ressourcen auf dem Konto bereit. AMS Accelerate bietet Unterstützung bei der Behebung von Infrastrukturproblemen, die sich auf Anwendungen auswirken. AMS Accelerate greift jedoch ohne Ihr Wissen und Ihre Zustimmung nicht auf Ihre Anwendungskonfigurationen zu oder validiert diese. Die Services und Änderungen von AMS Accelerate werden direkt in der AWS Konsole bereitgestellt APIs, sodass Sie Ihre bestehenden Konten weiterhin mit AWS den verfügbaren AWS-Marketplace-Lösungen nutzen können. AMS Accelerate ändert keinen Code in Ihren infrastructure-as-code Vorlagen (z. B. CloudFormation Vorlagen), kann Ihre Teams jedoch darüber informieren, welche Änderungen erforderlich sind, um die besten Betriebs- und Sicherheitspraktiken einzuhalten.

Die wichtigsten Begriffe von AMS

- AMS Advanced: Die im Abschnitt „Servicebeschreibung“ der AMS Advanced-Dokumentation beschriebenen Dienste. Siehe Servicebeschreibung.
- AMS Advanced-Konten: AWS Konten, die jederzeit alle Anforderungen der AMS Advanced Onboarding Requirements erfüllen. Informationen zu den Vorteilen von AMS Advanced, Fallstudien und zur Kontaktaufnahme mit einem Vertriebsmitarbeiter finden Sie unter AWS Managed Services.

- AMS Accelerate-Konten: AWS Konten, die jederzeit alle Anforderungen der AMS Accelerate Onboarding-Anforderungen erfüllen. Siehe Erste Schritte mit AMS Accelerate.
- AWS Managed Services: AMS und/oder AMS Accelerate.
- AWS Managed Services Services-Konten: Die AMS-Konten und/oder AMS Accelerate-Konten.
- Kritische Empfehlung: Eine Empfehlung, die im AWS Rahmen einer Serviceanfrage ausgesprochen wurde und Sie darüber informiert, dass Ihre Maßnahmen zum Schutz vor potenziellen Risiken oder Störungen Ihrer Ressourcen oder der AWS-Services Wenn Sie sich entscheiden, einer kritischen Empfehlung bis zum angegebenen Datum nicht zu folgen, tragen Sie die alleinige Verantwortung für alle Schäden, die sich aus Ihrer Entscheidung ergeben.
- Vom Kunden angeforderte Konfiguration: Jede Software, Dienste oder andere Konfigurationen, die nicht identifiziert sind in:
  - Beschleunigen: Unterstützte Konfigurationen oder AMS Accelerate; Servicebeschreibung.
  - AMS Advanced: Unterstützte Konfigurationen oder AMS Advanced; Servicebeschreibung.
- Kommunikation mit einem Vorfall: AMS teilt Ihnen einen Incident mit oder Sie beantragen einen Incident bei AMS über einen Incident, der im Support Center für AMS Accelerate und in der AMS Console for AMS erstellt wurde. Die AMS Accelerate Console bietet eine Zusammenfassung der Vorfälle und Serviceanfragen auf dem Dashboard sowie Links zum Support Center für weitere Informationen.
- Verwaltete Umgebung: Die AMS Advanced-Konten und/oder die AMS Accelerate-Konten, die von AMS betrieben werden.

  Für AMS Advanced gehören dazu Multi-Account-Landingzone-Konten (MALZ) und Single-Account-Landingzone-Konten (SALZ).
- Startdatum der Abrechnung: Der nächste Werktag nach Erhalt AWS der in der AWS Managed Services Onboarding-E-Mail angeforderten Informationen. Die AWS Managed Services Onboarding-E-Mail bezieht sich auf die E-Mail, die von Ihnen gesendet wird AWS , um die Informationen zu sammeln, die für die Aktivierung von AWS Managed Services auf Ihren Konten erforderlich sind.

  Für Konten, die später von Ihnen registriert wurden, ist das Startdatum der Rechnungsstellung der nächste Tag, an dem AWS Managed Services eine Benachrichtigung über die Aktivierung von AWS Managed Services für das registrierte Konto gesendet hat. Eine Benachrichtigung zur Aktivierung von AWS Managed Services erfolgt in folgenden Fällen:

  1. Sie gewähren Zugriff auf ein kompatibles AWS Konto und übergeben es an AWS Managed Services.

2. AWS Managed Services entwirft und erstellt das AWS Managed Services Services-Konto.

- Kündigung des Dienstes: Sie können die AWS Managed Services für alle AWS Managed Services Services-Konten oder für ein bestimmtes AWS Managed Services Services-Konto aus beliebigem Grund kündigen, indem Sie eine Serviceanfrage mit einer Frist von AWS mindestens 30 Tagen angeben. Am Tag der Kündigung des Service können Sie entweder:
  1. AWS übergibt Ihnen die Kontrolle über alle AWS Managed Services Services-Konten oder gegebenenfalls die angegebenen AWS Managed Services Services-Konten oder
  2. Die Parteien entfernen die AWS Identity and Access Management Rollen, die AWS Zugriff gewähren, von allen AWS Managed Services Services-Konten oder den angegebenen AWS Managed Services Services-Konten, sofern zutreffend.
- Kündigungsdatum des Dienstes: Das Kündigungsdatum des Dienstes ist der letzte Tag des Kalendermonats, der auf das Ende der 30-tägigen Kündigungsfrist folgt. Fällt das Ende der erforderlichen Kündigungsfrist nach dem 20. Tag des Kalendermonats, ist das Kündigungsdatum der letzte Tag des folgenden Kalendermonats. Im Folgenden finden Sie Beispielszenarien für Kündigungstermine.
  - Wenn die Kündigung am 12. April erfolgt, endet die Kündigungsfrist von 30 Tagen am 12. Mai. Das Kündigungsdatum des Dienstes ist der 31. Mai.
  - Wenn am 29. April eine Kündigungsfrist erteilt wird, endet die Kündigungsfrist von 30 Tagen am 29. Mai. Das Kündigungsdatum des Dienstes ist der 30. Juni.
- Bereitstellung von AWS Managed Services: AWS stellt Ihnen die AWS Managed Services zur Verfügung und Sie können ab dem Startdatum des Services für jedes AWS Managed Services-Konto auf AWS Managed Services zugreifen und diese nutzen.
- Kündigung für bestimmte AWS Managed Services-Konten: Sie können die AWS Managed Services für ein bestimmtes AWS Managed Services Services-Konto aus beliebigem Grund kündigen, indem AWS Sie dies durch eine Serviceanfrage („Anfrage zur Kündigung eines AMS-Kontos“) mitteilen.

Bedingungen für das Incident-Management:

- Ereignis: Eine Änderung in Ihrer AMS-Umgebung.
- Warnung: Immer wenn ein unterstütztes Ereignis einen Schwellenwert AWS-Service überschreitet und einen Alarm auslöst, wird eine Warnung erstellt und eine Benachrichtigung an Ihre Kontaktliste gesendet. Darüber hinaus wird ein Vorfall in Ihrer Incident-Liste erstellt.

- Vorfall: Eine ungeplante Unterbrechung oder Leistungsverschlechterung Ihrer AMS-Umgebung oder AWS Managed Services, die zu einer von AWS Managed Services oder Ihnen gemeldeten Beeinträchtigung führt.
- Problem: Eine gemeinsame Grundursache für einen oder mehrere Vorfälle.
- Lösung eines Vorfalls oder Lösung eines Vorfalls:
  - AMS hat alle nicht verfügbaren AMS-Dienste oder -Ressourcen im Zusammenhang mit diesem Vorfall wieder in den verfügbaren Zustand versetzt, oder
  - AMS hat festgestellt, dass nicht verfügbare Stacks oder Ressourcen nicht auf einen verfügbaren Zustand zurückgesetzt werden können, oder
  - AMS hat eine von Ihnen autorisierte Wiederherstellung der Infrastruktur eingeleitet.
- Reaktionszeit bei Vorfällen: Der Zeitunterschied zwischen dem Zeitpunkt, zu dem Sie einen Vorfall erstellen, und dem Zeitpunkt, zu dem AMS eine erste Antwort über die Konsole, E-Mail, das Service Center oder das Telefon bereitstellt.
- Zeit zur Behebung eines Vorfalls: Der Zeitunterschied zwischen dem Zeitpunkt, zu dem entweder AMS oder Sie einen Vorfall auslösen, und dem Zeitpunkt, zu dem der Vorfall behoben wird.
- Priorität des Vorfalls: Wie Vorfälle von AMS oder von Ihnen als „Niedrig“, „Mittel“ oder „Hoch“ priorisiert werden.
  - Niedrig: Ein unkritisches Problem mit Ihrem AMS-Service.
  - Medium: Ein AWS-Service in Ihrer verwalteten Umgebung ist verfügbar, funktioniert aber nicht wie vorgesehen (gemäß der entsprechenden Servicebeschreibung).
  - Hoch: Entweder (1) die AMS-Konsole oder ein oder mehrere AMS APIs in Ihrer verwalteten Umgebung sind nicht verfügbar; oder (2) ein oder mehrere AMS-Stacks oder Ressourcen in Ihrer verwalteten Umgebung sind nicht verfügbar und die Nichtverfügbarkeit verhindert, dass Ihre Anwendung ihre Funktion erfüllt.

  AMS kann Vorfälle gemäß den oben genannten Richtlinien neu kategorisieren.
- Wiederherstellung der Infrastruktur: Erneutes Bereitstellen vorhandener Stacks auf der Grundlage von Vorlagen der betroffenen Stacks und Initiierung einer Datenwiederherstellung auf der Grundlage des letzten bekannten Wiederherstellungspunkts, sofern von Ihnen nicht anders angegeben, wenn eine Behebung des Vorfalls nicht möglich ist.

Bedingungen für die Infrastruktur:

- Verwaltete Produktionsumgebung: Ein Kundenkonto, in dem sich die Produktionsanwendungen des Kunden befinden.
- Verwaltete Nichtproduktionsumgebung: Ein Kundenkonto, das nur Anwendungen enthält, die nicht zur Produktion gehören, z. B. Anwendungen für Entwicklung und Tests.
- AMS-Stack: Eine Gruppe von einer oder mehreren AWS Ressourcen, die von AMS als eine Einheit verwaltet werden.
- Unveränderliche Infrastruktur: Ein für Amazon EC2 Auto Scaling Scaling-Gruppen (ASGs) typisches Infrastrukturwartungsmodell, bei dem aktualisierte Infrastrukturkomponenten (im AWS AMI) bei jeder Bereitstellung ersetzt werden, anstatt direkt aktualisiert zu werden. Die Vorteile einer unveränderlichen Infrastruktur bestehen darin, dass alle Komponenten synchron bleiben, da sie immer auf derselben Basis generiert werden. Die Unveränderlichkeit ist unabhängig von einem Tool oder Workflow zum Erstellen des AMI.
- Veränderbare Infrastruktur: Ein Infrastrukturwartungsmodell, das typisch für Stacks ist, die keine Amazon EC2 Auto Scaling Scaling-Gruppen sind und eine einzelne Instance oder nur wenige Instances enthalten. Dieses Modell entspricht am ehesten der traditionellen, hardwarebasierten Systembereitstellung, bei der ein System zu Beginn seines Lebenszyklus bereitgestellt wird und dann im Laufe der Zeit Updates auf dieses System übertragen werden. Alle Aktualisierungen des Systems werden einzeln auf die Instanzen angewendet und können aufgrund von Anwendungs- oder Systemneustarts zu Systemausfällen führen (abhängig von der Stack-Konfiguration).
- Sicherheitsgruppen: Virtuelle Firewalls für Ihre Instance zur Steuerung des ein- und ausgehenden Datenverkehrs. Sicherheitsgruppen wirken auf der Instance-Ebene und nicht auf der Subnetzebene. Daher kann jeder Instance in einem Subnetz in Ihrer VPC ein anderer Satz von Sicherheitsgruppen zugewiesen werden.
- Service Level Agreements (SLAs): Teil der AMS-Verträge mit Ihnen, die das erwartete Serviceniveau definieren.
- SLA nicht verfügbar und nicht verfügbar:
  - Eine von Ihnen eingereichte API-Anfrage, die zu einem Fehler führt.
  - Eine von Ihnen eingereichte Konsolenanfrage, die zu einer 5xx-HTTP-Antwort führt (der Server ist nicht in der Lage, die Anfrage auszuführen).
  - Alle AWS-Service Angebote, die Stacks oder Ressourcen in Ihrer von AMS verwalteten Infrastruktur bilden, befinden sich im Status „Serviceunterbrechung“, wie im Service Health Dashboard angezeigt.
  - Die Nichtverfügbarkeit, die direkt oder indirekt auf einen AMS-Ausschluss zurückzuführen ist, wird bei der Entscheidung über die Inanspruchnahme von Servicegutschriften

nicht berücksichtigt. Dienste gelten als verfügbar, sofern sie nicht die Kriterien für die Nichtverfügbarkeit erfüllen.

- Servicelevel-Ziele (SLOs): Teil der AMS-Verträge mit Ihnen, in denen spezifische Serviceziele für AMS-Services definiert werden.

Bedingungen für das Patchen:

- Obligatorische Patches: Wichtige Sicherheitsupdates zur Behebung von Problemen, die den Sicherheitsstatus Ihrer Umgebung oder Ihres Kontos gefährden könnten. Ein „Kritisches Sicherheitsupdate“ ist ein Sicherheitsupdate, das vom Hersteller eines AMS-unterstützten Betriebssystems als „Kritisch“ eingestuft wird.
- Angekündigte oder veröffentlichte Patches: Patches werden in der Regel nach einem bestimmten Zeitplan angekündigt und veröffentlicht. Neue Patches werden angekündigt, wenn festgestellt wird, dass der Patch benötigt wird. In der Regel wird der Patch bald danach veröffentlicht.
- Patch-Add-on: Tag-basiertes Patchen für AMS-Instances, das die AWS Systems Manager (SSM) -Funktionalität nutzt, sodass Sie Instances taggen und diese Instances mithilfe einer Baseline und eines von Ihnen konfigurierten Fensters patchen lassen können.
- Patch-Methoden:
  - In-Place-Patching: Patchen, das durch Ändern vorhandener Instanzen erfolgt.
  - AMI-Ersatz-Patching: Patching, das durch Ändern des AMI-Referenzparameters einer vorhandenen EC2 Auto Scaling Scaling-Gruppenstartkonfiguration erfolgt.
- Patch-Anbieter (Betriebssystemanbieter, Drittanbieter): Patches werden vom Anbieter oder vom zuständigen Gremium der Anwendung bereitgestellt.
- Patch-Typen:
  - Kritisches Sicherheitsupdate (CSU): Ein Sicherheitsupdate, das vom Hersteller eines unterstützten Betriebssystems als „Kritisch“ eingestuft wurde.
  - Wichtiges Update (IU): Ein Sicherheitsupdate, das vom Hersteller eines unterstützten Betriebssystems als „wichtig“ eingestuft wurde, oder ein nicht sicherheitsrelevantes Update, das vom Hersteller eines unterstützten Betriebssystems als „Kritisch“ eingestuft wurde.
  - Anderes Update (OU): Ein Update des Herstellers eines unterstützten Betriebssystems, bei dem es sich nicht um eine CSU oder eine IU handelt.
- Unterstützte Patches: AMS unterstützt Patches auf Betriebssystemebene. Upgrades werden vom Anbieter veröffentlicht, um Sicherheitslücken oder andere Fehler zu beheben oder die Leistung

zu verbessern. Eine Liste der derzeit unterstützten OSs Konfigurationen finden Sie unter Support-Konfigurationen.

Sicherheitsbedingungen:

- Detective Controls: Eine Bibliothek mit von AMS erstellten oder aktivierten Monitoren, die einen kontinuierlichen Überblick über vom Kunden verwaltete Umgebungen und Workloads für Konfigurationen bieten, die nicht den Sicherheits-, Betriebs- oder Kundenkontrollen entsprechen, und Maßnahmen ergreifen, indem sie Eigentümer benachrichtigen, Ressourcen proaktiv ändern oder beenden.

Bedingungen für Serviceanfragen:

- Serviceanfrage: Eine Anfrage von Ihnen nach einer Maßnahme, die AMS in Ihrem Namen ergreifen soll.
- Warnmeldung: Eine Benachrichtigung, die von AMS auf Ihrer Seite mit der Liste der Serviceanfragen veröffentlicht wird, wenn eine AMS-Warnung ausgelöst wird. Der für Ihr Konto konfigurierte Kontakt wird ebenfalls über die konfigurierte Methode (z. B. E-Mail) benachrichtigt. Wenn Ihre Instanzen/Ressourcen Kontakt-Tags enthalten und Ihrem Cloud Service Delivery Manager (CSDM) Ihre Zustimmung für tagbasierte Benachrichtigungen erteilt haben, werden die Kontaktinformationen (Schlüsselwert) im Tag auch bei automatisierten AMS-Benachrichtigungen benachrichtigt.
- Servicebenachricht: Eine Mitteilung von AMS, die auf Ihrer Seite mit der Liste Ihrer Serviceanfragen veröffentlicht wird.

Verschiedene Bedingungen:

- AWS Managed Services-Schnittstelle: Für AMS: Die AWS Managed Services Advanced Console, AMS CM API und Support API. Für AMS Accelerate: Die Support Konsole und die Support API.
- Kundenzufriedenheit (CSAT): AMS CSAT verfügt über umfassende Analysen, darunter Bewertungen der Fallkorrespondenz zu jedem Fall oder jeder etwaigen Korrespondenz, vierteljährliche Umfragen usw.
- DevOps: DevOps ist eine Entwicklungsmethodik, die sich nachdrücklich für Automatisierung und Überwachung aller Schritte einsetzt. DevOps zielt auf kürzere Entwicklungszyklen, eine höhere Bereitstellungshäufigkeit und zuverlässigere Releases ab, indem die traditionell getrennten Funktionen von Entwicklung und Betrieb auf einer Grundlage der Automatisierung

zusammengeführt werden. Wenn Entwickler den Betrieb verwalten können und der Betrieb die Entwicklung beeinflusst, können Probleme und Probleme schneller entdeckt und gelöst werden, und Geschäftsziele lassen sich leichter erreichen.

- ITIL: Die Information Technology Infrastructure Library (ITIL genannt) ist ein ITSM-Framework, mit dem der Lebenszyklus von IT-Services standardisiert werden soll. ITIL ist in fünf Phasen unterteilt, die den IT-Servicelebenszyklus abdecken: Servicestrategie, Servicedesign, Serviceübergang, Servicebetrieb und Serviceverbesserung.
- IT-Servicemanagement (ITSM): Eine Reihe von Praktiken, die IT-Services auf die Bedürfnisse Ihres Unternehmens abstimmen.
- Managed Monitoring Services (MMS): AMS betreibt sein eigenes Überwachungssystem, den Managed Monitoring Service (MMS), das AWS Gesundheitsereignisse verarbeitet und CloudWatch Amazon-Daten sowie Daten von anderen aggregiert und AMS-Betreiber (rund um die Uhr online) über alle Alarme informiert AWS-Services, die über ein Amazon Simple Notification Service (Amazon SNS) -Thema ausgelöst wurden.
- Namespace: Wenn Sie IAM-Richtlinien erstellen oder mit Amazon Resource Names (ARNs) arbeiten, identifizieren Sie einen AWS-Service mithilfe eines Namespace. Sie verwenden Namespaces bei der Identifikation von Aktionen und Ressourcen.

Service description (Service-Beschreibung)

AMS Accelerate ist ein Betriebsplan des AWS Managed Services Services-Service zur Verwaltung des Betriebs Ihrer AWS Infrastruktur.

Funktionen des AMS Accelerate-Betriebsplans von AWS Managed Services (AMS)

AMS Accelerate bietet die folgenden Funktionen:

- Verwaltung von Vorfällen:

  Incident Management ist der Prozess, mit dem der AMS-Service auf Ihre gemeldeten Vorfälle reagiert.

  AMS Accelerate erkennt und reagiert proaktiv auf Vorfälle und unterstützt Ihr Team bei der Lösung von Problemen. Über das AWS Support Center können Sie sich rund um die Uhr an die Betriebstechniker von AMS Accelerate wenden. Die Reaktionszeit SLAs hängt von der Antwortstufe ab, die Sie für Ihr Konto ausgewählt haben.

- Monitoring: (Überwachung:)

  Überwachung ist der Prozess, den der AMS-Service verwendet, um Ihre Ressourcen zu verfolgen.

  Konten, die bei AMS Accelerate registriert sind, sind mit einer Basisbereitstellung von CloudWatch Amazon-Ereignissen und -Alarmen konfiguriert, die optimiert wurden, um Störgeräusche zu reduzieren und mögliche bevorstehende Vorfälle zu identifizieren. Nach Erhalt der Benachrichtigungen setzt das AMS-Team automatisierte Abhilfemaßnahmen, Mitarbeiter und Prozesse ein, um die Ressourcen wieder in einen gesunden Zustand zu versetzen und gegebenenfalls mit Ihren Teams in Kontakt zu treten, um Einblicke in die Erkenntnisse über das Verhalten zu gewinnen und zu verhindern. Schlägt die Behebung fehl, startet AMS den Incident-Management-Prozess. Sie können die Baselines ändern, indem Sie die Standardkonfigurationsdatei aktualisieren.

- Sicherheit:

  Sicherheitsmanagement ist der Prozess, den der AMS-Service verwendet, um Ihre Ressourcen zu schützen. AWS Managed Services schützt Ihre Informationsressourcen und trägt dazu bei, Ihre AWS-Infrastruktur zu schützen, indem mehrere Kontrollen verwendet werden, darunter AWS Config Rules und Amazon GuardDuty.

  AMS Accelerate unterhält eine Sammlung von Maßnahmen AWS-Config-Regeln und Problembehebungsmaßnahmen, um sicherzustellen, dass all Ihre Konten den Industriestandards für Sicherheit und Betriebsintegrität entsprechen. AWS-Config-Regeln verfolgt kontinuierlich die Konfigurationsänderung Ihrer aufgezeichneten Ressourcen. Wenn eine Änderung gegen Regelbedingungen verstößt, meldet AMS die Ergebnisse und ermöglicht es Ihnen, Verstöße je nach Schweregrad des Verstoßes automatisch oder auf Anfrage zu beheben. AWS-Config-Regeln die Einhaltung der Standards erleichtern, die vom Center for Internet Security (CIS), dem National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), dem Health Insurance Portability and Accountability Act (HIPAA) und dem Payment Card Industry (PCI) Data Security Standard (DSS) festgelegt wurden.

  Darüber hinaus nutzt AMS Accelerate Amazon, GuardDuty um potenziell unautorisierte oder böswillige Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. GuardDuty Die Ergebnisse werden rund um die Uhr von AMS überwacht. AMS arbeitet mit Ihnen zusammen, um die Auswirkungen der Ergebnisse und Abhilfemaßnahmen auf der Grundlage von Best-Practice-Empfehlungen zu verstehen. AMS unterstützt Amazon Macie auch dabei, Ihre sensiblen Daten wie persönliche Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII) und Finanzdaten zu schützen. Schließlich überwacht und bewertet AMS alle Amazon Route 53 Resolver ALERT - und

BLOCK-Ereignisse, die in verwalteten Konten generiert wurden, um den Netzwerkverkehr weiter zu untersuchen und seine Erkennungsfunktionen zu erweitern.

- Patch-Verwaltung:

  Patch-Management ist der Prozess, mit dem der AMS-Service Ihre Ressourcen aktualisiert.

  Für ein AWS Konto mit dem Patch-Add-on wendet AWS Managed Services während der von Ihnen ausgewählten Wartungsfenster Anbieter-Updates für EC2 Amazon-Instances für unterstützte Betriebssysteme an und installiert diese. AMS erstellt vor dem Patchen einen Snapshot der Instance, überwacht die Patch-Installation und benachrichtigt Sie über das Ergebnis. Wenn der Patch fehlschlägt, untersucht AMS den Fehler und empfiehlt Ihnen eine Vorgehensweise zur Behebung des Problems. Oder AMS stellt die Instance auf Anfrage auf Rollback wieder her. AMS erstellt Berichte über den Umfang der Patch-Compliance und berät Sie über die empfohlene Vorgehensweise für Ihr Unternehmen.

- Backup-Verwaltung:

  AMS verwendet Backup-Management, um Schnappschüsse Ihrer Ressourcen zu erstellen.

  AWS Managed Services erstellt, überwacht und speichert Snapshots für AWS Services, die von AWS Backup unterstützt werden. Sie definieren die Backup-Zeitpläne, die Häufigkeit und den Aufbewahrungszeitraum, indem Sie beim Onboarding von Konten und Anwendungen AWS Backup Pläne erstellen. Sie ordnen die Pläne Ressourcen zu. AMS verfolgt alle Backup-Jobs und benachrichtigt unser Team, wenn ein Backup-Job fehlschlägt, eine Problembehebung durchzuführen. AMS nutzt Ihre Snapshots, um bei Bedarf Wiederherstellungsmaßnahmen bei Vorfällen durchzuführen. AMS stellt Ihnen einen Bericht über den Umfang der Backups und einen Bericht über den Status der Backups zur Verfügung.

- Problemmanagement:

  AMS führt Trendanalysen durch, um Probleme zu identifizieren und zu untersuchen und die Ursache zu ermitteln. Probleme werden entweder durch eine Behelfslösung oder durch eine dauerhafte Lösung behoben, die ein erneutes Auftreten ähnlicher future Auswirkungen auf den Service verhindert. Sobald das Problem behoben ist, kann für jeden Vorfall mit hoher Wahrscheinlichkeit ein Bericht nach dem Vorfall (PIR) angefordert werden. Der PIR erfasst die Grundursache und die ergriffenen Präventivmaßnahmen, einschließlich der Umsetzung präventiver Maßnahmen.

- Benannte Experten:

AMS Accelerate benennt außerdem einen Cloud Service Delivery Manager (CSDM) und einen Cloud Architect (CA), die mit Ihrem Unternehmen zusammenarbeiten und die betriebliche und sicherheitstechnische Exzellenz fördern. Ihr CSDM und Ihre CA stehen Ihnen während und nach der Konfiguration und dem Onboarding von AMS Accelerate beratend zur Seite, erstellen einen monatlichen Bericht über Ihre Betriebskennzahlen und arbeiten mit Ihnen zusammen, um mithilfe von Tools wie AWS Cost Explorer, Kosten- und Nutzungsberichten und mögliche Kosteneinsparungen zu ermitteln. Trusted Advisor

- Tools für den Betrieb:

  AMS Accelerate kann den laufenden Betrieb der Infrastruktur Ihres Workloads in AWS sicherstellen. Unsere Patch-, Backup-, Überwachungs- und Incident-Management-Services hängen davon ab, dass Ressourcen markiert sind und dass die AWS Systems Manager (SSM) und CloudWatch Agenten auf Ihren EC2 Amazon-Instances mit einem IAM-Instance-Profil installiert und konfiguriert sind, das sie zur Interaktion mit dem SSM und den Amazon-Services autorisiert. CloudWatch AMS Accelerate bietet Tools wie Resource Tagger, mit denen Sie Ihre Ressourcen anhand von Regeln taggen können, und eine automatisierte Instance-Konfiguration, um die erforderlichen Agenten in Ihren EC2 Amazon-Instances zu installieren. Wenn Sie sich an unveränderliche Infrastrukturpraktiken halten, können Sie die Voraussetzungen direkt in der Konsole oder infrastructure-as-code in den Vorlagen erfüllen.

- Kostenoptimierung:

  AMS Resource Scheduler automatisiert das Starten und Stoppen von Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Amazon Relational Database Service (Amazon RDS) -Instances und Amazon EC2 Auto Scaling Scaling-Gruppen. AMS Resource Scheduler hilft Ihnen dabei, die Betriebskosten zu senken, indem die Ressourcen, die nicht genutzt werden, gestoppt und wieder gestartet werden, wenn ihre Kapazität benötigt wird.

- Protokollierung und Berichterstattung:

  AWS Managed Services aggregiert und speichert Protokolle, die als Ergebnis von Vorgängen in CloudWatch CloudTrail, und Amazon VPC Flow Logs generiert wurden. Die Protokollierung von AMS hilft bei der schnelleren Behebung von Vorfällen und bei Systemprüfungen. AMS Accelerate stellt Ihnen außerdem einen monatlichen Servicebericht zur Verfügung, der die wichtigsten Leistungskennzahlen von AMS zusammenfasst, darunter eine Zusammenfassung und Einblicke, betriebliche Kennzahlen, verwaltete Ressourcen, Einhaltung der AMS Service Level Agreements (SLA) und Finanzkennzahlen zu Ausgaben, Einsparungen und Kostenoptimierung. Die Berichte werden von dem für Sie bestimmten AMS Cloud Service Delivery Manager (CSDM) bereitgestellt.

- Verwaltung von Serviceanfragen:

  Um Informationen über Ihre verwaltete Umgebung, AMS oder AWS Serviceangebote anzufordern, reichen Sie Serviceanfragen über die AMS Accelerate-Konsole ein. Sie können eine Serviceanfrage mit Anleitungen zu AWS Diensten und Funktionen oder zur Anforderung zusätzlicher AMS-Services einreichen.

Alle AMS Accelerate-Kunden beginnen mit Vorfallmanagement, Überwachung, Sicherheitsüberwachung, Protokollaufzeichnung, erforderlichen Tools, Backup-Management und Berichtsfunktionen. Sie können das AMS-Patch-Management-Add-on gegen einen Aufpreis hinzufügen.

> **Note**
>
> Eine Liste der Funktionen, die in nicht unterstützt werden AWS GovCloud (US), finden Sie unter So unterscheidet sich AMS Accelerate von AWS GovCloud (US)

Unterstützte Konfigurationen

AMS Accelerate unterstützt die folgenden Konfigurationen:

- Sprache: Englisch.
- Regionen: Die von AWS Managed Services unterstützten AWS Regionen finden Sie auf der AWS Regional Services-Webseite.

> **Note**
>
> AWS-Regionen, die vor dem 20. März 2019 eingeführt wurden, gelten als „ursprüngliche“ Regionen und sind standardmäßig aktiviert. Regionen, die nach diesem Datum eingeführt wurden, sind „Opt-In“ -Regionen und sind standardmäßig deaktiviert. Wenn Ihr Konto mehrere Regionen verwendet und Sie AMS Accelerate für ein Konto mit einer aktivierten „Opt-In“ -Region als Standardregion einbinden, ist die AMS-Berichtsfunktion nur in dieser Region verfügbar. Wenn Sie keine Standardregion festlegen, ist die zuletzt besuchte Region Ihre Standardregion.
> Informationen zum Aktivieren einer Region finden Sie unter Region aktivieren.
> Informationen zum Festlegen einer Standardregion finden Sie unter Region auswählen.

Eine Liste des Opt-in-Status für jede Region finden Sie unter Verfügbare Regionen im Amazon Elastic Compute Cloud-Benutzerhandbuch.

- Betriebssystemarchitektur (x86-64 oder ARM64): jede, die sowohl von Systems Manager als auch unterstützt wird. CloudWatch
- Unterstützte Betriebssysteme:
  - AlmaLinux 8.3-8.9, 9.x (AlmaLinux wird nur mit der x86-Architektur unterstützt)
  - Amazon Linux 2023
  - Amazon Linux 2 (voraussichtliches Enddatum des AMS-Supports am 30. Juni 2026)
  - Oracle Linux 9.x, 8.x
  - RedHat Enterprise Linux (RHEL) 9.x, 8.x
  - SUSE Linux Enterprise Server 15 SP6
  - SUSE Linux Enterprise Server für SAP 15 SP3 und höher
  - Microsoft Windows Server 2022, 2019, 2016
  - Ubuntu 20.04, 22.04, 24.04
- Unterstützte Betriebssysteme mit End of Support (EOS):

> **Note**
>
> Betriebssysteme mit Ende des Support (EOS) laufen außerhalb des allgemeinen Supportzeitraums des Betriebssystemherstellers und bergen ein erhöhtes Sicherheitsrisiko. EOS-Betriebssysteme gelten nur dann als unterstützte Konfigurationen, wenn für AMS erforderliche Agenten das Betriebssystem unterstützen und...
>
> 1. Sie haben einen erweiterten Support mit dem Betriebssystemanbieter abgeschlossen, der es Ihnen ermöglicht, Updates zu erhalten, oder
> 2. alle Instanzen, die ein EOS-Betriebssystem verwenden, befolgen die von AMS im Accelerate-Benutzerhandbuch angegebenen Sicherheitskontrollen, oder
> 3. Sie halten sich an alle anderen von AMS geforderten ausgleichenden Sicherheitskontrollen.
>
> Falls AMS ein EOS-Betriebssystem nicht mehr unterstützen kann, gibt AMS eine kritische Empfehlung zur Aktualisierung des Betriebssystems ab.

Zu den für AMS erforderlichen Agenten gehören unter anderem: Amazon AWS Systems Manager CloudWatch, Endpoint Security (EPS) -Agent und Active Directory (AD) Bridge (nur Linux).

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3 und SP4 SP5
- SUSE Linux Enterprise Server für SAP 15 SP2
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Service für SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- RedHat Enterprise Linux (RHEL) :7.x
- Oracle Linux 7.5-7.9

- Wenn Sie Ihre Umgebung AWS Control Tower mit mehreren Konten verwalten, stellen Sie sicher, dass Sie die neueste Version von verwenden, um die Kompatibilität mit Accelerate zu AWS Control Tower gewährleisten. Umgebungen, die AWS Control Tower Versionen vor 2.7 (veröffentlicht im April 2021) verwenden, werden nicht unterstützt. Informationen zum Aktualisieren finden Sie unter Aktualisieren AWS Control Tower Sie Ihre Landing Zone.

Unterstützte Services

AWS Managed Services bietet Unterstützungsservices für das Betriebsmanagement für die folgenden AWS Services. Jeder AWS Service ist anders und daher variiert der Umfang der Unterstützung für das Betriebsmanagement durch AMS je nach Art und Merkmalen des zugrunde liegenden AWS Services. Wenn Sie beantragen, dass AWS Managed Services Services für Software oder Services bereitstellt, die in der folgenden Liste nicht ausdrücklich als unterstützt gekennzeichnet sind, werden alle AWS Managed Services, die für solche vom Kunden angeforderten Konfigurationen bereitgestellt werden, gemäß den Servicebedingungen als „Beta-Service“ behandelt.

- Vorfälle: Alle Dienste AWS
- Serviceanfrage: Alle AWS Dienste
- Patchen: Amazon EC2

- Backups und Wiederherstellung: Alles AWS-Services unterstützt von AWS Backup. Eine Liste der Dienste, die von unterstützt werden AWS Backup, finden Sie unter AWS Backup Unterstützte Ressourcen.
- Resource Scheduler: Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Amazon Relational Database Service (Amazon RDS) und Amazon EC2 Auto Scaling Scaling-Gruppen
- Dienste, die auf betriebliche Ereignisse hin überwacht werden: Unterstützte Prüfungen und Trusted Advisor, Application Load Balancer, Aurora, Amazon EC2, Elastic Load Balancing, Amazon FSx for NetApp ONTAP, Amazon FSx für Windows File Server, NAT-Gateway (ein Network Address Translation (NAT) -Service),, OpenSearch Health Dashboard, Amazon Redshift, Amazon Relational Database Service (Amazon RDS), VPN. Site-to-Site Weitere Informationen darüber, was AMS Accelerate im Rahmen eines Services überwacht, finden Sie unter Warnmeldungen aus der Basisüberwachung in AMS.
- Dienste, die durch Sicherheitskonfigurationsregeln überwacht werden: AWS Account GuardDuty, Macie, Amazon API Gateway,, AWS Certificate Manager, AWS Config, CloudTrail, CloudWatch AWS CodeBuild, Amazon DynamoDB AWS Database Migration Service, Amazon EC2, Amazon Elastic Block Store (Amazon EBS) ElastiCache, Amazon Elastic File System (Amazon EFS), Amazon Elastic Kubernetes Service (Amazon EKS), Elastic Load Balancing, Amazon Service, Amazon EMR, AWS Identity and Access Management (IAM),,, Amazon Redshift, Amazon Relational Database OpenSearch Service AWS Key Management Service AWS Lambda, Amazon S3, Amazon AI,, SageMaker AWS Secrets Manager Amazon Simple Notification Service AWS Systems Manager, Amazon VPC (Sicherheitsgruppe, Volumen, elastische IP-Adresse, VPN-Verbindung, Internet-Gateways), Amazon VPC Flow Logs. Weitere Informationen finden Sie unter Konformität mit der Konfiguration in Accelerate und Datenschutz in Accelerate. Weitere AMS-Sicherheitsinformationen finden Sie in unserem privaten Sicherheitsleitfaden AWS Artifact, auf den Sie über die Registerkarte Berichte für AWS Managed Services zugreifen können.

> **Note**
>
> AMS Accelerate für die Region Naher Osten (VAE) unterstützt eine Reihe von Funktionen, die im Leistungsumfang enthalten sind, wie in der folgenden Tabelle beschrieben. Der Zugriff auf die AMS-Kontokonsole und die Instances in dieser Region erfolgt ausschließlich über Trigger für eingehende Serviceanfragen. Weitere Informationen zur Verfügbarkeit von Accelerate in der Region Naher Osten (VAE) erhalten Sie von Ihrem Account Manager oder AWS Cloud Service Delivery Manager (CSDM).

Im Leistungsumfang enthaltene Funktionen von AMS Accelerate für die Region Naher Osten (VAE)	Beschreibung der Funktionen
Vorfallmanagement	AMS reagiert auf Vorfälle und unterstützt Ihr Team bei der Lösung von Problemen. Damit AMS Sie beim Incident Management unterstützen kann, müssen Sie eine Serviceanfrage einreichen. AMS erkennt oder reagiert nicht proaktiv auf Vorfälle in dieser Region.
Überwachung	Nach Erhalt einer Serviceanfrage von Ihnen kann AMS Sie bei der Behebung von Ressourcen unterstützen. AMS setzt automatisierte Problembehebungen, Mitarbeiter und Prozesse ein, um Ihre Ressourcen wieder in einen gesunden Zustand zu versetzen. AMS konfiguriert in dieser Region keine CloudWatch Basisereignisse und Alarme. Wenn Sie bereits über Überwachungstools verfügen, kann eine proaktive Nachverfolgung Ihrer Ressourcen auf der Grundlage von Cloud Architect (CA) und CSDM Assessments möglich sein.
Sicherheit	Nach Erhalt einer Serviceanfrage von Ihnen kann AMS Sie bei der Behebung von Sicherheitsproblemen unterstützen. AMS setzt in dieser Region keine Sicherheitskontrollen ein AWS-Config-Regeln und GuardDuty überwacht auch keine Sicherheitslücken. Wenn Sie bereits über Sicherheitstools verfügen, ist auf der Grundlage von CA- und CSDM-Bewertungen möglicher weise eine proaktive Sicherheitsüberwachung verfügbar.
Patch-Management	AMS kann während bestimmter Wartungsfenster Anbieter-Updates auf EC2 Amazon-

Im Leistungsumfang enthaltene Funktionen von AMS Accelerate für die Region Naher Osten (VAE)	Beschreibung der Funktionen
	Instances für unterstützte Betriebssysteme anwenden und Snapshots vor dem Patchen erstellen. Damit AMS Sie beim Patch-Management unterstützen kann, müssen Sie eine Serviceanfrage einreichen. AMS-Patch-Benachrichtigungen und -Berichte sind in dieser Region nicht verfügbar.
Backup-Verwaltung	AMS kann Snapshots erstellen und speichern, die von AWS-Services unterstützt werden AWS Backup, und unterstützt Sie bei der Wiederherstellung von Backups. Damit AMS Sie beim Backup-Management unterstützen kann, müssen Sie eine Serviceanfrage einreichen. AMS verfolgt keine Backup-Jobs in dieser Region.
Ausgewiesene Experten	AMS ernennt einen Cloud Architect (CA) und einen Cloud Service Delivery Manager (CSDM), um mit Kundenorganisationen zusammenzuarbeiten und die betriebliche und sicherheitstechnische Exzellenz zu fördern.
Verwaltung von Serviceanfragen	Um Informationen über Ihre verwaltete Umgebung, AMS oder AWS-Service Angebote anzufordern, reichen Sie Serviceanfragen über die AMS Accelerate-Konsole ein. Sie können eine Serviceanfrage mit „Anleitungen“ AWS-Services und Funktionen einreichen oder um AMS-Services, die in dieser Region verfügbar sind, wie in dieser Tabelle beschrieben, in Anspruch zu nehmen.

Rollen und Zuständigkeiten

Die RACI-Matrix von AMS Accelerate (verantwortlich, rechenschaftspflichtig, konsultiert und informiert) weist entweder dem Kunden oder AMS die Hauptverantwortung für eine Vielzahl von Aktivitäten zu. In der Tabelle werden Ihre (der „Kunde“) Verantwortlichkeiten im Vergleich zu unseren („AMS Accelerate“) Verantwortlichkeiten beschrieben.

Umfang der von AMS Accelerate vorgenommenen ÄnderungenIn diesem Abschnitt sind die spezifischen Umstände aufgeführt, unter denen AMS berechtigt ist, Änderungen an Ihrem Konto vorzunehmen, sowie einige Arten von Änderungen, die AMS niemals vornimmt.

AMS Accelerate RACI Matrix

AMS Accelerate verwaltet Ihre AWS-Infrastruktur. Die folgende Tabelle bietet einen Überblick über die Rollen und Verantwortlichkeiten von Ihnen und AMS Accelerate für Aktivitäten im Lebenszyklus einer Anwendung, die in der verwalteten Umgebung ausgeführt wird.

- R steht für Verantwortliche Partei, die die Arbeit zur Erfüllung der Aufgabe erledigt.
- C steht für Konsultiert, eine Partei, deren Meinung eingeholt wird, in der Regel als Fachexperten, und mit der bilaterale Kommunikation besteht.
- I steht für Informiert, d. h. eine Partei, die über den Fortschritt informiert wird, oft erst, wenn die Aufgabe abgeschlossen ist.

> **Note**
>
> Einige Abschnitte enthalten „R“ sowohl für AMS als auch für Kunden. Dies liegt daran, dass im Modell der AWS gemeinsamen Verantwortung sowohl AMS als auch die Kunden gemeinsam Verantwortung übernehmen, um Infrastruktur- und Anwendungsprobleme zu lösen.

Aktivität	Kunde	AWS Managed Services (AMS)
AMS-Muster		

Aktivität	Kunde	AWS Managed Services (AMS)
Erstellen Sie neue Muster	I	R
Stellen Sie Muster bereit und passen Sie sie an	R	C, I
Testen und entfernen Sie Muster	R	I
Anwendungslebenszyklus		
Anwendungsentwicklung	R	I
Anforderungen, Analyse und Design der Anwendungsinfrastruktur	R	I
Bereitstellen von Anwendungen	R	I
Bereitstellung AWS AWS-Ressourcen	R	I
Anwendungsüberwachung	R	I
Testen/Optimierung von Anwendungen	R	I
Beheben und lösen Sie Anwendungsprobleme	R	I
Probleme beheben und lösen	R	I
Überwachung wird für die AWS-Infrastruktur unterstützt	C	R
Reaktion auf Vorfälle bei AWS-Netzwerkproblemen	C	R
Reaktion auf Vorfälle bei AWS-Ressourcenproblemen	C	R
Onboarding verwalteter Konten		
Gewähren Sie dem AMS-Team und den Tools Zugriff auf das AWS-Verwaltungskonto	R	C

Aktivität	Kunde	AWS Managed Services (AMS)
Implementieren Sie Änderungen im Konto oder in der Umgebung, um die Bereitstellung von Tools im Konto zu ermöglichen. Zum Beispiel Änderungen an den Dienststeuerungsrichtlinien (SCPs)	R	C
Installieren Sie SSM-Agenten in Instanzen EC2	R	C
Installieren und konfigurieren Sie die Tools, die für die Bereitstellung von AMS-Diensten erforderlich sind. Zum Beispiel CloudWatch Agenten, Skripte für Patches, Alarme, Protokolle und andere	I	R
Verwalten Sie den Zugriffs- und Identitätslebenszyklus für AMS-Techniker	I	R
Sammeln Sie alle erforderlichen Eingaben, um die AMS-Dienste zu konfigurieren. Zum Beispiel Dauer, Zeitplan und Ziele für die Patch-Wartung	R	I
Fordern Sie die Konfiguration der AMS-Dienste an und geben Sie alle erforderlichen Eingaben ein	R	I
Konfigurieren Sie die AMS-Dienste wie vom Kunden gewünscht. Zum Beispiel Patch-Wartungsfenster, Resource Tagger und Alarmmanager	C	R
Verwalten Sie den Lebenszyklus von Benutzern und deren Berechtigungen für lokale Verzeichnisdienste, die für den Zugriff auf AWS-Konten und -Instances verwendet werden	R	I
Empfehlen Sie die Optimierung reservierter Instanzen	I	R
Integrieren Sie Konten in Trusted Remediator	C, I	R
Patch-Verwaltung		

Aktivität	Kunde	AWS Managed Services (AMS)
Sammeln Sie alle erforderlichen Eingaben, um die Patch-Wartungsfenster, die Patch-Baselines und das Ziel zu konfigurieren	R	I
Fordern Sie die Konfiguration der Patch-Wartungsfenster und -Baselines an und geben Sie alle erforderlichen Eingaben an	R	I
Konfigurieren Sie die Wartungsfenster, die Patch-Baselines und die Ziele für die Patch-Wartung nach den Wünschen des Kunden	C	R
Halten Sie Ausschau nach geeigneten Updates für unterstützte Betriebssysteme und Software, bei denen das unterstützte Betriebssystem für Instanzen vorinstalliert ist EC2	I	R
Melden Sie, ob Updates für unterstützte Betriebssysteme fehlen und ob das Wartungsfenster abgedeckt ist	I	R
Machen Sie Schnappschüsse von Instanzen, bevor Sie Updates anwenden	I	R
Wenden Sie Updates auf EC2 Instanzen pro Kundenkonfiguration an	I	R
Untersuchen Sie fehlgeschlagene Updates für EC2 Instanzen	C	R
Update AMIs und Stacks für Auto-Scaling-Gruppen () ASGs	R	C
Patchen Sie das Windows-Betriebssystem und die auf dem Betriebssystem installierten Microsoft-Pakete, die von Windows Update gesteuert werden	I	R
Patchen Sie installierte Anwendungen, Software oder Anwendungsabhängigkeiten, die nicht von Windows Update verwaltet werden	R	I

Aktivität	Kunde	AWS Managed Services (AMS)
Patchen Sie das Linux-Betriebssystem und alle Pakete, die für die Verwaltung durch den systemeigenen Paketmanager des Betriebss ystems aktiviert sind (z. B. Yum, Apt, Zypper)	I	R
Patchen Sie installierte Anwendungen, Software oder Anwendung sabhängigkeiten, die nicht vom systemeigenen Paketmanager des Linux-Betriebssystems verwaltet werden	R	I
Backup		
Sammeln Sie alle erforderlichen Eingaben, um Backup-Pläne und Zielressourcen zu konfigurieren	R	I
Fordern Sie die Konfiguration der Backup-Pläne an und geben Sie alle erforderlichen Eingaben an	R	I
Konfigurieren Sie die Backup-Pläne und -ziele wie vom Kunden gewünscht	C	R
Geben Sie Backup-Zeitpläne und Zielressourcen an	R	I
Führen Sie Backups pro Plan durch	I	R
Untersuchen Sie fehlgeschlagene Sicherungsaufträge	I	R
Bericht über den Status der Backup-Jobs und den Umfang der Backups	I	R
Backups validieren	R	I
Fordern Sie die Wiederherstellung von Backups für Ressourcen unterstüt zter AWS-Serviceressourcen als Teil des Incident Managements an	R	I
Führen Sie Backup-Wiederherstellungsaktivitäten für Ressourcen unterstützter AWS-Services durch	I	R

Aktivität	Kunde	AWS Managed Services (AMS)
Stellen Sie die betroffenen benutzerdefinierten Anwendungen oder Anwendungen von Drittanbietern wieder her	R	I
Netzwerkfunktionen		
Bereitstellung und Konfiguration von Managed Account VPCs IGWs, Direct Connect und anderen AWS-Netzwerkservices	R	I
Konfiguration und Betrieb von AWS Security Groups/NAT/NACL innerhalb des verwalteten Kontos	R	I
Netzwerkkonfiguration und Implementierung innerhalb des Kundennetzwerks (zum Beispiel DirectConnect)	R	I
Netzwerkkonfiguration und Implementierung innerhalb des AWS-Netzwerks	R	I
Von AMS definierter Monitor für die Netzwerksicherheit, einschließlich Sicherheitsgruppen	I	R
Konfiguration und Verwaltung der Protokollierung auf Netzwerkebene (VPC-Flow-Logs und andere)	I	R
Protokollierung		
Zeichnen Sie alle Anwendungsänderungsprotokolle auf	R	I
AWS-Infrastrukturänderungsprotokolle aufzeichnen	I	R
AWS-Audit-Trail aktivieren und aggregieren	I	R
Protokolle aus AWS-Ressourcen zusammenfassen	I	R
Überwachung und Problembehebung		

Aktivität	Kunde	AWS Managed Services (AMS)
Sammeln Sie alle erforderlichen Eingaben, um den Alarmmanager, den Resource Tagger und die Alarmschwellenwerte zu konfigurieren	R	I
Fordern Sie die Konfiguration des Alarmmanagers an und geben Sie alle erforderlichen Eingaben an	R	I
Konfigurieren Sie den Alarmmanager, den Resource Tagger und die Alarmschwellenwerte nach Kundenwunsch.	C	R
Stellen Sie CloudWatch AMS-Basismetriken und Alarme pro Kundenkon figuration bereit	I	R
Überwachen Sie unterstützte AWS-Ressourcen mithilfe von CloudWatch Basismetriken und Alarmen	I	R
Untersuchen Sie Warnmeldungen von AWS-Ressourcen	C	R
Korrigieren Sie Warnungen auf der Grundlage einer definierten Konfigura tion oder erstellen Sie einen Vorfall	I	R
Definieren, überwachen und untersuchen Sie kundenspezifische Monitore	R	I
Untersuchen Sie Warnmeldungen aus der Anwendungsüberwachung	R	C
Konfigurieren Sie Trusted Advisor Prüfungen zur Problembehebung	R	C
Korrigieren Sie automatisch unterstützte Prüfungen Trusted Advisor	I	R
Korrigieren Sie unterstützte Prüfungen manuell Trusted Advisor	R	C
Den Status der Problembehebung melden	I	R
Beheben Sie Fehler bei der Behebung	R	C

Aktivität	Kunde	AWS Managed Services (AMS)
Sicherheitsarchitektur		
Überprüfen Sie die AMS-Ressourcen und den Code auf Sicherheitsprobleme und potenzielle Bedrohungen	I	R
Implementieren Sie Sicherheitskontrollen in AMS-Ressourcen und Code, um Sicherheitsrisiken zu minimieren	I	R
Unterstützte AWS-Services für die Sicherheitsverwaltung des Kontos und seiner AWS-Ressourcen aktivieren	I	R
Verwalten Sie privilegierte Anmeldeinformationen für den Konto- und Betriebssystemzugriff für AMS-Techniker	I	R
Management von Sicherheitsrisiken		
Überwachen Sie unterstützte AWS-Services für das Sicherheitsmanagement, wie GuardDuty und Macie	I	R
Definieren und erstellen Sie AMS-definierte Konfigurationsregeln, um festzustellen, ob AWS-Ressourcen den bewährten Sicherheitsmethoden von Center for Internet Security (CIS) und NIST entsprechen.	I	R
AMS-definierte Konfigurationsregeln überwachen	I	R
Konformitätsstatus der Konfigurationsregeln melden	I	R
Definieren Sie eine Liste der erforderlichen Konfigurationsregeln und korrigieren Sie sie	I	R
Evaluieren Sie die Auswirkungen der Korrektur von AMS-definierten Konfigurationsregeln	R	I
Beantragen Sie die Korrektur der von AMS definierten Konfigurationsregeln im AWS-Konto	R	I

Aktivität	Kunde	AWS Managed Services (AMS)
Ressourcen nachverfolgen, die von den AMS-definierten Konfigura tionsregeln ausgenommen sind	R	I
Unterstützte AMS-definierte Konfigurationsregeln im AWS-Konto korrigier en	C	R
Korrigieren Sie nicht unterstützte AMS-definierte Konfigurationsregeln im AWS-Konto	R	I
Definieren, überwachen und untersuchen Sie kundenspezifische Konfigurationsregeln	R	I
Verwaltung von Vorfällen		
Benachrichtigung über Vorfälle, die von AMS in AWS-Ressourcen entdeckt wurden	I	R
Informieren Sie sich über Vorfälle in AWS Ressourcen	R	I
Informieren Sie sich über Vorfälle für AWS Ressourcen, die auf der Überwachung basieren	I	R
Bewältigen Sie Leistungsprobleme und Ausfälle von Anwendungen	R	I
Kategorisieren Sie die Priorität von Vorfällen	I	R
Bereitstellen einer Reaktion auf Vorfälle	I	R
Sorgen Sie für die Behebung von Vorfällen oder die Wiederherstellung der Infrastruktur für Ressourcen mit verfügbaren Backups	C	R
Reaktion auf Sicherheitsvorfälle — Bereiten Sie sich darauf vor		
Kommunikation		

Aktivität	Kunde	AWS Managed Services (AMS)
Bereitstellung und Aktualisierung der Kontaktinformationen für Kundensicherheit, die AMS bei Benachrichtigungen über Sicherheitsereignisse und Sicherheitseskalationen verwenden kann	R	I
Speichern und verwalten Sie die vom Kunden bereitgestellten Sicherheitskontaktdaten, um sie bei Sicherheitsereignissen und Sicherheitseskalationen zu verwenden	C	R
Training		
Stellen Sie dem Kunden Unterlagen zur Verfügung, um AMS bei der Reaktion auf Vorfälle zu unterstützen	I	R
Üben Sie die gemeinsame Verantwortung bei der Reaktion auf Sicherheitsvorfälle im Rahmen von Sicherheitsvorfällen	R	R
Ressourcenmanagement		
Konfigurieren Sie ein unterstütztes Sicherheitsmanagement AWS-Services für Warnmeldungen, Korrelation von Warnmeldungen, Geräuschreduzierung und zusätzliche Regeln	I	R
Führen Sie ein umfassendes Inventar der AWS Ressourcen (Amazon EC2, Amazon S3 usw.), einschließlich Einzelheiten zum Wert und zur Wichtigkeit der einzelnen Ressourcen für das Unternehmen. Diese Informationen werden bei der Festlegung einer effektiven Eindämmungsstrategie von entscheidender Bedeutung sein	R	C
Verwenden Sie AWS Tags, um Ressourcen und Workloads zu identifizieren	R	C
Definieren und konfigurieren Sie die Aufbewahrung und Archivierung von Protokollen	I	R

Aktivität	Kunde	AWS Managed Services (AMS)
Schaffen Sie eine sichere Grundlage, indem Sie die Sicherheitsrichtlinien und -konfigurationen des Unternehmens für AWS Konten, Dienste und Zugriffsverwaltung definieren und durchsetzen	R	I
Reaktion auf Sicherheitsvorfälle — Erkennen		
Protokollierung, Indikatoren und Überwachung		
Konfigurieren Sie die Protokollierung und Überwachung, um das Ereignismanagement für Instanzen und Konten zu ermöglichen	I	R
Monitor wird AWS-Services für Sicherheitswarnungen unterstützt	I	R
Stellen Sie Sicherheitstools für Endgeräte bereit und verwalten Sie sie	R	I
Überwachen Sie Instanzen mithilfe von Endpoint Security auf Malware	R	I
Informieren Sie den Kunden durch ausgehende Nachrichten über erkannte Ereignisse	I	R
Koordinieren Sie die interne Kommunikation mit Stakeholdern und aktuelle Informationen für Führungskräfte, um die Reaktionszeit zu verbessern	R	I
Definition, Bereitstellung und Wartung von AMS-Standarderkennungsdiensten (z. B. Amazon GuardDuty und AWS Config)	C	R
Protokollen von AWS Infrastrukturänderungen aufzeichnen	R	I
Aktivieren und konfigurieren Sie die Protokollierung und Überwachung, um das Ereignismanagement für die Anwendung zu ermöglichen	R	C
Implementieren und verwalten Sie eine Zulassungsliste, eine Ablehnungsliste und benutzerdefinierte Erkennungen für unterstützte AWS Sicherheitsdienste (z. B. Amazon) GuardDuty	R	R

Aktivität	Kunde	AWS Managed Services (AMS)
Berichterstattung über Sicherheitsereignisse		
AMS über eine verdächtige Aktivität oder eine aktive Sicherheitsuntersuchung benachrichtigen	R	I
Informieren Sie den Kunden über festgestellte Sicherheitsereignisse und -vorfälle	I	R
Informieren Sie über ein geplantes Ereignis, das den Prozess zur Reaktion auf Sicherheitsvorfälle auslösen könnte	R	I
Reaktion auf Sicherheitsvorfälle — Analysieren		
Untersuchung und Analyse		
Führen Sie eine erste Reaktion auf eine unterstützte Sicherheitswarnung durch, die von einer unterstützten Erkennungsquelle generiert wurde	I	R
Beurteilen Sie die false/true positiven Ergebnisse anhand der verfügbaren Daten	R	R
Generieren Sie eine Momentaufnahme der betroffenen Instanzen, die Sie bei Bedarf mit dem Kunden teilen können	I	R
Führen Sie forensische Aufgaben wie Chain of Custody, Dateisystemanalyse, Speicherforensik und Binäranalyse durch	R	C
Sammeln Sie Anwendungsprotokolle, um die Untersuchung zu unterstützen	R	I
Sammeln Sie Daten und Protokolle, um die Untersuchung von Sicherheitswarnungen zu unterstützen	R	R
Nehmen SMEs Sie AWS-Services an Sicherheitsuntersuchungen teil	C	R

Aktivität	Kunde	AWS Managed Services (AMS)
Teilen Sie während einer Untersuchung Ermittlungsprotokolle vom Support AWS-Services an Kunden weiter	I	R
Kommunikation		
Senden Sie Warnmeldungen und Benachrichtigungen von AMS-Erken nungsquellen für verwaltete Ressourcen	I	R
Verwalten Sie Warnmeldungen und Benachrichtigungen für Sicherhei tsereignisse in Anwendungen	R	I
Wenden Sie sich bei der Untersuchung eines Sicherheitsvorfalls an den Sicherheitsbeauftragten des Kunden	R	I
Reaktion auf Sicherheitsvorfälle — Eindämmen		
Eindämmungsstrategie und Umsetzung		
Beurteilen Sie die Risiken und entscheiden Sie über die Eindämmun gsstrategie, wobei Sie mögliche Auswirkungen auf den Service berücksic htigen	R	C
Erstellen Sie zur weiteren Analyse eine Sicherungskopie der betroffenen Systeme	I	R
Beschränken Sie Anwendungen und Workloads (durch anwendung sspezifische Konfiguration oder Reaktionsaktivitäten)	R	C
Definieren Sie die Eindämmungsstrategie auf der Grundlage des Sicherheitsvorfalls und der betroffenen Ressource	I	R
Aktivieren Sie die Verschlüsselung und sichere Speicherung von Point-in-Time-Backups der betroffenen Systeme	C	R

Aktivität	Kunde	AWS Managed Services (AMS)
Führen Sie unterstützte Containment-Aktionen für AWS Ressourcen wie EC2 Instanzen, Netzwerk und IAM aus	I	R
Reaktion auf Sicherheitsvorfälle — Eliminieren		
Strategie und Umsetzung der Ausrottung		
Definieren Sie die Eliminierungsoptionen auf der Grundlage des Sicherheitsvorfalls und der betroffenen Ressource für die Workloads der Kundenanwendungen	C	R
Legen Sie die vereinbarte Ausrottungsstrategie, den Zeitpunkt der Durchführung und die Konsequenzen fest	R	I
Definieren Sie die Maßnahmen zur Beseitigung auf der Grundlage des Sicherheitsvorfalls und der betroffenen Ressource auf AMS-verwalteten Workloads	C	R
Beseitigen Sie Bedrohungen und schützen Sie AWS Ressourcen, einschließlich EC2 Instanzen, Netzwerk und IAM-Beseitigung	R	C
Beseitigen Sie Bedrohungen und schützen Sie Anwendungen und Workloads (durch anwendungsspezifische Konfiguration oder Reaktions aktivitäten)	R	I
Reaktion auf Sicherheitsvorfälle — Wiederherstellung		
Vorbereitung und Durchführung der Wiederherstellung		
Konfigurieren Sie Backup-Pläne und -Ziele wie vom Kunden gewünscht	I	R
Überprüfen Sie die Backup-Pläne zur Wiederherstellung von AMS-verwa lteten Workloads	R	I

Aktivität	Kunde	AWS Managed Services (AMS)
Führen Sie Aktivitäten zur Wiederherstellung von Backups für unterstützte Ressourcen durch AWS-Services	I	R
Backup die Kundenanwendung, die APP-Konfiguration und die Bereitstellungseinstellungen und überprüfen Sie die Backup-Pläne, um Kundenanwendungen und Workloads nach einem Vorfall wiederherzustellen	R	I
Stellen Sie Anwendungen und Kunden-Workloads wieder her (durch anwendungsspezifische Wiederherstellungsschritte)	R	I
Reaktion auf Sicherheitsvorfälle — Bericht nach dem Vorfall		
Berichterstattung nach dem Vorfall		
Teilen Sie dem Kunden nach dem Vorfall bei Bedarf die entsprechenden Erfahrungen und Maßnahmen mit	I	R
Problemmanagement		
Korrelieren Sie Vorfälle, um Probleme zu identifizieren	I	R
Führen Sie eine Ursachenanalyse (RCA) für Probleme durch	I	R
Probleme beheben	I	R
Identifizieren und beheben Sie Anwendungsprobleme	R	I
Servicemanagement		
Fordern Sie Informationen mithilfe von Serviceanfragen an	R	I
Beantworten Sie Serviceanfragen	I	R
Geben Sie Empfehlungen zur Kostenoptimierung	I	R

Aktivität	Kunde	AWS Managed Services (AMS)
Bereiten Sie einen monatlichen Servicebericht vor und stellen Sie ihn bereit	I	R
Verwaltung von Änderungen		
Change-Management-Prozesse und Tools für die Bereitstellung und Aktualisierung von Ressourcen in der verwalteten Umgebung	R	I
Pflege des Kalenders für Anwendungsänderungen	R	I
Hinweis auf das bevorstehende Wartungsfenster	R	I
Notieren Sie die von AMS Operations vorgenommenen Änderungen	I	R
Kostenoptimierung		
Sammeln Sie alle erforderlichen Eingaben, um Resource Scheduler zu konfigurieren	R	I
Fordern Sie das Onboarding und die Konfiguration von Resource Scheduler an und geben Sie alle erforderlichen Eingaben ein	R	I
Stellen Sie Resource Scheduler pro Kundenkonfiguration bereit	C, I	R
Deaktivieren und aktivieren Sie den Resource Scheduler im Kundenkonto	R	C
Zeitpläne erstellen, löschen, beschreiben und aktualisieren	C	R
Perioden erstellen, löschen, beschreiben und aktualisieren	C	R
Untersuchen und beheben Sie Probleme mit Resource Scheduler	I	R
Anfrage für das Offboarding des Resource Schedulers	R	I
Offboarding des Resource Schedulers aus dem Konto	C, I	R

Umfang der von AMS Accelerate vorgenommenen Änderungen

AMS Accelerate nimmt Änderungen nur für die spezifischen Zwecke und Situationen vor, die im Folgenden beschrieben werden. AMS nimmt Änderungen nur auf der Infrastrukturebene vor, indem es die Konsole oder verwendet APIs. AMS ändert niemals Ihre Anwendungs-, Steuerungs- oder Domänenebene. Sie können alle Änderungen sehen, die von AMS (oder anderen Benutzern) mithilfe unserer vorgefertigten Abfragen vorgenommen wurden. Informationen dazu finden Sie unterÄnderungen in Ihren AMS Accelerate-Konten verfolgen.

AWS Ressourcen

AMS Accelerate stellt AWS Ressourcen nur in den folgenden Situationen bereit oder aktualisiert sie:

- Um die von AMS benötigten Tools und Ressourcen bereitzustellen und zu aktualisieren.
- Als Teil der AMS-Überwachung als Reaktion auf Ereignisse und Alarme.
- Zur Behebung von Sicherheitsproblemen im Rahmen von Reaktionen auf Verstöße in Accelerate (Anpassung von Ressourcen, die nicht den Vorschriften entsprechen, an bewährte Sicherheitsverfahren anpassen).
- Während der Behebung und Wiederherstellung im Rahmen einer Reaktion auf Vorfälle.
- Bei der Beantwortung von Kundenanfragen zur Konfiguration von AMS-Funktionen, wie z. B. den folgenden:
  - Alarmmanager
  - Ressourcen-Tagger
  - Patch-Baselines und Wartungsfenster
  - Ressourcenplaner
  - Backup-Pläne

AMS Accelerate stellt außerhalb dieser Situationen keine Ressourcen bereit oder aktualisiert sie. Wenn Sie Hilfe von AMS benötigen, um in anderen Situationen Änderungen vorzunehmen, sollten Sie die Nutzung von Operations on Demand in Betracht ziehen.

Betriebssystem-Software

AMS Accelerate kann bei Nichtverfügbarkeit Änderungen an Ihrer Betriebssystemsoftware vornehmen, indem Vorfälle gemäß unseren Service Level Agreements behoben werden. AMS kann im Rahmen von auch Änderungen an Ihren Betriebssystemen vornehmen. Automatisierte Instanzkonfiguration in AMS Accelerate

Anwendungscode und Konfiguration

AMS Accelerate ändert niemals Ihren Code (z. B. CloudFormation AWS-Vorlagen, andere infrastructure-as-code Vorlagen oder Lambda-Funktionen), kann Ihre Teams jedoch darüber informieren, welche Änderungen erforderlich sind, um die besten Betriebs- und Sicherheitspraktiken einzuhalten. AMS Accelerate bietet Unterstützung bei der Behebung von Infrastrukturproblemen, die sich auf Anwendungen auswirken, AMS Accelerate greift jedoch nicht auf Ihre Anwendungskonfigurationen zu oder validiert diese.

Funktionen für nicht unterstützte Betriebssysteme in Accelerate

Ein nicht unterstütztes Betriebssystem ist jedes Betriebssystem, das nicht in der aufgeführt ist. Unterstützte Konfigurationen AMS betrachtet Instances mit nicht unterstützten Betriebssystemen als „vom Kunden angeforderte Konfigurationen“, die den Nutzungsbedingungen für AWS Betas und Previews unterliegen.

Die folgenden begrenzten AMS-Funktionen sind für Instances mit nicht unterstützten Betriebssystemen verfügbar:

Funktionalität	Hinweise
Vorfallmanagement	AMS reagiert auf Vorfälle.
Verwaltung von Serviceanfragen	AMS reagiert auf Serviceanfragen.
Überwachung	AMS überwacht und reagiert auf EC2 Amazon-Sy stemstatusprüfungen und Instance-Statusprüfungen. Zu den Systemstatusprüfungen gehören: Verlust der Netzwerkkonnektivität, Verlust der Systemleistung, Softwareprobleme auf dem physischen Host und Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen. Zu den Instanzstatusprüfungen gehören: falsche Netzwerk- oder Startkonfiguration, erschöpfter Arbeitssp eicher, beschädigtes Dateisystem und inkompatibler Kernel.

Funktionalität	Hinweise
Sicherheitsmanagement	AMS überwacht die EC2 GuardDuty Ergebnisse und AWS Config Regeln von Amazon und reagiert darauf.
Backup-Verwaltung	AMS bietet Continuity Management in Accelerate für die EC2 Verwendung von AMS-maßgeschneiderten AWS Backup Plänen und Tresoren.

Kontakt und Eskalation

Sie haben einen eigenen Cloud Service Delivery Manager (CSDM), der Ihnen bei AMS Accelerate beratend zur Seite steht und über ein detailliertes Verständnis Ihres Anwendungsfalls und Ihrer Technologiearchitektur für die verwaltete Umgebung verfügt. CSDMs arbeiten mit Kundenbetreuern, technischen Kundenbetreuern, AWS Managed Services Services-Cloudarchitekten (CAs) und AWS-Lösungsarchitekten (SAs) zusammen, um bei der Einführung neuer Projekte zu helfen und während der gesamten Softwareentwicklungs- und Betriebsprozesse Best-Practice-Empfehlungen zu geben. Das CSDM ist die wichtigste Anlaufstelle für AMS. Die wichtigsten Aufgaben Ihres CSDM sind:

- Organisieren und leiten Sie monatliche Besprechungen zur Servicebewertung mit Kunden.
- Geben Sie Einzelheiten zur Sicherheit, zu Softwareupdates für die Umgebung und zu Optimierungsmöglichkeiten an.
- Machen Sie sich für Ihre Anforderungen, einschließlich Funktionsanfragen für AMS Accelerate, stark.
- Beantworten und lösen Sie Anfragen zur Abrechnung und Serviceberichterstattung.
- Bieten Sie Einblicke für Empfehlungen zur Finanz- und Kapazitätsoptimierung.

Kontakt-Stunden

Sie können AMS Accelerate aus verschiedenen Gründen zu unterschiedlichen Zeiten kontaktieren.

Funktion	AMS Accelerate
	Premium-Stufe
Serviceanfrage	24/7
Verwaltung von Zwischenfällen (P2-P3)	24/7
Sicherung und Wiederherstellung	24/7
Patch-Management	24/7
Überwachen und Warnen	24/7
Manager für die Bereitstellung von Cloud-Diensten (CSDM)	Montag bis Freitag: 08:00 — 17:00 Uhr, lokale Geschäftszeiten

Geschäftszeiten

Funktion	AMS Accelerate
	Premium-Stufe
Serviceanfrage	24/7
Verwaltung von Zwischenfällen (P1)	Rund um die
Verwaltung von Zwischenfällen (P2-P3)	Rund um die
Sicherung und Wiederherstellung	24/7
Patch-Management	24/7
Überwachen und Warnen	24/7
Manager für die Bereitstellung von Cloud-Diensten (CSDM)	Montag bis Freitag: 09:00 — 17:00 Uhr, lokale Geschäftszeiten

Eskalationspfad

AMS unterstützt Kunden mit Incident Management und Service Request Management, 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr, gemäß dem für das Konto geltenden AMS Service Level Agreement.

Um ein Leistungsproblem mit dem AWS- oder AMS-Service zu melden, das sich auf Ihre verwaltete Umgebung auswirkt, verwenden Sie die AMS-Konsole und reichen Sie einen Incident-Fall ein. Details hierzu finden Sie unter Einen Vorfall für Accelerate einreichen. Allgemeine Informationen zum AMS Incident Management finden Sie unterVorfallmanagement in AMS Accelerate.

Verwenden Sie die AMS-Konsole und senden Sie eine Serviceanfrage, um Informationen oder Ratschläge zu erhalten oder zusätzliche Services von AMS in Anspruch zu nehmen. Details hierzu finden Sie unter Eine Serviceanfrage in Accelerate erstellen. Allgemeine Informationen zu AMS-Serviceanfragen finden Sie unterVerwaltung von Serviceanfragen in Accelerate.

Ressourceninventar für Accelerate

Alle Ressourcen, die AMS Accelerate für Ihre Konten AWS-Konto oder Konten bereitstellt, sind in der Tabelle mit der `resource_inventory.zip`Datei resource_inventory.xlsx (komprimiert) aufgeführt.

> **Note**
>
> In der Spalte Ressourcenname steht das Präfix CFN: für eine CloudFormation logische ID statt für einen Ressourcennamen. Diese werden für unbenannte Ressourcen angezeigt, beispielsweise für S3-Bucket-Richtlinien.

AMS stellt eine Reihe von Diensten bereit, wie in der beschrieben. Service description (Service-Beschreibung) Die Kosten für deren Bereitstellung sind gering, wenn sie für ein leeres Konto bereitgestellt werden, aber die Kosten steigen, wenn die Auslastung zunimmt. Beispielsweise werden Protokolle erstellt und Konfigurationsregeln aufgerufen, wenn sich Ressourcen ändern.

Wenn mehrere Änderungen an den Konfigurationsregeln vorgenommen werden, können mehrere Aufrufe zur Einhaltung der Konfigurationsbestimmungen ausgelöst werden, was zu höheren Kosten führt. Die gleiche Möglichkeit gilt für Amazon, das für die Überwachung von Instances CloudWatch verwendet wird. Je detaillierter Ihre Überwachung ist, desto höher sind die Kosten für den Service. AWS Backup ist ein weiteres Beispiel. Wenn Sie mehrere Backups gespeichert haben oder wenn Sie längere Aufbewahrungsfristen haben, verwenden Sie mehr Speicherplatz und die Kosten sind höher.

Diese Zahlen sind schwer vorherzusagen. Behalten Sie bei Ihrem monatlichen Geschäftsbericht mit Ihrem Cloud Service Delivery Manager (CSDM) den Überblick über die Änderungen und arbeiten Sie daran, Bereiche zu identifizieren, in denen sich Kosten senken lassen.

Erste Schritte mit AMS Accelerate

Wenn Sie noch kein Konto bei AWS Managed Services (AMS) haben, wenden Sie sich zunächst über unsere Seite AWS Managed Services — Vertrieb kontaktieren an einen Vertriebsmitarbeiter von Amazon Web Services (AWS).

Nachdem Sie sich für ein AMS angemeldet haben, führt Sie das AMS Accelerate-Team durch den folgenden Onboarding-Prozess für jeden Ihrer AWS-Konten Mitarbeiter.

Sehen Sie sich den Funktionsumfang hier an: Funktionen von AWS Managed Services

> **Note**
>
> AMS Accelerate unterstützt GovCloud Regionen. Wenn sich Ihr Service in einem befindet AWS GovCloud (US) Region, finden Sie weitere Informationen unter Erste Schritte mit AWS GovCloud (US).

Konto-Onboarding-Prozess für Accelerate

Die Aufnahme eines Kontos in AMS Accelerate besteht aus vier Phasen.

1. Schritt 1. Kontoermittlung in Acceleratebewertet den aktuellen Status Ihres Kontos und identifiziert technische Hindernisse für das Onboarding Ihres Kontos.
2. Schritt 2. Einführung von Verwaltungsressourcen in Acceleratefordert Sie auf, die Allgemeinen Geschäftsbedingungen zu akzeptieren und eine Onboarding-Rolle für AMS Accelerate Cloud-Architekten (CAs) einzurichten, die Sie bei der Festlegung von Sicherheitsstandards und bei Bedarf bei der Lösung von Problemen unterstützen.
3. Schritt 3. Onboarding von AMS-Funktionen mit Standardrichtlinienfür Accelerate-Funktionen wie Überwachung, Patching und Backup.
4. Schritt 4. Passen Sie Funktionen in Accelerate anstellt sicher, dass Ressourcen, einschließlich EC2 Instanzen, korrekt für Ihre Anwendung konfiguriert sind.

Beschleunigen Sie die Onboarding-Voraussetzungen

Bevor Sie mit dem Onboarding-Prozess beginnen, ist es wichtig, die technischen Abhängigkeiten zu verstehen, auf die Accelerate-Komponenten angewiesen sind.

> **Note**
>
> Um AMS Accelerate nutzen zu können, müssen Sie einen der beiden unterstützten Support Tarife nutzen: Enterprise On-Ramp oder Enterprise. Die Tarife Developer und Business qualifizieren sich nicht für AMS Accelerate. Weitere Informationen zu den verschiedenen Plänen finden Sie unter Support Tarife vergleichen.

AMS Accelerate VPC-Endpunkte

Ein VPC-Endpunkt ermöglicht private Verbindungen zwischen Ihrer VPC und unterstützten AWS Diensten und VPC-Endpunktdiensten, die von bereitgestellt werden. AWS Wenn Sie ausgehende Internetkonnektivität filtern müssen, konfigurieren Sie die folgenden VPC-Dienstendpunkte, um sicherzustellen, dass AMS Accelerate über Konnektivität mit seinen Dienstabhängigkeiten verfügt.

> **Note**
>
> *region*Stellt in der folgenden Liste den Bezeichner für eine AWS Region dar, beispielsweise `us-east-2` für die Region USA Ost (Ohio).

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

Informationen zur Konfiguration von AWS-VPC-Endpunkten finden Sie unter VPC-Endpunkte.

> **Note**
>
> Wenn Sie in Ihrem Konto VPC-Endpunkte für alle oben genannten Dienste erstellen, sehen Sie sich diese CloudFormation Beispielvorlage an. Sie können diese Vorlage aktualisieren und die VPC-Endpunktdefinition gemäß Ihrem Anwendungsfall entfernen oder hinzufügen.

Ausgehende Internetkonnektivität in Accelerate

1. Laden Sie egressMgmt.zip herunter.
2. Öffnen Sie die **ams-egress.json** Datei.
3. Suchen Sie URLs unter den JSON-Eigenschaften nach:
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. Erlauben Sie den Zugriff auf diese URLs.

Testen der ausgehenden Konnektivität in Accelerate

Testen Sie die ausgehende Konnektivität mit einer der folgenden Methoden.

> **Note**
>
> Bevor Sie das Skript/den Befehl ausführen, ersetzen Sie das Rot *region* durch Ihre Regionskennung, z. B. `us-east-1`

Windows-Skript PowerShell

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

Linux-Befehl

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

Amazon EC2 Systems Manager in Accelerate

Sie müssen den AWS Systems Manager Agenten (SSM-Agent) auf allen EC2 Instances installieren, die AMS verwalten soll. Sie müssen auch die Bucket-Berechtigungen hinzufügen, die der SSM-Agent benötigt. Eine Übersicht, die Amazon einschließt EC2, finden Sie unterSchritt 3. Onboarding von AMS-Funktionen mit Standardrichtlinien.

IAM in Accelerate

Damit Ihre Benutzer die Funktionen von AMS Accelerate lesen und konfigurieren können, z. B. den Zugriff auf die AMS-Konsole oder die Konfiguration von Backups, müssen Sie in AWS Identity and Access Management (IAM) explizite Berechtigungen zur Ausführung dieser Aktionen gewähren. Beispiele für IAM-Richtlinien finden Sie unter Berechtigungen zur Nutzung von AMS-Funktionen.

Schritt 1. Kontoermittlung in Accelerate

AMS arbeitet mit Ihnen bei der Kontoermittlung zusammen, um den aktuellen Status Ihres Kontos zu beurteilen und technische Hindernisse für die Kontoeröffnung zu identifizieren. AMS bietet während der Phase der Kontoermittlung keine operativen Dienstleistungen an. AMS verwendet die `AWSServiceRoleForSupport` dienstbezogene Rolle, um technische Hindernisse zu identifizieren, und arbeitet dann mit Ihnen zusammen, um diese zu beheben, bevor es zur Onboarding-Phase auf Kontoebene übergeht.

Prozess zur Kontoermittlung in Accelerate

Um Ihnen bei der Analyse und Erkennung Ihres Kontos zu helfen, führt AMS mithilfe schreibgeschützter API-Aufrufe Betriebsprüfungen durch, um technische Hindernisse zu identifizieren. Nachdem Ihr Konto bei AMS registriert wurde, werden diese Prüfungen auf Abruf durchgeführt, um den Status Ihres Kontos aufrechtzuerhalten. AMS arbeitet mit Ihnen zusammen, um bei Bedarf alle mit diesen Prüfungen verbundenen Mängel zu korrigieren. AMS verwendet im Rahmen von Account Discovery die folgenden operativen Prüfungen und schreibgeschützten API-Aktionen:

Betriebsüberprüfung	Zweck	AWS Verwendete API-Aufrufe
AWS Control Tower Evaluierung der Version	Identifiziert die AWS Control Tower Version, um sicherzustellen, dass es sich um die	• `ControlTower:GetLandingZone`

Betriebsüberprüfung	Zweck	AWS Verwendete API-Aufrufe
	unterstützte Mindestversion für das Onboarding Ihrer AWS-Konto handelt.	• `ControlTower:ListEnabledControls` • `ControlTower:ListLandingZones`
AWS CloudTrail Evaluierung	Identifiziert AWS CloudTrail Wanderwege und deren Konfigurationen für die Aufnahme Ihrer Wanderwege AWS-Konto zur Minimierung der CloudTrail Trailkosten.	• `CloudTrail:GetTrail` • `CloudTrail:ListTrails` • `S3:GetBucketOwnershipControls` • `S3:GetBucketPolicy` • `KMS:GetKeyPolicy` • `CloudTrail:GetEventSelectors` • `S3:GetBucketLogging` • `S3: GetBucketLifecycleConfiguration` • `S3: GetBucketEncryption`
CloudFormation Bewertung von Hooks	Identifiziert CloudFormation Hooks in Ihrem Onboarding AWS-Konto , die die Bereitstellung von AMS-Services in Ihrem AWS-Konto blockieren.	• `CloudFormation:ListTypes`
Evaluierung Amazon EC2 Amazon-Instances	Identifiziert EC2 Instances in Ihrem AWS-Konto System, auf denen kein AWS Systems Manager Agent (SSM-Agent) ausgeführt wird und die nicht von AMS unterstützt werden.	• `EC2:DescribeInstances` • `EC2:DescribeImages` • `SSM:DescribeInstanceInformation`

AMS Accelerate befolgt branchenweit bewährte Verfahren, um die Compliance-Anforderungen zu erfüllen und aufrechtzuerhalten. Der Zugriff von AMS Accelerate Discovery auf Ihr Konto wird AWS CloudTrail über die AWSServiceRoleForSupport serviceverknüpfte Rolle erfasst. Dies hilft bei den Überwachungs- und Prüfanforderungen. Informationen zu AWS CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

Schritt 2. Einführung von Verwaltungsressourcen in Accelerate

Dies ist ein Überblick über den Prozess der Eingliederung von Verwaltungsressourcen.

Sie akzeptieren die Bedingungen

Ihr Cloud Services Delivery Manager (CSDM) führt Sie durch den Akzeptanzprozess. Sie müssen die Allgemeinen Geschäftsbedingungen AWS-Regionen, ausgewählte Zusatzleistungen und ein Service Level Agreement (SLA) akzeptieren.

Sie gewähren AMS-Rollen Berechtigungen

Sie müssen Zugriff auf AMS-Prozesse und auf Ihren Cloud Architect gewähren. Dazu erstellen Sie für jede Rolle einen CloudFormation Stack. Sehen Die Vorlage zum Erstellen von AMS-Rollen und dannErstellen `aws_managedservices_onboarding_role` mit CloudFormation for Accelerate. Weitere Informationen finden Sie unter Zugriffsverwaltung in AMS Accelerate.

AMS überprüft Ihre Konfiguration

Ihr Cloud Architect (CA) sucht auch nach möglichen Konfigurationsproblemen in Ihrem Konto, wie z. B. Service Control-Richtlinien (SCPs), und nach Sicherheitsergebnissen, die AMS daran hindern könnten, die von AMS benötigten Tools und Ressourcen bereitzustellen. Ihre CA arbeitet mit Ihnen zusammen, um Sie bei der Behebung von Fehlern und bei der Beseitigung aller Hindernisse zu unterstützen, die dem Einsatz von AMS-Tools und -Ressourcen im Wege stehen.

AMS überprüft Ihre Testkonfigurationen AWS CloudTrail

Ihr Cloud Architect (CA) überprüft Ihre CloudTrail Trail-Konfigurationen und bestätigt, ob AMS einen globalen CloudTrail Trail bereitstellen oder Accelerate in die Trail-Ressourcen Ihres CloudTrail Kontos oder Ihrer Organisation integrieren soll. Wenn Sie sich für die Integration von Accelerate in Ihren CloudTrail Trail entscheiden, führt Sie Ihre CA durch die erforderlichen Aktualisierungen der Konfigurationen für Ihre CloudTrail Trail-Ressourcen.

AMS stellt Verwaltungsressourcen bereit

Das AMS-Team setzt Tools und AWS Ressourcen ein, um die verschiedenen Dienste von AMS Accelerate bereitzustellen. Nach Abschluss des Vorgangs hat AMS das AWS Managed Services Services-Konto erstellt und AMS benachrichtigt Sie, dass Ihr Konto aktiv ist.

Damit ist die Phase der Onboarding-Management-Ressourcen abgeschlossen. Sie können direkt mit dem nächsten Schritt des Onboarding-Prozesses fortfahren:. Schritt 3. Onboarding von AMS-Funktionen mit Standardrichtlinien

> **Note**
>
> Jetzt, da Ihr Konto aktiv ist, haben Sie die Möglichkeit, eine der folgenden Aufgaben auszuführen:
>
> - Erstellen Sie mithilfe der Support Center-Konsole Vorfälle und Serviceanfragen für die AWS Infrastruktur. Siehe Vorfallberichte, Serviceanfragen und Fragen zur Abrechnung in AMS Accelerate.
> - Sehen Sie sich in Ihrem Konto den Konformitätsstatus der von AMS bereitgestellten AWS Config Regeln an,Konformität mit der Konfiguration in Accelerate.
> - Lokalisieren GuardDuty und analysieren Sie die Ergebnisse sowie Macie (optional). Siehe Überwachen Sie mit GuardDuty.
> - Zugriffs- und Prüfprotokolle CloudTrail
> - Verfolgen Sie Änderungen in Ihrem AMS Accelerate-Konto. Siehe Änderungen in Ihren AMS Accelerate-Konten verfolgen.
> - Verwenden Sie Resource Tagger, um Tags zu erstellen. Siehe Beschleunigen Sie Resource Tagger.
> - Fordern Sie Patches, Backup und AWS Config Berichte an. Siehe Berichte und Optionen.

Überprüfen und aktualisieren Sie Ihre Konfigurationen, damit AMS Accelerate Ihren CloudTrail Trail nutzen kann

AMS Accelerate stützt sich auf die AWS CloudTrail Protokollierung, um Audits und die Einhaltung von Vorschriften für alle Ressourcen in Ihrem Konto zu verwalten. Während des Onboardings entscheiden Sie, ob Accelerate einen CloudTrail Trail in Ihrer AWS Hauptregion bereitstellt oder Ereignisse verwendet, die durch Ihr bestehendes CloudTrail Konto oder Ihren Organisationspfad generiert wurden. Wenn für Ihr Konto kein Trail konfiguriert ist, stellt Accelerate beim Onboarding einen verwalteten CloudTrail Trail bereit.

> **Important**
>
> CloudTrail Die Konfiguration der Protokollverwaltung ist nur erforderlich, wenn Sie AMS Accelerate in Ihr CloudTrail Konto oder Ihren Organization Trail integrieren möchten.

Überprüfen Sie mit Ihrem Cloud Architect (CA) Ihre CloudTrail Trail-Konfigurationen, die Amazon S3 S3-Bucket-Richtlinie und die AWS KMS wichtigsten Richtlinien für Ihr CloudTrail Event-Lieferziel

Bevor Accelerate Ihren CloudTrail Trail verwenden kann, müssen Sie mit Ihrem Cloud Architect (CA) zusammenarbeiten, um Ihre Konfigurationen zu überprüfen und zu aktualisieren, um die Accelerate-Anforderungen zu erfüllen. Wenn Sie Accelerate in Ihren CloudTrail Organization Trail integrieren möchten, aktualisiert Ihre CA gemeinsam mit Ihnen Ihren CloudTrail Amazon S3 S3-Bucket und die AWS KMS wichtigsten Richtlinien, um kontoübergreifende Abfragen von Ihrem Accelerate-Konto aus zu ermöglichen. Ihr Amazon S3 S3-Bucket kann sich in einem Konto befinden, das von Accelerate verwaltet wird, oder in einem Konto, das Sie verwalten. Während des Onboardings überprüft Accelerate, ob Anfragen an Ihr CloudTrail Unternehmen gestellt werden können, verfolgt Ereignisse, an das sie geliefert werden, und unterbricht das Onboarding, falls die Anfragen fehlschlagen. Sie arbeiten mit Ihrer CA zusammen, um diese Konfigurationen zu korrigieren, sodass das Onboarding wieder aufgenommen werden kann.

Überprüfen und aktualisieren Sie die CloudTrail Trail-Konfigurationen Ihres Kontos oder Ihrer Organisation

Die folgenden Konfigurationen sind erforderlich, um Accelerate CloudTrail Log Management in Ihre CloudTrail Konto- oder Organization-Trail-Ressourcen zu integrieren:

- Ihr CloudTrail Trail ist so konfiguriert, dass er Ereignisse von allen protokolliert AWS-Regionen.
- Für deinen CloudTrail Trail sind globale Serviceereignisse aktiviert.
- Ihr CloudTrail Konto- oder Organisations-Trail protokolliert alle Verwaltungsereignisse, einschließlich Lese- und Schreibereignisse, AWS KMS und die Amazon RDS Data API-Ereignisprotokollierung ist aktiviert.
- Für Ihren CloudTrail Trail ist die Überprüfung der Integrität der Protokolldatei aktiviert.
- Der Amazon S3 S3-Bucket Your CloudTrail Trail übermittelt Ereignisse, um Ereignisse entweder mit SSE-S3- oder SSE-KMS-Verschlüsselung zu verschlüsseln.
- Für den Amazon S3 S3-Bucket, an den Ihr CloudTrail Trail das Ereignis übermittelt, ist die Serverzugriffsprotokollierung aktiviert.

- Der Amazon S3 S3-Bucket, an den Ihr CloudTrail Trail ausliefert, hat eine Lebenszykluskonfiguration, die Ihre CloudTrail Trail-Daten für mindestens 18 Monate aufbewahrt.
- Für den Amazon S3 S3-Bucket, an den Ihr CloudTrail Trail das Ereignis übermittelt, wurde die Objektverwaltung auf Bucket-Besitzer gesetzt.
- Der Amazon S3 S3-Bucket, an den Ihr CloudTrail Trail das Ereignis übermittelt, ist über Accelerate zugänglich.

Überprüfen und aktualisieren Sie die Amazon S3 S3-Bucket-Richtlinie für Ihr CloudTrail Event-Lieferziel

Während des Onboardings arbeiten Sie mit Ihrem Cloud Architect (CA) zusammen, um Amazon S3 S3-Bucket-Richtlinienerklärungen zu Ihrem Lieferziel für CloudTrail Veranstaltungen hinzuzufügen. Damit Ihre Benutzer von Ihrem Accelerate-Konto aus Änderungen an Ihrem Amazon S3 S3-Bucket für die Zustellung von CloudTrail Veranstaltungen abfragen können, können Sie für jedes Konto in Ihrer Organisation, das Accelerate verwaltet, eine einheitlich benannte IAM-Rolle bereitstellen und sie der `aws:PrincipalArn` Liste in allen Amazon S3 S3-Bucket-Richtlinienerklärungen hinzufügen. Mit dieser Konfiguration können Ihre Benutzer die CloudTrail Organization-Trail-Ereignisse Ihres Kontos in Accelerate mithilfe von Athena abfragen und analysieren. Weitere Informationen zum Aktualisieren einer Amazon S3 S3-Bucket-Richtlinie finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole im Amazon Simple Storage Service-Benutzerhandbuch.

> **Important**
>
> Die Aktualisierung Ihrer Amazon S3 S3-Bucket-Richtlinie ist nur erforderlich, wenn Accelerate in einen CloudTrail Trail integriert ist, der Ereignisse an einen zentralen S3-Bucket weiterleitet. Accelerate unterstützt nicht die Integration mit einem CloudTrail Trail, der an einen zentralen Bucket liefert, aber die Konten nicht unter einer AWS Organisation hat.

> **Note**
>
> Bevor Sie Ihre Amazon S3 S3-Bucket-Richtlinie aktualisieren, ersetzen Sie *red* Felder durch entsprechende Werte:
>
> - *amzn-s3-demo-bucket*mit dem Namen des Amazon S3 S3-Buckets, der die Trail-Ereignisse aus Ihren Konten enthält.
> - *your-organization-id*mit der ID der AWS Organisation, der Ihre Konten angehören.

- *your-optional-s3-log-delievery-prefix*mit dem Amazon S3 S3-Bucket-Lieferpräfix Ihres CloudTrail Trails. Zum Beispiel`my-bucket-prefix`, das Sie möglicherweise bei der Erstellung Ihres CloudTrail Trails festgelegt haben.

  Wenn Sie kein Amazon S3 S3-Bucket-Lieferpräfix für Ihren Trail konfiguriert haben, entfernen Sie "*your-optional-s3-log-delievery-prefix*" und den fortlaufenden Schrägstrich (`/`) aus den folgenden Amazon S3 S3-Bucket-Richtlinienerklärungen.

Die folgenden drei Amazon S3 S3-Bucket-Richtlinienerklärungen gewähren Accelerate Zugriff, um die Konfigurationen von AWS Athena-Abfragen abzurufen und auszuführen, um die CloudTrail Ereignisse in Ihrem Amazon S3 S3-Bucket für die Lieferung von Veranstaltungen von Ihrem Accelerate-Konto aus zu analysieren.

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
```

```
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
```

```
}
```

Überprüfen und aktualisieren Sie die AWS KMS wichtigsten Richtlinien für Ihr Lieferziel für CloudTrail Veranstaltungen

Während des Onboardings arbeiten Sie mit Ihrem Cloud Architect (CA) zusammen, um die AWS KMS Schlüsselrichtlinie zu aktualisieren, die zur Verschlüsselung der CloudTrail Trail-Ereignisse verwendet wird, die an Ihren Amazon S3 S3-Bucket gesendet werden. Stellen Sie sicher, dass Sie die Richtlinienerklärungen zu den AWS KMS Referenzschlüsseln an Ihren vorhandenen Schlüssel anhängen. AWS KMS Dadurch wird Accelerate so konfiguriert, dass es in Ihren vorhandenen Amazon S3 S3-Bucket für die Zustellung von CloudTrail Trail-Ereignissen integriert und Ereignisse entschlüsselt werden. Damit Ihre Benutzer von Ihrem Accelerate-Konto aus Änderungen an Ihrem Amazon S3 S3-Bucket für die Zustellung von CloudTrail Veranstaltungen abfragen können, können Sie für jedes Konto in Ihrer Organisation, das Accelerate verwaltet, eine einheitlich benannte IAM-Rolle bereitstellen und sie der Liste „aws:PrincipalArn“ hinzufügen. Mit dieser Konfiguration können Ihre Benutzer Ereignisse abfragen.

Es gibt verschiedene AWS KMS wichtige Szenarien zur Aktualisierung von Richtlinien, die berücksichtigt werden müssen. Möglicherweise haben Sie nur einen AWS KMS Schlüssel für Ihren CloudTrail Trail konfiguriert, um alle Ereignisse zu verschlüsseln, und keinen AWS KMS Schlüssel, der Objekte in Ihrem Amazon S3 S3-Bucket verschlüsselt. Oder vielleicht haben Sie einen AWS KMS Schlüssel, der Ereignisse verschlüsselt, die von übermittelt wurden CloudTrail, und einen anderen AWS KMS Schlüssel, der alle in Ihrem Amazon S3 S3-Bucket gespeicherten Objekte verschlüsselt. Wenn Sie über zwei AWS KMS Schlüssel verfügen, aktualisieren Sie die AWS KMS Schlüsselrichtlinie für jeden Schlüssel, um Accelerate Zugriff auf Ihre CloudTrail Ereignisse zu gewähren. Stellen Sie sicher, dass Sie die AWS KMS Referenzschlüsselrichtlinie an Ihre bestehende AWS KMS wichtige Richtlinie anpassen, bevor Sie die Richtlinie aktualisieren. Weitere Informationen zum Aktualisieren einer AWS KMS wichtigen Richtlinie finden Sie unter Ändern einer wichtigen Richtlinie im AWS Key Management Service Benutzerhandbuch.

> **Important**
>
> Sie müssen Ihre AWS KMS Schlüsselrichtlinie nur aktualisieren, wenn Accelerate in einen CloudTrail Trail integriert ist, bei dem die SSE-KMS-Verschlüsselung für Protokolldateien aktiviert ist.

> **Note**
>
> Bevor Sie diese AWS KMS wichtige Richtlinienerklärung auf den Schlüssel anwenden, der AWS KMS zur Verschlüsselung Ihrer an Ihren Amazon S3 S3-Bucket übermittelten AWS CloudTrail Ereignisse verwendet wird, ersetzen Sie die folgenden *red* Felder durch die entsprechenden Werte:
>
> - *YOUR-ORGANIZATION-ID*mit der ID der AWS Organisation, der Ihre Konten angehören.

Diese AWS KMS wichtige Grundsatzerklärung gewährt Accelerate Zugriff auf die Entschlüsselung und Abfrage von Trail-Ereignissen, die von jedem Konto in Ihrer Organisation an den Amazon S3 S3-Bucket gesendet werden, wobei der Zugriff auf Athena beschränkt ist und von Accelerate zur Abfrage und Analyse CloudTrail von Ereignissen verwendet wird. .

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Die Vorlage zum Erstellen von AMS-Rollen

Die folgende AMS-Rolle gewährt Ihrem AMS-Cloud-Architekten (CA) Berechtigungen. Die folgende ZIP-Datei enthält Terraform-Code und eine CloudFormation Vorlage, die die Erstellung der IAM-Rolle, der Berechtigungsrichtlinie und der Vertrauensrichtlinie vereinfachen. Weitere Informationen erhalten Sie von Ihrer CA.

Name der Rolle	Erforderlich von	Mustervorlagen
`aws_managedservices_onboarding_role`	Nur AMS-Personal beim Onboarding	onboarding_role_minimal.zip

> **Note**
>
> Nachdem Sie eine Beispielvorlage (eine pro Rolle) ausgewählt und heruntergeladen haben, laden Sie diese als Definitionen von CloudFormation Stacks in Erstellen `aws_managedservices_onboarding_role` mit CloudFormation for Accelerate hoch.

Erstellen **`aws_managedservices_onboarding_role`** mit CloudFormation for Accelerate

Sie können die AWS Identity and Access Management Rolle,`aws_managedservices_onboarding_role`, mit CloudFormation dem AWS-Managementkonsole erstellen. Oder Sie können Befehle von verwenden AWS CloudShell , um die Rolle bereitzustellen.

Verwenden Sie die AWS-Managementkonsole

> **Note**
>
> Bevor Sie beginnen, sollten Sie für jede Rolle eine JSON- oder YAML-Datei zum Hochladen bereithalten. Weitere Informationen finden Sie unter Die Vorlage zum Erstellen von AMS-Rollen.

Gehen Sie wie folgt vor AWS-Managementkonsole, um die Rolle aus der zu erstellen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.

2. Wählen Sie Stack erstellen > Mit neuen Ressourcen (Standard). Sie sehen die folgende Seite.

3. Wählen Sie Vorlagendatei hochladen, laden Sie die JSON- oder YAML-Datei der IAM-Rolle hoch und wählen Sie dann Weiter. Sie sehen die folgende Seite.

4. Geben Sie den Stacknamen "**`ams-onboarding-role`**" in das Feld Stackname ein. Geben Sie ein DateOfExpiryim Format „YYYY-MM-DDT 00:00:00 Z“ ein (30 Tage ab dem aktuellen Datum werden empfohlen). Scrollen Sie weiter nach unten und wählen Sie Weiter, bis Sie diese Seite erreichen:

5. Vergewissern Sie sich, dass das Kontrollkästchen aktiviert ist, und wählen Sie dann Stapel erstellen aus.
6. Stellen Sie sicher, dass der Stack erfolgreich erstellt wurde.

Verwenden Sie Befehle von AWS CloudShell

Um die `aws_managedservices_onboarding_role` IAM-Rolle bereitzustellen, führen Sie den folgenden Befehl in AWS CloudShellaus:

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

Nachdem Sie die Rolle erstellt haben, arbeiten Sie mit Ihrem Cloud Architect (CA) zusammen, um den Schritt 2. Einführung von Verwaltungsressourcen in Accelerate Vorgang abzuschließen. Nachdem AMS Sie darüber informiert hat, dass Ihr Konto aktiv ist, sind Sie bereit, Ihre Instances zu integrieren.

Schritt 3. Onboarding von AMS-Funktionen mit Standardrichtlinien

In dieser Phase integrieren Sie AMS-Funktionen mit Standardrichtlinien. Dazu gehören das Hinzufügen von EC2 Amazon-Instances und die Konfiguration von Monitoring, Backup, AWS Config Remediation und Patch (falls zutreffend, AMS Patch Orchestrator ist ein Add-on, das Sie ausdrücklich anfordern müssen) gemäß Ihren Präferenzen. Sie können dies selbst tun oder verlangen, dass AMS Funktionen auf der Grundlage Ihrer Eingaben einbaut. Um Hilfe von AMS anzufordern, erstellen Sie eine Serviceanfrage und geben Sie alle erforderlichen Eingaben ein, um die Aufgabe abzuschließen. Denken Sie daran, dass Serviceanfragen nicht sofort gelöst werden.

> **Note**
>
> Ein Konto kann zwar Standardrichtlinien für Backup, Patch oder Überwachung verwenden, aber Ressourcen müssen markiert werden, damit die entsprechende Richtlinie wirksam wird.

Themen

- (Optional) Schnellstart-Vorlage in Accelerate
- Onboarding Beschleunigen Sie die Überwachung
- EC2 Instances zur Beschleunigung einbinden

- Einführung AWS Backup in Accelerate
- Onboarding-Patching in Accelerate
- Berichte über Nichtkonformitäten in Accelerate überprüfen

(Optional) Schnellstart-Vorlage in Accelerate

Die Quick Start-Vorlage automatisiert die Bereitstellung und Konfiguration von AMS Resource Tagger in AWS Accelerate-fähigen Konten. Diese Vorlage spart Zeit und Mühe im Vergleich zur manuellen Einrichtung. Verwenden Sie diese Vorlage unverändert, um die Grundlagen für Überwachung, Patching und Backup in einem Konto zu definieren. Oder verwenden Sie es, StackSet um Einstellungen auf alle Organisationseinheiten anzuwenden, um die Einstellungen für mehrere Konten zu standardisieren.

Sie können es auch als Ausgangspunkt verwenden, um Ihr eigenes benutzerdefiniertes AMS Resource Tagger-Profil zu erstellen und Auszüge aus der Dokumentation zu verwenden, um komplexere Definitionen für Tagging zu erstellen.

Funktionalität der Schnellstart-Vorlage

Mit der Schnellstart-Vorlage werden die folgenden Aufgaben ausgeführt:

- Erstellt eine Konfigurationsversion für AMS Resource Tagger und stellt sie bereit.
- Wendet Tags auf EC2 Amazon-Instances an, die das AMS-Management und die Erstellung von Überwachungsressourcen ermöglichen.
- (Optional) Wendet Tags auf verwaltete EC2 Instances an, sodass diese nach einem gewünschten Zeitplan gepatcht werden können, und erstellt ein Patch-Wartungsfenster, um das Patchen zu erleichtern.

  > **Warning**
  >
  > Standardmäßig werden Instanzen neu gestartet und gestoppte Instanzen werden automatisch für die Patch-Installation gestartet.

- (Optional) Wendet Tags auf verwaltete EC2 Instances an, sodass diese gemäß der Definition im standardmäßigen AMS-Backup-Plan gesichert werden können.
- (Optional) Wendet Tags auf verwaltete Amazon Relational Database Service (Amazon RDS) -Ressourcen an, sodass sie gemäß dem erweiterten Backup-Plan gesichert werden können. Ein Backup-Plan ermöglicht auch Point-in-Time-Recovery (PITR) für Amazon RDS. Wenn das

automatische Amazon RDS-Backup nicht aktiviert ist, wird die Datenbank kurz vor dem nächsten Backup-Fenster neu gestartet.

Überschreibungen und Ausschlüsse von Quick Start-Vorlagen

Nachdem Sie diese Vorlage verwendet haben, um einen Quick Start-Stack zu erstellen, gehen Sie wie folgt vor, um bestimmte Instanzen von Management/Monitoring, Patching oder Backup auszuschließen:

- Verwaltung und Überwachung: Um eine EC2 Instanz von der Verwaltung und Überwachung durch AMS auszuschließen, fügen Sie der Instanz dieses Tag hinzu:. `ExcludeFromAMSQuickStartMonitoring=true`
- Patchen: EC2 Instances, die Mitglieder einer Auto Scaling Scaling-Gruppe, eines Amazon Elastic Container Service- oder Amazon Elastic Kubernetes Service Service-Clusters sind, werden durch diese Quick Start-Vorlage vom Patchen ausgeschlossen.

  Um die Erstellung eines Patching-Fensters und das patch-bezogene Tagging von Instances zu deaktivieren, setzen Sie den Stack-Parameter auf. EC2 CloudFormation `EnablePatching=false`

  Wenn Sie ausschließen möchten, dass eine EC2 Instanz vom Schnellstart-Patchfenster als Ziel ausgewählt wird`EnablePatching=true`, fügen Sie der Instanz dieses Tag hinzu:. `ExcludeFromAMSQuickStartPatching=true`
- Backup: EC2 Instances, die Mitglieder einer Auto Scaling Scaling-Gruppe, eines ECS- oder EKS-Clusters sind, werden durch diese Schnellstart-Vorlage vom Backup ausgeschlossen.

  Um auszuschließen, dass eine EC2 Instance vom standardmäßigen AMS-Backup-Plan als Ziel ausgewählt wird`EnableBackup=true`, wenn, fügen Sie dieser Instance dieses Tag hinzu:`ExcludeFromAMSQuickStartBackup=true`.

> **Tip**
>
> Sie können EC2 Instances in großen Mengen taggen. Verwenden Sie den Tag-Editor, um Ressourcen in einem Schritt massenweise auszuwählen und zu taggen. AWS-Managementkonsole

Parameter der Schnellstart-Vorlage

Diese Schnellstart-Vorlage konfiguriert Resource Tagger so, dass das Tag `ams:rt:ams-managed=true` allen EC2 Instanzen im Konto hinzugefügt wird, mit Ausnahme der Instanzen, denen Sie das `ExcludeFromAMSQuickStartMonitoring=true` Tag hinzufügen. Verwenden Sie die folgenden Parameter, um die optionalen Teile dieses Stacks Ihren Anforderungen entsprechend zu steuern:

CFN-Parameter	Wert	Auswirkung
EnableBackup	'wahr' (Standard)	Alle AMS-verwalteten EC2 Instanzen (`ams:rt:ams-managed=true`) sind gemäß dem standardmäßigen AMS-Backup-Plan `ams:rt:backup-orchestrator=true` für tägliche Backups um 4 Uhr UTC gekennzeichnet. Für alle RDS-Instances und -Cluster wendet die Vorlage das `ams:rt:backup-orchestrator-enhanced=true` „kontinuierliche Backup“ mit maximaler Aufbewahrung (31 Tage) gemäß dem erweiterten Backup-Plan an. Wenn sich dadurch Ihre PITR-Aufbewahrungsfrist ändert, wird die Datenbank in einigen Fällen möglicherweise neu gestartet, z. B. wenn weitere Konfigurationsupdates ausstehen.
	'falsch'	Diese Schnellstartvorlage zielt nicht auf ein Backup von Instanzen ab.

CFN-Parameter	Wert	Auswirkung
EnablePatching	'false' (Standard)	Diese Schnellstart-Vorlage zielt nicht auf das Patchen von Instanzen ab.
	'wahr'	Alle vom AMS verwalteten Instanzen (`ams:rt:ams-managed=true`) sind mit gekennzeichnet, `ams:rt:Patch Group=AMSQuickStartPatchWindow` und es wird eine grundlegende SSM-Wartungsfenster-Ressource erstellt, um das Patchen gemäß dem unter definierten Zeitplan zu erleichtern. `CronExpression` Um das `ams:rt:Patch Group` Tag auf die EC2 Instanz anzuwenden, müssen Sie den Zugriff auf Tags in den Instanz-Metadaten für diese Instanz deaktivieren.
CronExpression	-	Der Standardwert von `cron(0 30 19 ? * SAT#2 *)` legt den zweiten Samstag des Monats entsprechend dem `Timezone` Parameter um 19:30 Uhr fest. Verwenden Sie die Cron-Syntax.
Zeitzone	-	Zielinstanzen werden entsprechend gepatcht. `CronExpression` Verwenden Sie das IANA-Format.

Laden Sie die Schnellstart-Vorlage herunter

Laden Sie die Datei AMSQuick Start.zip herunter.

Oder führen Sie den folgenden Befehl aus AWS CloudShell, um Folgendes bereitzustellen`AMSQuickStart.yaml`:

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

Eine Beschreibung der einzelnen Parameter finden Sie im vorherigen Abschnitt,Parameter der Schnellstart-Vorlage.

Onboarding Beschleunigen Sie die Überwachung

Die Überwachung ist standardmäßig für alle neuen Ressourcen außer EC2 Amazon-Instances aktiviert. Sie können mit der Überwachung Ihrer EC2 Amazon-Instances beginnen, indem Sie Ihre Instances taggen.

Um die Überwachung zu integrieren, stellen Sie zunächst sicher, dass Ihre Konfiguration die Ressourcen überwacht, die AMS überwachen soll, und die Ressourcen ignoriert, die von AMS ignoriert werden sollen.

Mithilfe der folgenden CloudWatch Dashboards können Sie herausfinden, auf wie viele Ihrer Ressourcen das AMS-Monitoring und -Tagging abzielt und auf wie viele nicht. Navigieren Sie in Ihrem Konto zur CloudWatch Dashboard-Konsole und wählen Sie eine der folgenden Optionen aus:

- AMS-Alarm-Manager-Berichts-Dashboard
- AMS-Resource-Tagger-Berichts-Dashboard

Eine vollständige Beschreibung der Dashboard-Metriken finden Sie unter:

- Anzahl der von Alarm Manager for Accelerate überwachten Ressourcen anzeigen
- Die Anzahl der von Resource Tagger verwalteten Ressourcen anzeigen

Onboarding-Ressourcen, die in Accelerate überwacht werden sollen

Um das Standardverhalten zu überschreiben, z. B. um die Standardüberwachung für EC2 Nicht-Ressourcen zu deaktivieren, müssen Sie die Markierung dieser Ressourcen mithilfe eines benutzerdefinierten Konfigurationsprofils aufheben. Weitere Informationen zum Tagging für die Überwachung finden Sie unter. Überwachung in Accelerate

Die Überwachung ist für EC2 Instances deaktiviert, bis Sie Ihre Instances einbinden. Dazu gehört auch das Taggen Ihrer Instances mithilfe eines benutzerdefinierten Konfigurationsprofils. Im nächsten Abschnitt wird das Onboarding von EC2 Instanzen beschrieben.

Erstellen eines Monitoring-Konfigurationsprofils in Accelerate

- Hinweise zur Verwendung der Standardkonfiguration finden Sie unterBeschleunigen Sie den Alarm Manager.
- Hinweise zur Verwendung einer benutzerdefinierten Konfiguration finden Sie unterÄndern der Standardkonfiguration des Beschleunigungsalarms.

EC2 Instances zur Beschleunigung einbinden

EC2 Instances werden über einen Prozess namens Automated Instance Configuration in AMS Accelerate integriert. Dabei wird sichergestellt, dass jede Instance die richtigen Logs schreibt und die richtigen Metriken ausgibt, damit AMS die Instance ordnungsgemäß verwalten kann. Sie sollten alle Ihre EC2 Instances einbinden, es sei denn, Sie möchten ausdrücklich, dass AMS einige ignoriert. Für die automatische Instanzkonfiguration müssen bestimmte Bedingungen erfüllt sein, die es AMS ermöglichen, die Instance zu konfigurieren (weitere Informationen finden Sie unterVoraussetzungen für die automatisierte Instanzkonfiguration in Accelerate). Die wichtigste Bedingung ist, dass der AWS Systems Manager Agent (SSM-Agent) auf jeder EC2 Amazon-Instance installiert werden muss, die AMS für Sie verwalten soll. Weitere Informationen zum SSM-Agenten finden Sie unter Mit dem SSM-Agenten arbeiten.

SSM ist standardmäßig für Accelerate vorinstalliert AMIs

Der SSM-Agent ist bereits installiert auf AWS-bereitgestellt AMIs für die folgenden Betriebssysteme.

- Amazon Linux und Amazon Linux 2
- SUSE Linux Enterprise Server (SLES) 12 und 15
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012
- Ubuntu Linux 18.04 und 20.04

Wenn Sie eines der bereitgestellten Programme verwenden, finden Sie weitere Informationen unter. AWS AMIs Markieren von Instanzen in Accelerate

Manuelle SSM-Installation von SSM in Accelerate

Für die folgenden Betriebssysteme oder wenn Sie ein benutzerdefiniertes AMI verwenden, können Sie den SSM-Agenten manuell installieren. Sie können auch die auto Installationsfunktion des AMS SSM Agents verwenden. Weitere Informationen zur auto Installation von SSM finden Sie unterAutomatische Installation des SSM-Agenten. Anweisungen zur manuellen Installation finden Sie unter dem Link für Ihr Betriebssystem:

- CentOS SSM-Installation
- Installation von Oracle SSM
- Installation von Red Hat SSM
- Installation von SUSE Linux Enterprise Server SSM
- Installation von Windows SSM

Markieren von Instanzen in Accelerate

Nach der Installation des SSM-Agenten müssen Sie Ihre Instanzen taggen. Siehe Taggen in AMS Accelerate.

Automatisierte Instanzkonfiguration in Accelerate

Sobald Ihre Instance markiert ist, führt AMS eine automatisierte Instance-Konfiguration durch, die Folgendes beinhaltet:

- Protokollierung und Metriken des Betriebssystems aufzeichnen
- Ermöglichen Sie den Fernzugriff für AMS-Techniker
- Führen Sie Fernbefehle auf der Instanz aus

Diese Aufgaben sind für die Überwachungs-, Patch- und Protokolldienste von AMS sowie für die Reaktion von AMS auf Vorfälle unerlässlich. Einzelheiten zur Einrichtung der automatisierten Instanzkonfiguration finden Sie unterAutomatisierte Instanzkonfiguration in AMS Accelerate.

Nachdem die automatische Instanzkonfiguration abgeschlossen ist, können Sie:

- Erstellen Sie mithilfe der Support Center-Konsole Vorfälle und Serviceanfragen für EC2 Amazon-Instances und Betriebssysteme. Weitere Informationen finden Sie unter Vorfallberichte, Serviceanfragen und Fragen zur Abrechnung in AMS Accelerate.
- Zugriff und Prüfung von EC2 Amazon-Protokollen
- Besorgen Sie sich Patch-Berichte

Einführung AWS Backup in Accelerate

Um Backups zu konfigurieren, müssen Sie Backup-Richtlinien, sogenannte Backup-Pläne, erstellen. Ein Backup-Plan gibt an, welche AWS Ressourcen gesichert werden sollen, wie oft sie gesichert werden müssen und wie lange Backups aufbewahrt werden. Wir empfehlen, die Kontinuitäts-, Sicherheits- und Compliance-Anforderungen Ihres Unternehmens zu überprüfen, um festzustellen, welche Backup-Pläne Sie benötigen.

Melden Sie sich an

- Stellen Sie sicher, dass AWS Backup dies für jedes Konto, jede Region und jeden Ressourcentyp aktiviert ist, indem Sie die folgenden Schritte ausführen:

Erste Schritte 1: Service-Opt-In.

Optional: Erste Schritte 2: Backup auf Abruf erstellen.

Wählen Sie einen Backup-Plan

- Informationen zur Auswahl eines Backup-Plans finden Sie unterWählen Sie einen AMS-Backup-Plan.

Ressourcen hinzufügen

Ressourcen sind standardmäßig keinem Backup-Plan zugeordnet. Sie müssen einem Backup-Plan hinzugefügt werden.

- Informationen zum Hinzufügen von Ressourcen zu einem Backup-Plan finden Sie unterKennzeichnen Sie Ihre Ressourcen, um AMS-Backup-Pläne anzuwenden.
- Informationen zum Aktivieren von Backups für alle Ressourcen mithilfe von Tags finden Sie unterVerwaltung von Tags für Backups in Accelerate.

Onboarding-Patching in Accelerate

Sie müssen das Patchen konfigurieren, um sicherzustellen, dass Ihre Software Ihren Compliance-Richtlinien entspricht up-to-date und diese erfüllt.

AWS Backup Voraussetzung: Um die Erstellung eines Root-Volume-Snapshots während des Patch-Wartungsfensters zu ermöglichen, stellen Sie sicher, dass dieser für jedes Konto und jede Region für den Amazon EBS-Ressourcentyp aktiviert AWS Backup ist. Gehen Sie dazu wie folgt vor: Erste Schritte 1: Service Opt-In. (Sie müssen nicht mit Erste Schritte 2: Ein On-Demand-Backup erstellen fortfahren.)

Wann sollte gepatcht werden: Das Patchen erfolgt während eines Wartungsfensters. Sie können Wartungsfenster so planen, dass Patches nur zu festgelegten Zeiten angewendet werden.

Was gepatcht werden muss: Sie müssen die EC2 Amazon-Instances, die Sie patchen möchten, mit einem Wartungsfenster verknüpfen. Um die Instances einem Wartungsfenster zuzuordnen, müssen die EC2 Amazon-Instances markiert werden, und das Wartungsfenster sollte diese Tags als Ziel haben.

Welche Patches installiert werden sollen: Mithilfe von Patch-Baselines legen Sie Regeln für die automatische Genehmigung bestimmter Arten von Patches fest, z. B. Betriebssystem-Patches oder Patches mit hohem Schweregrad. Sie können auch Ausnahmen von Ihren Regeln angeben, z. B. Listen von Patches, die immer genehmigt oder abgelehnt werden.

Anleitungen Empfehlungen zum Patchen zu den EC2 Amazon-Patch-Richtlinien finden Sie unter.

- Informationen zum Starten der Konfiguration des Patch-Managements finden Sie unter Patch-Management in AMS Accelerate verstehen
- Informationen zum Erstellen einer benutzerdefinierten Patch-Konfiguration finden Sie unterBenutzerdefinierte Patch-Baseline mit AMS Accelerate.

Berichte über Nichtkonformitäten in Accelerate überprüfen

AMS setzt AWS Config Regeln ein, mit deren Hilfe Sie Verstöße gegen Standards erkennen können, die vom Center for Internet Security (CIS), dem National Institute of Standards and Technology (NIST), vom Cloud Security Framework (CSF) festgelegt wurden. Wir empfehlen Ihnen, den Bericht über die Nichtkonformität mit Ihrem Bereitstellungsteam zu überprüfen, um Maßnahmen zur Behebung zu priorisieren, damit Ihr Konto als konform eingestuft wird.

Schritt 4. Passen Sie Funktionen in Accelerate an

In dieser Phase haben Sie bereits Überwachung, Patching und Backup mit Standardrichtlinien integriert. Jetzt haben Sie die Möglichkeit, Richtlinien an Ihre Bedürfnisse anzupassen.

Sie können wählen, ob Sie die Standardrichtlinien für Patches, Backups oder Überwachung verwenden oder eine benutzerdefinierte Richtlinie auswählen möchten, die Ihren Anforderungen entspricht. AMS verwendet Tags, um Ressourcen betrieblichen Richtlinien zuzuordnen. AMS bietet einen Resource Tagger, mit dem Sie Regeln dafür festlegen können, wie Tags auf Ihre AWS Ressourcen angewendet werden, basierend auf Anwendungsgruppierung oder anderer Gruppierungslogik. Weitere Informationen finden Sie unter. Beschleunigen Sie Resource Tagger

Mit der vom Kunden bereitgestellten Tags-Funktion können Sie benutzerdefinierte Tags zu AMS-Ressourcen hinzufügen und löschen. Weitere Informationen finden Sie unter Vom Kunden bereitgestellte Tags in Accelerate.

Themen

- Passen Sie die Überwachung in Accelerate an

- Passen Sie das Backup in Accelerate an
- Passen Sie das Patchen in Accelerate an

Passen Sie die Überwachung in Accelerate an

So passen Sie die Überwachung Ihrer Cloud-Ressourcen an Ihre Anwendungsanforderungen an:

1. Erstellen Sie eine benutzerdefinierte Überwachungsrichtlinie. Siehe Ändern der Standardkonfiguration des Beschleunigungsalarms.
2. Wenden Sie mithilfe von Tags eine benutzerdefinierte Richtlinie auf Ressourcen an. Siehe Überwachung in Accelerate
3. Leiten Sie Benachrichtigungen an den Besitzer der Ressource weiter. Siehe Tag-basierte Warnmeldung.

Mithilfe der folgenden CloudWatch Dashboards können Sie herausfinden, auf wie viele Ihrer Ressourcen das AMS-Monitoring und -Tagging abzielt und auf wie viele nicht. Navigieren Sie in Ihrem Konto zur CloudWatch Dashboard-Konsole und wählen Sie eine der folgenden Optionen aus:

- AMS-Alarm-Manager-Berichts-Dashboard
- AMS-Resource-Tagger-Berichts-Dashboard

Eine vollständige Beschreibung der Dashboard-Metriken finden Sie unter:

- Anzahl der von Alarm Manager for Accelerate überwachten Ressourcen anzeigen
- Die Anzahl der von Resource Tagger verwalteten Ressourcen anzeigen

Passen Sie das Backup in Accelerate an

Sie können die Standard-Backup-Pläne von AMS nicht anpassen. Erstellen Sie stattdessen einen neuen Backup-Plan, der auf Ihren Anwendungsanforderungen basiert, und fügen Sie dann mithilfe von Tags Ressourcen zu Ihrem benutzerdefinierten Plan hinzu. Es liegt an Ihnen, zu entscheiden, welche Ressourcen AMS wie oft und für welchen Aufbewahrungszeitraum sichern soll. Wir empfehlen, die Kontinuitäts-, Sicherheits- und Compliance-Anforderungen Ihres Unternehmens zu bewerten, um festzustellen, welche Backup-Pläne Sie benötigen.

- Informationen zum Erstellen eines Backup-Plans finden Sie unter Erstellen eines Backup-Plans.

- Informationen zum Zuweisen von Ressourcen zu einem Backup-Plan finden Sie unter Ressourcen einem Backup-Plan zuweisen.

Passen Sie das Patchen in Accelerate an

Durch das Patchen wird sichergestellt, dass Ihre Software Ihren Compliance-Richtlinien entspricht up-to-date und diese erfüllt.

Wann sollte gepatcht werden: Das Patchen erfolgt während eines Wartungsfensters. Sie können Wartungsfenster so planen, dass Patches nur zu festgelegten Zeiten angewendet werden.

Was gepatcht werden muss: Sie müssen die EC2 Amazon-Instances, die Sie patchen möchten, mit einem Wartungsfenster verknüpfen. Um die Instances einem Wartungsfenster zuzuordnen, müssen die EC2 Amazon-Instances markiert werden, und das Wartungsfenster sollte diese Tags als Ziel haben.

Welche Patches installiert werden sollen: Mithilfe von Patch-Baselines legen Sie Regeln für die automatische Genehmigung bestimmter Arten von Patches fest, z. B. Betriebssystem-Patches oder Patches mit hohem Schweregrad. Sie können auch Ausnahmen von Ihren Regeln angeben, z. B. Listen von Patches, die immer genehmigt oder abgelehnt werden.

- Allgemeine Empfehlungen zum Patchen finden Sie unterEmpfehlungen zum Patchen.
- Informationen zum Erstellen benutzerdefinierter Wartungsfenster finden Sie unterErstellen Sie ein Patch-Wartungsfenster in AMS.
- Informationen zum Erstellen benutzerdefinierter Patch-Baselines finden Sie unter. Benutzerdefinierte Patch-Baseline mit AMS Accelerate
- Informationen zum Weiterleiten von Patch-Benachrichtigungen an den Besitzer der Ressource finden Sie unter. Verstehen Sie Patch-Benachrichtigungen und Patch-Fehler in AMS Accelerate

Verwendung der AMS-Konsolen

Die AMS-Konsolen in der AWS Management Console stehen Ihnen zur Verfügung, um mit AMS zu interagieren und Ihre von AMS Advanced-verwalteten Ressourcen und AMS Accelerate-Ressourcen zu bedienen. Die AMS-Konsolen verhalten sich im Allgemeinen wie jede andere AWS Konsole. Da AMS jedoch eine private Organisation ist, können nur Konten, die für AMS aktiviert sind, auf die Konsole zugreifen. Sobald AMS in Ihrem Konto aktiviert ist, können Sie auf die Konsole zugreifen, indem Sie in der einheitlichen Suchleiste nach „Managed Services“ suchen.

> **Note**
>
> Abhängig von Ihrer Kontorolle greifen Sie auf die AMS Advanced-Konsole oder die AMS Accelerate-Konsole zu.

Beachten Sie bei der Verwendung der AMS-Konsolen die folgenden Einschränkungen:

- Die AMS-Konsole ist kontospezifisch. Wenn Sie also ein „Test“ -Konto für Ihre Organisation haben, können Sie im „Prod“ -Konto für diese Organisation keine Ressourcen sehen. Ebenso benötigen Sie eine AMS-Advanced-Rolle, um auf die AMS Advanced-Konsole zugreifen zu können.
- Die AMS-Konsolen wenden bei der Authentifizierung eine IAM-Richtlinie an, die festlegt, auf welche Konsole Sie zugreifen können und was Sie dort tun können. Ihr Administrator kann zusätzliche Richtlinien auf die AMS-Standardrichtlinie anwenden, um einzuschränken, was Sie in der Konsole sehen und tun können.

Die AMS Accelerate-Konsole bietet die folgenden Funktionen:

- Erste Seite: Die erste Seite enthält Informationsfelder und Links, die Ihnen den Zugriff auf Ihre Serviceanfragen und Berichte erleichtern.
- Feature-Seiten, Links im linken Navigationsbereich:
  - Dashboard: Bietet einen Überblick über den aktuellen Status Ihres Kontos, einschließlich:
    - Vorfälle in Ihren Ressourcen: Eine Schaltfläche zum Öffnen eines Incident-Falls im AWS Support Center sowie darüber, wie viele Incident-Fälle noch auf Genehmigung warten und Ihre Aufmerksamkeit erfordern, und wie viele noch offen sind
    - Compliance-Status: Links zu Regeln und Ressourcen, die nicht konform oder konform sind
    - Serviceanfragen: Eine Schaltfläche zum Öffnen einer Serviceanfrage im AWS Support Center sowie darüber, wie viele auf Genehmigung warten und Ihre Aufmerksamkeit erfordern, und wie viele offen sind
    - Sicherheit auf Kontoebene: Links zu Einzelheiten zu den Ergebnissen der Bedrohungserkennung in Echtzeit und den GuardDuty Ergebnissen von Macie zu Datensicherheit und Datenschutz
    - Schnelle Aktionen: Öffnen Sie die Konfigurationsseiten Ihrer Backup-Tresore oder Patch-Instanzen

  - Berichte: Öffnet die Seite „Berichte“ und die Standardberichte „Tägliches Backup“ und „Tägliches Patch“ und „Monatliche Abrechnung“
  - Konfiguration: Stellen Sie sicher, dass Ihre Ressourcen erfolgreich und gemäß Ihren Spezifikationen verwaltet werden.
    - SSM-Agent installieren: Der SSM-Agent ist erforderlich
    - Tagging-Regeln konfigurieren: Öffnet AMS Resource Tagger
    - Alarme konfigurieren: Öffnet die CloudWatch AMS-Alarmkonfiguration
    - Patch-Zeitplan konfigurieren: Öffnet die AWS Systems Manager Manager-Konsole
    - Patch-Baselines konfigurieren: Öffnet die AWS Patch Manager-Konsole
    - Backup-Pläne konfigurieren: Öffnet die AWS-Backup-Konsole
- Funktionen im Fokus: Informationen zu den neuesten Updates der Konsole
- Dokumentation: Die Landingpage der AWS Managed Services Services-Dokumentation

AMS-Muster

Ein AWS Managed Services (AMS) -Muster ist eine generalisierte Lösung, die für eine Reihe von Anwendungsfällen in der von AMS verwalteten Umgebung geeignet ist.

Während Sie auf der AMS-Plattform arbeiten, arbeiten die AMS-Cloud-Architekten (CAs) mit Ihnen zusammen, um Ihre geschäftlichen und betrieblichen Anforderungen zu erfüllen. AMS-Kunden arbeiten zwar auf einzigartige Weise, wir stellen jedoch fest, dass Kunden ähnliche Anwendungsfälle haben. CAs Erstellen Sie in solchen Fällen allgemeine Lösungsvorlagen oder „Muster“, die in mehreren Kundenumgebungen mit minimalem Aufwand für Konfiguration und Bereitstellung verwendet werden.

AMS-Muster dienen der Bereitstellung von Funktionen für AMS-Kunden und werden in der Regel von der Account-CA des Kunden erstellt, der sie anfordert.

Wie funktionieren AMS-Muster

Um weitere Informationen zu den einzelnen Mustern, einschließlich der für die Implementierung des Musters erforderlichen Cloudformation-Vorlagen, anzufordern, reichen Sie eine AMS-Serviceanfrage mit dem Betreff „Anfrage nach zusätzlichen Informationen zum Muster*`Pattern_Name`*“ ein (ersetzen Sie das gewünschte Muster) und fügen Sie Ihren AMS-Cloud-Architekten (CA) zur Option Zusätzliche Kontakte hinzu.

AMS-Muster werden in zwei (2) Kategorien eingeteilt:

- Allgemeine Verwendung: Muster gelten als stabil, da sie von mehreren AMS-Kunden bereitgestellt und genutzt wurden
- Vorschaumodus: AMS empfiehlt, Muster im Vorschaumodus zur Validierung in Ihren Umgebungen außerhalb der Produktion einzusetzen und den Anwendungsfall vor der Bereitstellung mit Ihrem Cloud-Architekten zu besprechen.

> **Important**
>
> AMS-Muster entsprechen nicht Ihren standardmäßigen AMS Service Level Agreements, Service Level Agreements (SLAs) und Service Level Objectives (SLOs). Support und Aktualisierungen des Patterns werden nach bestem Wissen und Gewissen durchgeführt. Dieser AWS Inhalt wird gemäß den Bedingungen der AWS Kundenvereinbarung oder einer anderen schriftlichen Vereinbarung zwischen dem Kunden und entweder Amazon Web Services, Inc. oder Amazon Web Services EMEA SARL („AWS Europa“) oder beiden bereitgestellt.
> Das in dieser Software enthaltene Material wird Ihnen „wie es ist“ und ohne jegliche ausdrückliche, stillschweigende oder sonstige Garantie, einschließlich, aber nicht beschränkt auf jegliche Garantie der Eignung für einen bestimmten Zweck, zur Verfügung gestellt.

AMS-Muster

AMS-Muster.

AMS-Muster

Name	Übersicht	Vorteile	Kategorie
Passen Sie CloudWatch Alarmbenachrichtigungen an	Passen Sie die CloudWatch Alarmbenachrichtigungen so an, dass sie Informationen aus Instanz-Tags wie Instanzname,	Das Hinzufügen von Kontextinformationen zu den Alarmbenachrichtigungen macht sie aussagekräftiger und liefert umsetzbare Informationen.	Überwachung

Name	Übersicht	Vorteile	Kategorie
	Anwendungs-ID usw. enthalten.		
Berichterstattung zur Festplattennutzung	Das Disk Usage Reporting-Muster erfasst den Speicherverbrauch von Volumes über mehrere App-Konten hinweg und präsentiert das Ergebnis als zentralisierten Bericht in Amazon S3 mit Athena-Tabellenabfragefunktion.	Bieten Sie Einblicke in die tatsächliche Nutzung von Speichervolumen, um Möglichkeiten zur Kosteneinsparung zu ermitteln.	Kostenoptimierung
Prowler Stack	Führt Prowler-Prüfungen für Konten EC2 bei Amazon durch, die nicht verwendet werden CloudShell können.	Hilft dabei, das Accelerate Onboarding (Prowler) in Fällen zu entsperren, in denen es entweder aufgrund von Berechtigungen oder Timeout-Problemen nicht verwendet werden CloudShell kann, ohne dass dies Auswirkungen auf die aktuelle Sicherheitslage hat.	Sicherheit

Name	Übersicht	Vorteile	Kategorie
AMS Amazon S3 S3-Replikation mit benutzerdefinierten Objektschlüsseln	Erstellen Sie Kopien von Amazon S3 S3-Objekten und behalten Sie alle Metadaten und Objektschlüssel (Ordner) bei. Entfernt einen Teil der Quellobjektschlüssel oder erstellt während der Replikation benutzerdefinierte Zielobjektschlüssel.	Passen Sie die Objektschlüssel (Ordner) während der Amazon S3 S3-Replikation an, ohne dass zusätzliche Skripts erforderlich sind, um Objekte in die erforderlichen Ordner zu verschieben.	Zuverlässigkeit
Löschen von Amazon EBS-Snapshots	Automatisierung auf Basis von Lambda und CloudWatch Events zur Automatisierung des Löschens von Amazon EBS-Snapshots, die außerhalb von aufgenommen wurden AWS Backup, auf der Grundlage der Aufbewahrung.	Helfen Sie dabei, einzelne Snapshots zu löschen, die außerhalb des AWS Backup Orchestrator aufgenommen wurden, und sparen Sie so im Laufe der Zeit zusätzliche Kosten.	Kostenoptimierung

Name	Übersicht	Vorteile	Kategorie
Rotation von AMS Amazon RDS-Geheimnissen	Stellen Sie mithilfe einer CloudFormation Vorlage automatisch alle erforderlichen Ressourcen (Lambda-Funktion, Sicherheitsgruppen, elastische Netzwerkschnittstellen oder ENIs) bereit, die für die Rotation von Geheimnissen für unterstützte Amazon RDS-Datenbanken, Redshift und DocumentDB benötigt werden.	Automatisieren Sie die Rotation von Datenbankgeheimnissen und stellen Sie einen Benachrichtigungsmechanismus bereit, wenn die Rotation fehlschlägt.	Sicherheit
Automatisierte Schlüsselrotation	Automatische Rotation von Zugriffs- und Geheimschlüsseln für IAM-Benutzer auf der Grundlage von CloudWatch Ereignissen und Lambda.	Einfachere Rotation von Zugriffs- und Geheimschlüsseln für IAM-Benutzer.	Sicherheit

Name	Übersicht	Vorteile	Kategorie
Amazon EBS Volume Snapshot Tagger	Taggen Sie alle Amazon EBS-Volumes und -Snapshots mithilfe der Tags in den EC2 Amazon-Instances.	Mithilfe aussagekräftiger, relevanter Geschäftsinformationen können Sie Kosten kategorisieren und nachverfolgen. So können Sie leichter überprüfen, wofür Geld ausgegeben wird, und ermöglichen den Einsatz von Automatisierung für markierte Volumes und Snapshots. Sehr empfehlenswerte bewährte Methode aus dem Bereich AWS Kostenoptimierung.	Tagging (Kostenoptimierung, Sicherheit, Vorfallmanagement und Automatisierung)

Automatisierte Instanzkonfiguration in AMS Accelerate

AMS Accelerate bietet einen automatisierten Service zur Instanzkonfiguration. Dieser Service stellt sicher, dass eine Instance die richtigen Logs und Metriken ausgibt, damit AMS die Instance ordnungsgemäß verwalten kann. Die automatisierte Instanzkonfiguration hat ihre eigenen Voraussetzungen und Schritte für das Onboarding, die später in diesem Abschnitt beschrieben werden.

Themen

So funktioniert die automatisierte Instanzkonfiguration in Accelerate

Durch die automatisierte Instanzkonfiguration kann AMS Accelerate täglich bestimmte Konfigurationen für Instances durchführen, die Sie durch Hinzufügen bestimmter Agenten und Tags angeben.

Voraussetzungen für die automatisierte Instanzkonfiguration in Accelerate

Diese Bedingungen müssen erfüllt sein, damit AMS Accelerate die zuvor beschriebenen automatisierten Aktionen auf verwalteten Instances ausführen kann.

Der SSM-Agent ist installiert

Für die automatische Instanzkonfiguration von AMS Accelerate muss der AWS Systems Manager SSM Agent installiert sein.

Informationen zur Verwendung der auto Installationsfunktion des AMS SSM Agents finden Sie unterAutomatische Installation des SSM-Agenten.

Informationen zur manuellen Installation des SSM-Agenten finden Sie im Folgenden:

- Linux: SSM Agent manuell auf EC2 Amazon-Instances für Linux installieren - AWS Systems Manager
- Windows: SSM Agent manuell auf EC2 Amazon-Instances für Windows Server installieren - AWS Systems Manager

Der SSM-Agent befindet sich im verwalteten Zustand

Für die automatische Instanzkonfiguration von AMS Accelerate ist ein betriebsbereiter SSM-Agent erforderlich. Der SSM-Agent muss installiert sein und die EC2 Amazon-Instance muss sich im verwalteten Status befinden. Weitere Informationen finden Sie in der AWS Dokumentation Arbeiten mit SSM Agent.

Automatisierte Einrichtung der Instanzkonfiguration

Vorausgesetzt, dass die Voraussetzungen erfüllt sind, initiiert das Hinzufügen eines bestimmten EC2 Amazon-Instance-Tags automatisch die automatische AMS Accelerate-Instance-Konfiguration. Verwenden Sie eine der folgenden Methoden, um dieses Tag hinzuzufügen:

1. (Dringend empfohlen) Verwenden Sie den AMS Accelerate Resource Tagger

   Informationen zur Konfiguration der Tagging-Logik für Ihr Konto finden Sie unter. So funktioniert Tagging Nachdem das Tagging abgeschlossen ist, werden Tags und die automatische Instanzkonfiguration automatisch verarbeitet.
2. Manuelles Hinzufügen von Tags

   Fügen Sie den EC2 Amazon-Instances manuell das folgende Tag hinzu:

   Schlüssel: ams:rt:ams-managed, Wert: true.

> **Note**
>
> Der Instanzkonfigurationsdienst versucht, die erforderlichen AMS-Konfigurationen anzuwenden, sobald das ams:rt:ams-managed-Tag auf die Instance angewendet wurde. Der Service bestätigt die für AMS erforderlichen Konfigurationen, wenn eine Instance gestartet wird und wenn eine tägliche AMS-Konfigurationsprüfung stattfindet.

Automatische Installation des SSM-Agenten

Damit AMS Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwaltet, müssen Sie AWS Systems Manager SSM Agent auf jeder Instance installieren. Wenn auf Ihren Instances kein SSM Agent installiert ist, können Sie die Funktion zur automatischen Installation von AMS SSM Agent verwenden.

> **Note**
>
> - Wenn Ihr Konto nach dem 06.03.2024 in AMS Accelerate integriert wurde, ist diese Funktion standardmäßig aktiviert. Um diese Funktion zu deaktivieren, wenden Sie sich an Ihre CA oder CSDM.
> - Um diese Funktion für Konten zu aktivieren, die vor dem 06.03.2024 eingerichtet wurden, wenden Sie sich an Ihre CA oder CSDM.
> - Diese Funktion ist nur für EC2 Instances verfügbar, die nicht zu einer Auto Scaling Scaling-Gruppe gehören und auf denen von AMS unterstützte Linux-Betriebssysteme ausgeführt werden.

Voraussetzungen für die Verwendung des SSM-Agenten

- Stellen Sie sicher, dass das mit den Ziel-Instances verknüpfte Instanzprofil über eine der folgenden Richtlinien verfügt (oder über gleichwertige Berechtigungen, die in den Zielinstanzen aufgeführt sind):
  - Amazon SSMManaged EC2 InstanceDefaultPolicy
  - Amazon SSMManaged InstanceCore
- Stellen Sie sicher, dass es keine Service Control-Richtlinie auf der AWS Organizations Ebene gibt, die die in den vorherigen Richtlinien aufgeführten Berechtigungen ausdrücklich verweigert.

  Weitere Informationen finden Sie unter Erforderliche Instance-Berechtigungen für Systems Manager konfigurieren.
- Um ausgehenden Datenverkehr zu blockieren, stellen Sie sicher, dass die folgenden Schnittstellenendpunkte auf der VPC aktiviert sind, auf der sich die Ziel-Instances befinden (ersetzen Sie „Region“ in der URL entsprechend):
  - ssm.<region>.amazonaws.com
  - ssmmessages.<region>.amazonaws.com
  - ec2-Nachrichten. <region>.amazonaws.com

  Weitere Informationen finden Sie unter Verbessern der Sicherheit von EC2 Instances mithilfe von VPC-Endpunkten für Systems Manager.

Allgemeine Tipps zur Aktivierung oder Fehlerbehebung bei der Verfügbarkeit verwalteter Knoten finden Sie unter Lösung 2: Stellen Sie sicher, dass ein IAM-Instanzprofil für die Instanz angegeben wurde (nur EC2 Instanzen).

> **Note**
>
> AMS stoppt und startet jede Instanz im Rahmen der automatischen Installation. Wenn eine Instance gestoppt wird, gehen die auf den Instance-Speicher-Volumes gespeicherten Daten und die im RAM gespeicherten Daten verloren. Weitere Informationen finden Sie unter Was passiert, wenn Sie eine Instance beenden.

Fordern Sie die automatische Installation des SSM-Agenten auf Ihren Instances an

Wenn Ihre Konten in das AMS Accelerate Patch Add-On integriert sind, konfigurieren Sie ein Patch-Wartungsfenster (MW) für die Instances. Ein funktionierender SSM-Agent ist erforderlich, um den Patch-Vorgang abzuschließen. Wenn der SSM-Agent auf einer Instanz fehlt, versucht AMS, ihn während des Patch-Wartungsfensters automatisch zu installieren.

> **Note**
>
> AMS stoppt und startet jede Instanz im Rahmen der automatischen Installation. Wenn eine Instance gestoppt wird, gehen die auf den Instance-Speicher-Volumes gespeicherten Daten und die im RAM gespeicherten Daten verloren. Weitere Informationen finden Sie unter Was passiert, wenn Sie eine Instance beenden.

So funktioniert die automatische Installation des SSM-Agenten

AMS verwendet EC2 Benutzerdaten, um das Installationsskript auf Ihren Instances auszuführen. Um das Benutzerdatenskript hinzuzufügen und es auf Ihren Instances auszuführen, muss AMS jede Instance beenden und starten.

Wenn Ihre Instance bereits über ein Benutzerdatenskript verfügt, führt AMS während des auto Installationsvorgangs die folgenden Schritte aus:

1. Erstellt eine Sicherungskopie des vorhandenen Benutzerdatenskripts.
2. Ersetzt das vorhandene Benutzerdatenskript durch das SSM-Agent-Installationsskript.
3. Startet die Instanz neu, um den SSM Agent zu installieren.
4. Stoppt die Instanz und stellt das ursprüngliche Skript wieder her.
5. Startet die Instanz mit dem Originalskript neu.

Automatisierte Änderungen der Instanzkonfiguration

Die Automatisierung der AMS Accelerate-Instance-Konfiguration nimmt die folgenden Änderungen in Ihrem Konto vor:

1. IAM-Berechtigungen

Fügt die von IAM verwalteten Richtlinien hinzu, die erforderlich sind, um der Instanz die Erlaubnis zu erteilen, die von AMS Accelerate installierten Agenten zu verwenden.

2. Agent
   a. Der CloudWatch Amazon-Agent ist für die Ausgabe von Betriebssystemprotokollen und Metriken verantwortlich. Die Automatisierung der Instance-Konfiguration stellt sicher, dass der CloudWatch Agent installiert ist und die AMS Accelerate-Mindestversion ausführt.
   b. Der AWS Systems Manager SSM-Agent ist für die Ausführung von Remote-Befehlen auf der Instance verantwortlich. Die Automatisierung der Instanzkonfiguration stellt sicher, dass auf dem SSM Agent die AMS Accelerate-Mindestversion ausgeführt wird.
3. CloudWatch Konfiguration
   a. Um sicherzustellen, dass die erforderlichen Metriken und Protokolle ausgegeben werden, passt AMS Accelerate die CloudWatch Konfiguration an. Weitere Informationen finden Sie im folgenden Abschnitt,CloudWatch Details zur Konfigurationsänderung.

Bei der automatisierten Instanzkonfiguration werden Änderungen oder Ergänzungen an Ihren IAM-Instanzprofilen und der CloudWatch Konfiguration vorgenommen.

Details zur Änderung von IAM-Berechtigungen

Jede verwaltete Instanz muss über eine AWS Identity and Access Management Rolle verfügen, die die folgenden verwalteten Richtlinien umfasst:

- arn:aws:iam: :aws:policy/Amazon SSMManaged InstanceCore
- arn:aws:iam: :aws:policy/ CloudWatchAgentServerPolicy
- arn:aws:iam: :aws:policy/ AMSInstance ProfileBasePolicy

Bei den ersten beiden handelt es sich um verwaltete Richtlinien. AWS Die vom AMS verwaltete Richtlinie lautet:

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Wenn Ihrer Instance bereits eine IAM-Rolle zugewiesen ist, aber eine dieser Richtlinien fehlt, fügt AMS die fehlenden Richtlinien zu Ihrer IAM-Rolle hinzu. Wenn Ihre Instance keine IAM-Rolle hat, fügt AMS die IAM-Rolle hinzu. AMSOSConfigurationCustomerInstanceProfile Die AMSOSConfigurationCustomerInstanceProfileIAM-Rolle enthält alle Richtlinien, die für AMS Accelerate erforderlich sind.

> **Note**
>
> Wenn das standardmäßige Instanzprofillimit von 10 erreicht ist, erhöht AMS das Limit auf 20, sodass die erforderlichen Instanzprofile angehängt werden können.

CloudWatch Details zur Konfigurationsänderung

Zusätzliche Details zur CloudWatch Konfiguration.

- CloudWatch Speicherort der Konfigurationsdatei auf der Instanz:
  - Windows:%ProgramData%\ Amazon\AmazonCloudWatchAgent\ amazon-cloudwatch-agent .json

  - Linux:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-accelerate-config.json
- CloudWatch Speicherort der Konfigurationsdatei in Amazon S3:
  - Windows: https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazon.aws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
  - Linux: https://- .s3. ams-configuration-artifacts *REGION_NAME* *REGION_NAME*.amazonaws. com/configurations/cloudwatch/latest/linux-cloudwatch-config.json
- Gesammelte Metriken:
  - Windows:
    - AWS Systems Manager SSM-Agent (CPU_Usage)
    - CloudWatch Agent (CPU_Usage)
    - Speicherauslastung für alle Festplatten (% freier Speicherplatz)
    - Arbeitsspeicher (% der belegten, zugesicherten Byte)
  - Linux:
    - AWS Systems Manager SSM-Agent (CPU_Usage)
    - CloudWatch Agent (CPU_Usage)
    - Zentralprozessor (cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system)
    - Festplatte (verwendet_Prozent, inodes_used, inodes_total)
    - Dis.io (io_time, write_bytes, read_bytes, schreibt, liest)
    - Mem (mem_used_percent)
    - Tauschen Sie (swap_used_percent)
- Gesammelte Protokolle:
  - Windows:
    - SSMAgentAmazon-Protokoll
    - AmazonCloudWatchAgentLog
    - SSMErrorAmazon-Protokoll
    - AmazonCloudFormationLog
    - ApplicationEventLog
    - EC2ConfigServiceEventLog
    - MicrosoftWindowsAppLockerEXEAndDLLEventLoggen
    - MicrosoftWindowsAppLockerMSIAndScriptEventLog

  - MicrosoftWindowsGroupPolicyOperationalEventLog
  - SecurityEventLog
  - SystemEventLog
- Linux:
  - /var/log/amazon/ssm/amazon-ssm-agent.log
  - /var/log/amazon/ssm/errors.log
  - /.log var/log/audit/audit
  - /-init-output.log var/log/cloud
  - /var/log/cloud-init.log
  - /var/log/cron
  - /var/log/dpkg.log
  - /var/log/maillog
  - /var/log/messages
  - /var/log/secure
  - /var/log/spooler
  - /var/log/syslog
  - /.log var/log/yum
  - /.log var/log/zypper

Offboard von AMS Accelerate

AMS Accelerate bietet eine einfache Möglichkeit, eine Betriebsumgebung der Enterprise-Klasse zu betreiben. Und AMS Accelerate bietet das unterstützende Infrastrukturbetriebsmodell für AWS Migration und Nutzung. Nach der Nutzung von AMS Accelerate können Sie sich jedoch dafür entscheiden, die Verantwortung für den Infrastrukturbetrieb intern zu übernehmen oder anderen Teams die Verantwortung für den AWS Infrastrukturbetrieb zuzuweisen. Dazu müssen Sie Ihre Konten vom AMS-Service trennen.

Wenn Sie ein Konto bei AMS Accelerate auslagern, überträgt AMS Ihnen alle in unserer Servicebeschreibung definierten Verantwortlichkeiten zurück. Sie werden beispielsweise nicht in der Lage sein, Vorfälle oder Serviceanfragen an AMS zu reduzieren. Ebenso werden unsere Betriebsingenieure und unsere Automatisierungsabteilung keinen Zugriff mehr auf Ihre Accelerate-Konten haben, sodass wir Fehler in Bezug auf Gesundheit, Verfügbarkeit, Sicherheit und Compliance

nicht mehr korrigieren können. Ihre AWS Workloads können weiterhin auf denselben Konten ausgeführt werden, die AMS betrieben hat.

Das Team, das in Zukunft Ihre Infrastrukturbetriebsdienste ausführen wird, muss einbezogen werden, um zu definieren, welche Personen, Tools und Prozesse Sie nach Ihrem Accelerate-Offboarding einsetzen werden. AMS lässt einige der AMS-Tools wie Leitplanken und Protokolle übrig, um die Entwicklung einer Betriebsumgebung und eines Modells zu ermöglichen, das „wie es sein soll“. Lesen Sie die folgende Dokumentation sorgfältig durch, um zu erfahren, welche Tools Sie weiterhin verwenden können und wie Sie die Offboardung eines Kontos beantragen können.

Die Offboarding-Effekte von AMS Accelerate

Beachten Sie bei der Vorbereitung der Ausgliederung von Accelerate die folgenden Überlegungen.

- Zugriff: Der `ams-access-management` CloudFormation Stack, der die `ams-access-management` AWS Identity and Access Management Rolle definiert, wird nicht gelöscht. Nach dem Offboarding bleiben diese Ressourcen erhalten, werden aber von anderen Komponenten, die zurückgelassen werden, nicht genutzt. Sie können den Stack und die Rolle nach Belieben löschen.
- Aufbewahrung von AMS-Ressourcen: Nach dem Offboarding verbleiben einige AMS-Ressourcen in Ihrem Konto. Welche Ressourcen beibehalten werden und was Sie damit machen können, finden Sie in der `resource_inventory.zip`Tabelle (komprimiert).
- Automatisierung: Nach dem Offboarding sind die von AMS kuratierten AWS SSM-Automatisierungsrunbooks und AWS Lambda Lambda-Funktionen nicht mehr verfügbar.
- Backup-Management: AMS verwendet Backup-Management, um Schnappschüsse Ihrer Ressourcen zu erstellen. Nach dem Offboarding können Sie mit AWS Backup Ausnahme der AMS-Backup-Pläne weiterhin die am definierten Backup-Zeitpläne, die Häufigkeit und die Aufbewahrungsfristen verwenden; siehe. Wählen Sie einen AMS-Backup-Plan Die von AMS Backup Orchestrator erstellten AWS Identity and Access Management Ressourcen werden entfernt, nicht jedoch die von AMS erstellten Backup-Tresore und der entsprechende Schlüssel. AWS KMS Accelerate überwacht die Backup-Jobs nicht mehr und führt bei Vorfällen keine Wiederherstellungsaktionen mehr durch.
- Kostenoptimierung: Nach dem Offboarding wird AMS Resource Scheduler gelöscht. AMS Resource Scheduler hilft Ihnen dabei, die Betriebskosten zu senken, indem die Ressourcen, die nicht genutzt werden, gestoppt und wieder gestartet werden, wenn ihre Kapazität benötigt wird. AMS gibt nicht weiter Empfehlungen zur Kostenoptimierung ab. Einzelheiten zu Resource Scheduler finden Sie unter Kostenoptimierung mit AMS Resource Scheduler.

- Ausgewiesene Experten: Nach dem Offboarding stehen Ihnen Ihr zugewiesener Cloud Service Delivery Manager (CSDM) und ein Cloud Architect (CA) nicht mehr beratend zur Seite, berichten nicht mehr darüber und fördern auch nicht die betriebliche und sicherheitstechnische Exzellenz für Ihre externen Accelerate-Konten.
- Incident Management: Incident Management ist der Prozess, mit dem der AMS-Service auf Ihre gemeldeten Vorfälle reagiert. Nach dem Offboarding erkennt Accelerate keine Vorfälle mehr und reagiert nicht mehr darauf und unterstützt Ihr Team auch nicht mehr bei der Lösung von Problemen. Sie können mit Accelerate keine Kommunikation zwischen Vorfällen und Serviceanfragen austauschen und der Zugriff auf die Accelerate-Konsole für Ihre Accelerate-Konten ist deaktiviert.
- Protokollierung und Berichterstattung: Nach dem Offboarding behalten Sie die Protokolle, die als Ergebnis von CloudWatch CloudTrail, und VPC Flow Logs gespeichert wurden. Sie können die Konfiguration dieser Dienste unverändert lassen, um weiterhin Protokolle zu generieren. AMS überwacht solche Konfigurationen jedoch nicht mehr. Accelerate stellt den monatlichen Servicebericht, der die wichtigsten Leistungskennzahlen von AMS zusammenfasst, nicht mehr zur Verfügung. Sie behalten die aus Self-Service Reporting (SSR) generierten Daten (siehe Self-Service-Berichte), Accelerate generiert jedoch keine neuen.
- Überwachung: Überwachung ist der Prozess, den der AMS-Service verwendet, um Ihre Ressourcen zu verfolgen. Beim Offboarding entfernt AMS AMS-spezifische Tools wie Alarm Manager und Resource Tagger sowie alle EventBridge Ereignisregeln und CloudWatch Alarme, die AMS im Rahmen der AMS-Monitoring-Baseline bereitgestellt hat. Accelerate reagiert nach dem Offboarding nicht mehr auf Alarme und konfiguriert auch keine neuen Alarme mehr. Einzelheiten zu Alarm Manager und Resource Tagger finden Sie unter Tag-basierter Alarm Manager und Resource Tagger.
- Betriebstools: AMS Accelerate kann den laufenden Betrieb der Infrastruktur Ihres Workloads in AWS sicherstellen. Nach dem Offboarding eines Accelerate-Kontos haben Sie keinen Zugriff mehr auf Tools wie Resource Tagger, mit denen Sie Ihre Ressourcen anhand von Regeln taggen können, oder auf automatisierte Instance-Konfiguration zur Installation der erforderlichen Agenten in Ihren EC2 Instances. CloudWatch und SSM-Agenten auf den Instanzen bleiben mit den vorhandenen Konfigurationen an Ort und Stelle. Das `AMSOSConfigurationCustomerInstanceRole` IAM-Profil und die `AMSInstanceProfileBasePolicy` werden von Ihren Instances getrennt und aus Ihren Accelerate-Konten entfernt.
- Patch-Management: Patch-Management ist der Prozess, den der AMS-Service verwendet, um Ihre EC2 Instances zu aktualisieren. Nach dem Offboarding erstellt AMS vor dem Patchen

keinen Snapshot der Instance mehr, installiert und überwacht die Patch-Installation nicht mehr und benachrichtigt Sie nicht mehr über das Ergebnis. Sie behalten die in der Vergangenheit erstellten Patch-Baselines und Snapshots bei. Darüber hinaus bleibt die Konfiguration Ihrer Patch-Wartungsfenster erhalten, aber die Patches werden nicht mehr von Accelerate installiert.

- Problemmanagement: Nach dem Offboarding führt Accelerate keine Analysen mehr durch, um Probleme zu identifizieren und zu untersuchen und die Ursache zu ermitteln.
- Sicherheit: Sicherheitsmanagement ist der Prozess, den der AMS-Service verwendet, um Ihre Ressourcen zu schützen. Nach dem Offboarding behalten Sie Ihren GuardDuty Amazon-Detektor und die Ergebnisse sowie alle AWS Config Regeln, die Sie erstellt haben. AWS Config Die von Accelerate bereitgestellten Regeln werden entfernt. Accelerate überwacht die Ergebnisse dieser Tools nicht mehr, behebt sie nicht mehr und erstellt keine Berichte mehr darüber.
- Kündigungsdatum des Dienstes: Das Kündigungsdatum des Dienstes ist der letzte Tag des Kalendermonats, der auf das Ende der 30-tägigen Kündigungsfrist folgt. Fällt das Ende der erforderlichen Kündigungsfrist nach dem 20. Tag des Kalendermonats, ist das Kündigungsdatum der letzte Tag des folgenden Kalendermonats. Im Folgenden finden Sie Beispielszenarien für Kündigungstermine.
  - Wenn die Kündigung am 12. April erfolgt, endet die Kündigungsfrist von 30 Tagen am 12. Mai. Das Kündigungsdatum des Dienstes ist der 31. Mai.
  - Wenn am 29. April eine Kündigungsfrist erteilt wird, endet die Kündigungsfrist von 30 Tagen am 29. Mai. Das Kündigungsdatum des Dienstes ist der 30. Juni.

Offboarding von AMS Accelerate mit Abhängigkeiten von Alarm Manager und Resource Tagger

Maßgeschneiderte CloudFormation Stacks, die Konfigurationen für Alarm Manager oder Resource Tagger bereitstellen, verbleiben zusammen mit den von AMS bereitgestellten Alarm Manager- und Resource Tagger-Konfigurationsstapeln in Ihrem Konto, wenn Sie AWS Managed Services verlassen.

Um die AMS-Konfigurationsstapel während des Offboarding-Prozesses zu löschen, müssen Sie alle Abhängigkeiten und Verweise auf Alarm Manager oder Resource Tagger aus den benutzerdefinierten Vorlagen entfernen, bevor Sie den Offboarding-Prozess einleiten. CloudFormation Durch das Entfernen der Verweise können Sie sicherstellen, dass die Stacks ordnungsgemäß aus Ihrem Konto entfernt werden, wenn Sie das AMS verlassen.

> **Important**
>
> Prüfen Sie Ihre CloudFormation Vorlagen sorgfältig und entfernen Sie alle Verweise auf Alarm Manager und Resource Tagger, bevor Sie mit dem Offboarding-Prozess beginnen. Wenn Sie dies nicht tun, können diese Stacks in Ihrem Konto verbleiben, auch wenn Sie Ihr Konto bei AMS verlassen. Beachten Sie, dass diese Stacks zwar spezifische Konfigurationsinformationen für Alarm Manager und Resource Tagger enthalten, dass für ihr Vorhandensein jedoch keine laufenden Kosten oder Gebühren anfallen.

Holen Sie sich Offboarding-Unterstützung für ein Accelerate-Konto

AMS sperrt Ihr Konto, nachdem Sie mindestens 30 Tage im Voraus eine Kündigungsanfrage für den AMS-Kontoservice erhalten haben. Das Kündigungsdatum des Dienstes ist der letzte Tag des Kalendermonats, der auf das Ende der vorgeschriebenen Kündigungsfrist von 30 Tagen folgt. Sofern das Ende der erforderlichen Kündigungsfrist nach dem 20. Tag des Kalendermonats liegt, gilt als Kündigungsdatum der letzte Tag des darauffolgenden Kalendermonats.

Um das Offboarding eines Accounts zu beantragen, müssen Sie:

1. Reichen Sie mithilfe einer Serviceanfrage einen formellen Antrag auf Offboarding für das Konto ein. Eine Serviceanfrage (SR), in der alle Konten dokumentiert werden, die Sie extern lassen möchten, oder eine Serviceanfrage pro Konto.

   Geben Sie in der Anfrage die Liste der Konten IDs an, für die ein Offboarding vorgesehen ist, den Grund für das Offboarding und alle weiteren Überlegungen.
2. Informieren Sie Ihren CSDM über die Konten, die Sie auslagern möchten, und bitten Sie ihn um Hilfe bei der Durchführung des Offboarding-Prozesses.

Benachrichtigungseinstellungen in Accelerate

Die Kommunikation zwischen Ihnen und AMS erfolgt aus vielen Gründen:

- Ereignisse, die durch die Überwachung von Warnmeldungen erzeugt wurden
- Benachrichtigungen über den Patch-Service, wenn Sie sich für das Patch-Add-On angemeldet haben
- Serviceanfragen und Vorfallberichte

- Gelegentlich wichtige AWS Ankündigungen (Ihr CSDM kontaktiert Sie, falls Maßnahmen Ihrerseits erforderlich sind)

Alle Benachrichtigungen werden über eine E-Mail gesendet, die Sie beim Onboarding für Patch-Benachrichtigungen angegeben haben. Andernfalls werden Benachrichtigungen an die Standard-E-Mail gesendet, die Sie AMS beim Onboarding zur Verfügung gestellt haben. Da es schwierig ist, einzelne E-Mails auf dem neuesten Stand zu halten, empfehlen wir Ihnen, eine Gruppen-E-Mail zu verwenden, die auf Ihrer Seite aktualisiert werden kann. Alle an Sie gesendeten Benachrichtigungen werden ebenfalls von AMS Operations empfangen und analysiert, bevor eine Antwort erfolgt.

Sie können benannte Kontaktlisten für Benachrichtigungen verwenden, die nicht auf Ressourcen basieren, z. B. Benachrichtigungen, die auf GuardDuty oder AWS Config basieren. Beispielsweise können Sie eine Liste mit einem Namen `SecurityContacts` und eine andere mit einem Namen haben. `OperationsContacts` AMS sendet Alarme und Benachrichtigungen an diese Listen.

Weitere Details finden Sie unter AWS Config Bericht zur Einhaltung der Kontrollvorschriften.

Taggen in AMS Accelerate

Die meisten Accelerate-Funktionen (Patching, Backup, Überwachung) verwenden Tags und Konfigurationsprofile, um zu entscheiden, welche Ihrer Ressourcen verwaltet werden sollen, welche Aktionen angewendet werden sollen und wann sie angewendet werden sollen. Tags sind Bezeichnungen, die Sie auf Ressourcen anwenden. Konfigurationsprofile enthalten Regeln, die auf diesen Tags basieren.

Jede Accelerate-Funktion hat ihre eigenen Tagging-Anforderungen. Bei einigen Funktionen müssen Sie bestimmte Tags verwenden, bei anderen können Sie eigene Tags verwenden.

Informationen zu den erforderlichen Tags finden Sie unterVon Kunden verwaltete Tags in Accelerate.

Informationen zu Stichwörtern, die als Kunden definiert werden können, finden Sie unter Vom Kunden bereitgestellte Tags in Accelerate

Inhalt

Schlagworte in AMS Accelerate

Inhalt

Was sind Tags?

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jeder Tag besteht aus einem Schlüssel und einem optionalen Wert, die sie beide festlegen können.

Sie verwenden Tags, um Ihre AWS Ressourcen auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Sie könnten beispielsweise eine Reihe von Tags für die EC2 Amazon-Instances Ihres Kontos definieren, mit deren Hilfe Sie den Besitzer und die Stack-Ebene jeder Instance verfolgen können.

Tags haben für Amazon keine semantische Bedeutung EC2 und werden ausschließlich als Zeichenfolge interpretiert.

Weitere Informationen finden Sie unter Ressourcen zum Taggen AWS.

So funktioniert Tagging

Es gibt mehrere Möglichkeiten, Tags auf Ihre Ressourcen anzuwenden. Sie können Ressourcen direkt in der Konsole jedes AWS Dienstes taggen, wenn Sie die Ressource erstellen, den AWS Tag-Editor verwenden, um Tags für mehrere Ressourcen hinzuzufügen, zu entfernen oder zu bearbeiten, oder Bereitstellungstools wie CloudFormation Resource Tag verwenden. AMS Accelerate bietet auch den AMS Accelerate Resource Tagger, mit dem Sie Regeln für einen automatisierten Tag-Lifecycle-Manager definieren können. Informationen zur Verwendung von Resource Tagger in AMS Accelerate finden Sie unter. Beschleunigen Sie Resource Tagger AMS Accelerate bietet auch vom Kunden bereitgestellte Tags zum Hinzufügen und Entfernen von benutzerdefinierten Tags zu Ihren AMS-Ressourcen. Weitere Informationen zu vom Kunden bereitgestellten Tags finden Sie unter. Vom Kunden bereitgestellte Tags in Accelerate

Von Kunden verwaltete Tags in Accelerate

Bestimmte Tags sind erforderlich, um verschiedene AMS Accelerate-Aktionen auszulösen.

Inhalt

Überwachung in Accelerate

AMS Accelerate überwacht die unterstützten Ressourcen auf Zustand, Verfügbarkeit und Zuverlässigkeit. Weitere Informationen zu diesem Serviceangebot finden Sie unterÜberwachung und Eventmanagement in AMS Accelerate.

AMS Accelerate wird zusätzlich AWS-Services zur Basisüberwachung regelmäßig integriert. Wenn Sie die Resource Tagger-Standardkonfiguration verwenden, werden diese Updates automatisch für Ihre Konten bereitgestellt, und die Änderungen werden auf die unterstützten Ressourcen übertragen.

Um sich dafür zu entscheiden, dass Ihre EC2 Amazon-Instances von AMS Accelerate verwaltet werden, müssen Sie das folgende Tag über das Anpassungsprofil in AppConfig anwenden. Weitere Informationen finden Sie unter Schritt 3: Konfiguration und Konfigurationsprofil erstellen.

Wenden Sie das folgende Tag auf Ihre Ressourcen an:

Key (Schlüssel)	Value (Wert)
ams:rt:ams-managed	true

Sie können beispielsweise ein benutzerdefiniertes Konfigurationsdokument wie dieses erstellen, um die Tags auf all Ihre AMS-unterstützten EC2 Ressourcen anzuwenden:

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Important**
>
> Denken Sie daran, Ihre Konfigurationsänderungen zu implementieren, nachdem Sie sie vorgenommen haben. In SSM AppConfig müssen Sie nach der Erstellung eine neue Version der Konfiguration bereitstellen.

Andere Dienste als Amazon EC2 verfügen standardmäßig über eine Basisüberwachung. Um zu verhindern, dass Ihre Ressourcen von AMS Accelerate überwacht werden, können Sie das Anpassungskonfigurationsprofil verwenden, um bestimmte Ressourcen auszuschließen oder AWS-Services. Auf diese Weise können Sie steuern, welche Ressourcen mit Monitoring-Tags versehen werden sollen, um grundlegende Alarmdefinitionen bereitzustellen. Siehe Resource Tagger-Anwendungsfälle in AMS Accelerate.

Verwenden von Resource Tagger

Die AMS Accelerate Resource Tagger-Konfiguration in Ihrem Konto trägt dazu bei, dass die folgenden Tags automatisch bereitgestellt werden, wenn Sie dieses eine Tag anwenden (ams:rt:ams-managed).

Sie werden sehen, dass die folgenden Tags auf Ihre unterstützten Ressourcen zur Basisüberwachung angewendet werden.

Key (Schlüssel)	Value (Wert)	Regel
ams:rt: ams-monitoring-policy	ams-überwacht	Gilt für alle von EC2 AMS unterstützten Ressourcen
ams:rt: ams-monitoring-policy-platform	ams-monitored-linux	Gilt für alle EC2 Amazon-Instances, auf denen Linux OS ausgeführt wird
ams:rt: ams-monitoring-policy-platform	ams-monitored-windows	Gilt für alle EC2 Amazon-Instances, auf denen Windows OS ausgeführt wird

Für andere unterstützte Dienste

Wenden Sie gemäß den angegebenen Regeln die folgenden Tags auf Ihre Ressourcen an:

Key (Schlüssel)	Value (Wert)	Regel
ams:rt: ams-monitoring-policy	ams-überwacht	Gilt für alle Ressourcen, die von AMS Accelerate Monitoring unterstützt werden.
ams:rt: ams-monitoring-with-kms	ams-monitored-with-kms	OpenSearch Domäne mit KMS
ams:rt: ams-monitoring-with-master	ams-monitored-with-master	OpenSearch Domäne mit dediziertem Master-Knoten

Wenn Sie Resource Tagger nicht verwenden

Hilfe Beschleunigen Sie Tags ohne Resource Tagger zum Anwenden der richtigen Monitoring-Tags mit anderen Methoden als mit AMS Resource Tagger finden Sie unter.

Konfiguration von Tags für EC2 Instanzen in Accelerate

AMS Accelerate verwaltet Agenten auf Ihren EC2 Amazon-Instances, wie den SSM-Agenten und den CloudWatch Agenten. Weitere Informationen zu diesem Serviceangebot finden Sie unter Automatisierte Instanzkonfiguration in AMS Accelerate

Um sich dafür zu entscheiden, dass Ihre EC2 Amazon-Instances von AMS Accelerate verwaltet werden, müssen Sie Ihren EC2 Amazon-Instances das folgende Tag zuweisen:

Key (Schlüssel)	Value (Wert)
ams:rt:ams-managed	true

Verwaltung von Tags für Backups in Accelerate

AMS Accelerate verwaltet die Sicherung der unterstützten Ressourcen. Weitere Informationen zu diesem Serviceangebot finden Sie unterKontinuitätsmanagement in AMS Accelerate.

AMS Accelerate Backup Management verwendet Tags, um zu identifizieren, welche Ressourcen automatisch gesichert werden sollten (und bietet auch manuelle Backup-Funktionen). Sie können

eine beliebige Kombination aus Schlüssel/Wert des Tags verwenden, um Ihre Ressourcen mit Backup-Plänen zu verknüpfen. Um sich für automatische Backups mithilfe des ams-default-backup-plan AWS Backup Plans zu entscheiden, müssen Sie Ihren unterstützten Ressourcen das folgende Tag zuordnen:

Key (Schlüssel)	Value (Wert)
ams:rt:backup-orchestrator	true

> **Note**
>
> Beim Onboarding kennzeichnet AMS Accelerate alle Ressourcen mit ams:rt: mit dem Wert true für backup-orchestrator-onboarding Snapshots mit kurzen Intervallen und kurzen Aufbewahrungsfristen. Dies wird durch den Backup-Plan verwaltet. ams-onboarding-backup-plan Weitere Informationen zu den von AMS Accelerate verwalteten AWS Backup Plänen finden Sie unter. Wählen Sie einen AMS-Backup-Plan

Beschleunigen Sie die Verwaltung von Tags

Während der Einführung in AMS Accelerate werden Ihrem Konto mehrere AWS Ressourcen zugewiesen. Damit Sie sie identifizieren können, sind diese Ressourcen mit den folgenden Tags versehen:

Key (Schlüssel)	Value (Wert)
AMS: ResourceOwner	AMS
ams: resourceOwnerService	Eine Beschreibung, von welchem AMS Accelerate-Dienst, der diese Ressource anbietet, stammt beispielsweise aus AMS Deployment, Backup, Controls, Monitoring, Patch usw.
AppId	AMSInfrastructure
AppName	

Key (Schlüssel)	Value (Wert)
Umgebung	

> **Note**
>
> Diese Tags werden mithilfe von Tags auf CloudFormation Stack-Ebene angewendet und basieren auf der Weitergabe der Tags CloudFormation an die erstellten Ressourcen. Weitere Informationen finden Sie unter Ressourcen-Tag.

Vom Kunden bereitgestellte Tags in Accelerate

Was sind vom Kunden bereitgestellte Tags?

Vom Kunden bereitgestellte Tags sind eine AMS Accelerate-Servicefunktion, mit der Regeln festgelegt werden, wie AMS-Ressourcen in Ihrem Konto markiert werden. Mit vom Kunden bereitgestellten Tags können Sie benutzerdefinierte Tags zu AMS-Ressourcen hinzufügen, die für Ihre Konten bereitgestellt werden. Die Funktion für vom Kunden bereitgestellte Tags wird den angeforderten Konten automatisch hinzugefügt, wenn Sie über einen automatisierten Dienst eine Anfrage an Ihren Cloud Service Delivery Manager (CSDM) stellen. Beachten Sie, dass Sie AMS-Tags nicht überschreiben können. AMS-Tags beginnen mit 'ams: '.

Sie können Ihre eigenen Tags (Labels) definieren und die Funktionen dieser Tags für all Ihre AMS Accelerate-Ressourcen spezifizieren. Sie können diese Tags bereitstellen, bevor Sie bei AMS einsteigen, sodass AMS-Tags und Ihre benutzerdefinierten Tags während des Onboarding-Prozesses angewendet werden. Oder Sie können Tags nach dem Onboarding bereitstellen.

Wie kann ich vom Kunden bereitgestellte Tags hinzufügen?

Wenn Sie das Hinzufügen dieser Tags zu Ihren Ressourcen beantragen möchten, wenden Sie sich an Ihren CSDM. Diese Tags werden auf AMS-Ressourcen in Ihrem Konto angewendet.

Was ist der Geltungsbereich der Tags?

Diese Funktion ist derzeit nur für Accelerate-Kunden und in AWS kommerziellen Regionen verfügbar. Sie können allen Konten, die Sie besitzen, oder einer bestimmten Kontenliste Stichwörter hinzufügen.

> **Note**
>
> Diese Tags gelten nur für AMS-Ressourcen und wirken sich nicht auf Ihre eigenen Ressourcen aus.

Tag-Management-Tools für Accelerate

Inhalt

Beschleunigen Sie Resource Tagger

Mit Resource Tagger können Sie Regeln festlegen, die festlegen, wie AWS Ressourcen in Ihrem Konto markiert werden. Beim Onboarding eines Kontos wendet AMS Accelerate Ihre Tagging-Richtlinie an, um sicherzustellen, dass Ressourcen in Ihren verwalteten Konten markiert werden.

Inhalt

- Konfigurationsänderungen werden bereitgestellt
- Terraform so konfigurieren, dass Resource Tagger-Tags ignoriert werden
- Die Anzahl der von Resource Tagger verwalteten Ressourcen anzeigen

Was ist Resource Tagger?

Resource Tagger ist ein AMS Accelerate-Dienst, mit dem Sie Regeln festlegen können, mit denen festgelegt wird, wie AWS Ressourcen in Ihrem Konto markiert werden. Ziel ist es, Ihnen einen vollständigen Überblick darüber zu geben, wie Ihre Tags auf Ihre AWS Ressourcen angewendet werden.

Resource Tagger erstellt, aktualisiert und löscht automatisch Tags auf unterstützten AWS Ressourcen, basierend auf den Tagging-Regeln, die Sie in Ihren Konfigurationsprofilen angeben. Sie können beispielsweise eine Regel angeben, die ein Tag auf eine Sammlung von EC2 Amazon-Instances anwendet und angibt, dass diese von AMS Accelerate verwaltet werden sollen, was dazu führt, dass die Instances überwacht oder gesichert werden. Sie können Tags wie diese verwenden, um den Compliance-Status für die AWS Ressourcen auf der Grundlage der in Ihren AWS AppConfig Konfigurationsprofilen definierten Richtlinie zu ermitteln. Weitere Informationen finden Sie unter AWS AppConfig.

AMS Accelerate bietet eine Standardkonfiguration für verwaltetes Tagging, sodass Sie Ihre Ressourcen von AMS Accelerate überwachen lassen können. Sie definieren, welche Ressourcen von AMS Accelerate verwaltet werden sollen, und die verwalteten Tagging-Regeln stellen sicher, dass die Ressourcen mit den entsprechenden Tags von AMS Accelerate überwacht werden.

Mit Resource Tagger können Sie auf Wunsch die standardmäßigen verwalteten AMS Accelerate-Tags überschreiben oder deaktivieren, Ihre eigenen Tagging-Regeln zur Einhaltung Ihrer Richtlinien festlegen und andere Mechanismen wie Terraform verwenden, um Abweichungen zu vermeiden. Sie können die Ausnahmen für die Skalierung auf der Grundlage Ihrer Betriebsabläufe definieren. Sie könnten beispielsweise eine Richtlinie definieren, um Tags für alle EC2 Amazon-Instances mit unterstützten Plattformen (wie Windows und Linux) anzuwenden und bestimmte Instances IDs vom Tagging auszuschließen.

> **Important**
>
> Resource Tagger kontrolliert alle Tags in Ihrem Konto, die das Präfix ams:rt: haben. Alle Tags, die mit diesem Präfix beginnen, werden gelöscht, sofern sie nicht in den

Konfigurationsregeln von Resource Tagger enthalten sind. Zusammenfassend lässt sich sagen, dass jedes Tag auf unterstützten Ressourcen, das mit ams:rt: beginnt, als Eigentum von Resource Tagger betrachtet wird. Wenn Sie etwas manuell mit z. B. ams:rt: taggen, würde dieses Tag automatisch entfernt, wenn es nicht in einem der Resource Tagger-Konfigurationsprofile angegeben wäre.

Wie funktioniert Resource Tagger

Wenn Ihr Konto in AMS Accelerate integriert ist, werden zwei JSON-Konfigurationsdokumente für Ihr Konto in bereitgestellt. AWS AppConfig Bei den beiden Dokumenten, den sogenannten Konfigurationsprofilen, handelt es sich um AMSManagedTags, die als Standardkonfigurationsprofil und CustomerManagedTagsals Anpassungskonfigurationsprofil bezeichnet werden. Sie verwenden das Anpassungskonfigurationsprofil, um Ihre eigenen Richtlinien und Regeln für Ihre Konten zu definieren, und diese werden nicht von AMS Accelerate überschrieben.

Beide Profile befinden sich in der AMSResourceTagger-Anwendung und in der Umgebung. AMSInfrastructure Alle vom Resource Tagger angewendeten Tags haben das key prefix ams:rt:.

Konfigurationsprofil zur Anpassung:

Das Anpassungskonfigurationsprofil ist zum Zeitpunkt der Kontoeröffnung zunächst leer. Alle im Profildokument enthaltenen Regeln werden jedoch zusätzlich zu den Regeln im Standardkonfigurationsprofil durchgesetzt. Jede Konfiguration im Anpassungskonfigurationsprofil wird vollständig von Ihnen verwaltet und nicht von AMS Accelerate überschrieben, außer auf Ihre Anfrage.

Sie können im benutzerdefinierten Konfigurationsprofil für die unterstützten AWS Ressourcen beliebige benutzerdefinierte Tagging-Regeln angeben. Außerdem können Sie hier Änderungen an der von AMS Accelerate verwalteten Standardkonfiguration angeben, siehe. Resource Tagger-Anwendungsfälle in AMS Accelerate

Important

Wenn Sie dieses Profil aktualisieren, erzwingt der Resource Tagger die Änderungen automatisch für alle relevanten Ressourcen in Ihrem. AWS-Konto Die Änderungen werden automatisch in Kraft gesetzt, es kann jedoch bis zu 60 Minuten dauern, bis sie wirksam werden.

Sie können dieses Profil mithilfe der oder mithilfe der AWS-Managementkonsole AWS CLI/SDK-Tools aktualisieren. Informationen zum Aktualisieren eines Anpassungskonfigurationsprofils finden Sie im AWS AppConfig Benutzerhandbuch: Was ist? AWS AppConfig

Standardkonfigurationsprofil:

Das Standardkonfigurationsprofildokument ist intern von AMS Accelerate und enthält von AMS Accelerate bereitgestellte Standardregeln, die Sie nicht dauerhaft ändern oder löschen können. Dieses Profil kann jederzeit von AMS Accelerate aktualisiert und Ihnen zur Überprüfung zur Verfügung gestellt werden. Alle Änderungen, die Sie daran vorgenommen haben, werden automatisch gelöscht. Wenn Sie eine der Standardkonfigurationsregeln ändern oder deaktivieren möchten, die Sie mithilfe des Anpassungskonfigurationsprofils verwenden, sieheResource Tagger-Anwendungsfälle in AMS Accelerate.

Resource Tagger-Konfigurationsprofile in AMS Accelerate

Mithilfe von Konfigurationsprofilen wird sichergestellt, dass Tags während der gesamten Lebensdauer der Ressourcen einheitlich auf Ressourcen angewendet werden.

Syntax und Struktur

Ein Konfigurationsprofil ist ein JSON-Objekt mit der folgenden Struktur:

```
{
   "Options": {
      "ReadOnly": false
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

Optionen: (optional) Geben Sie Optionen an, wie sich der verhalten ResourceTagger soll. Das Weglassen des Blocks entspricht dem Setzen aller Optionen auf ihre Standardwerte. Nachfolgend finden Sie die verfügbaren Optionseinstellungen:

- ReadOnly: (optional, standardmäßig falsch): Gibt den ReadOnly Modus für Resource Tagger an. Auf true setzen ReadOnly , um zu deaktivieren, dass Resource Tagger Tags auf AWS-Ressourcen erstellt oder entfernt. Weitere Informationen finden Sie unter Verhindern, dass Resource Tagger Ressourcen verändert.

ResourceType: Dieser Schlüssel muss eine der folgenden unterstützten Zeichenfolgen sein und steht für die gesamte Konfiguration, die sich auf den angegebenen Ressourcentyp bezieht:

- AWS::AutoScaling::AutoScalingGruppe
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS:EC2:: VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain
- AWS: :RDS: DBCluster
- AWS: :RDS: DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ConfigurationID: Dieser Schlüssel muss im Profildokument eindeutig sein und benennt den folgenden Konfigurationsblock eindeutig. Wenn zwei Konfigurationsblöcke im selben ResourceTypeBlock dieselbe ConfigurationID haben, wird der Block wirksam, der zuletzt im Profil erscheint. Wenn

Sie in Ihrem Anpassungsprofil eine ConfigurationID angeben, die mit der im Standarddokument angegebenen identisch ist, wird der im Anpassungsprofil definierte Konfigurationsblock wirksam.

> ⚠ Important
>
> Die ConfigurationID sollte ***not***sich mit dem AMS Accelerate-Profil überschneiden. Beispielsweise sollte es sich nicht um AMSMonitoringLinux oder AMSMonitoringWindows handeln, da andernfalls die entsprechende Konfiguration des Tags-Konfigurationsprofils deaktiviert wird. AMSManaged

Aktiviert (optional, standardmäßig auf true gesetzt): Gibt an, ob der Konfigurationsblock wirksam wird. Setzen Sie diesen Wert auf false, um einen Konfigurationsblock zu deaktivieren. Ein deaktivierter Konfigurationsblock hat keine Auswirkung.

Filter: Gibt die Ressourcen an, für die die Konfiguration gilt. Jedes Filterobjekt kann eines (aber nur eines) der folgenden Felder haben:

- AWS::AutoScaling::AutoScalingGruppe:
  - AutoScalingGroupName: Der Name der Autoscaling-Gruppe. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::DynamoDB::Table:
  - TableName: Der Name der DynamoDB-Tabelle. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::EC2::Instance:
  - AvailabilityZone: Der Filter entspricht einer EC2 Instanz in der angegebenen Availability Zone. Dieses Feld unterstützt den Platzhalterabgleich, sodass *a mit us-east-1a, ap-northeast-1a usw. übereinstimmt.
  - InstanceId: Der Filter entspricht einer Instanz mit der angegebenen Instanz-ID. EC2 Dieses Feld unterstützt den Platzhalterabgleich, sodass i-00000* mit jeder Instanz übereinstimmen würde, deren Instanz-ID mit i-00000 beginnt.
  - Plattform: Der Filter ordnet eine EC2 Instanz der angegebenen Plattform zu. Gültige Werte sind Windows, Linux oder der Platzhalter * (für jede Plattform).
- AWS::EC2::NatGateway:
  - NatGatewayId: Die ID des NAT-Gateways. Dieses Feld unterstützt den Platzhalterabgleich.
  - Status: Der Status des NAT-Gateways (ausstehend | ausgefallen | verfügbar | löschend | gelöscht oder Platzhalter „*“)

  - VpcId: Die ID der VPC, in der sich das NAT-Gateway befindet. Dieses Feld unterstützt den Platzhalterabgleich.
  - SubnetId: Die ID des Subnetzes, in dem sich das NAT-Gateway befindet. Dieses Feld unterstützt den Platzhalterabgleich
- AWS:EC2: VPNConnection:
  - VpnConnectionId: Die ID der Verbindung. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::EFS::FileSystem:
  - FileSystemId: Die ID des EFS-Dateisystems. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::EKS::Cluster:
  - ClusterName: Der Name des Clusters. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer):
  - LoadBalancerName: Der LoadBalancer Name. Dieses Feld unterstützt den Platzhalterabgleich.
  - Schema: Kann entweder „mit dem Internet verbunden“, „intern“ oder mit dem Platzhalter „*“ angegeben werden.
  - VPCId: Der Platzhalter, VPCId in dem der Loadbalancer bereitgestellt wird, kann der Platzhalter „*“ sein.
- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer (ALB)):
  - LoadBalancerArn: Der LoadBalancer Amazon-Ressourcenname (ARN).
  - DNSName: Der DNSName der LoadBalancer. Dieses Feld unterstützt den Platzhalterabgleich.
  - LoadBalancerName: Der LoadBalancer Name. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::Elasticsearch::Domain:
  - DomainId: Die DomainId der ElasticSearch Ressource. Dieses Feld unterstützt den Platzhalterabgleich.
  - DomainName: Die DomainName der ElasticSearch Ressource. Dieses Feld unterstützt den Platzhalterabgleich.
  - HasMasterNode: Boolescher Wert von wahr oder falsch. Stimmt überein, wenn die Domain über einen eigenen Master-Knoten verfügt.
  - HasKmsKeyBoolescher Wert von wahr oder falsch. Entspricht, wenn die Domäne über einen KMS-Schlüssel für die Verschlüsselung im Ruhezustand verfügt.
- AWS::FSx::FileSystem:
  - FileSystemId: Die ID des FSx Dateisystems. Dieses Feld unterstützt den Abgleich mit Platzhaltern.

- AWS::OpenSearch::Domain:
  - DomainId: Die DomainId der OpenSearch Ressource. Dieses Feld unterstützt den Platzhalterabgleich.
  - DomainName: Die DomainName der OpenSearch Ressource. Dieses Feld unterstützt den Platzhalterabgleich.
  - HasMasterNode: Boolean; Wenn die Domain über einen eigenen Master-Knoten verfügt, kann dieser auf true gesetzt werden.
  - HasKmsKey: Wenn die Domain über einen KMS-Schlüssel für die Verschlüsselung im Ruhezustand verfügt, kann dieser auf true gesetzt werden.
- AWS: :RDS:: DBCluster
  - DBClusterBezeichner: Der Filter ordnet eine RDS-Cluster-ID der angegebenen Kennung zu. Dieses Feld unterstützt keinen Platzhalterabgleich, daher muss eine Cluster-ID angegeben werden.
  - Engine: Die Engine, die von der RDS-Instance verwendet wird. Dieses Feld unterstützt den Platzhalterabgleich.
  - EngineVersion: Die Engine-Version. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS: :RDS:: DBInstance
  - DBInstanceIdentifier: Der Filter gleicht eine RDS-Instance mit der angegebenen Instance-ID ab. Dieses Feld unterstützt keinen Platzhalterabgleich, daher muss eine Instanz-ID angegeben werden.
  - Engine: Die Engine, die von der RDS-Instance verwendet wird. Dieses Feld unterstützt den Platzhalterabgleich.
  - EngineVersion: Die Engine-Version. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::Redshift::Cluster:
  - ClusterIdentifier: Die Cluster-ID. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::S3::Bucket:
  - BucketName: Der Name des S3-Buckets. Dieses Feld unterstützt den Platzhalterabgleich.
- AWS::Synthetics::Canary:
  - CanaryName: Der Name des Synthetics Canary.

Weitere Filtereigenschaften:

- Tag: Der Filter gilt für jede Ressource, auf die das angegebene Tag bereits angewendet wurde. Der Wert für diese Eigenschaft muss ein JSON-Objekt mit den folgenden Feldern sein:
  - Schlüssel: Muss eine exakte Zeichenfolge sein und gibt an, dass die Ressourcen ein Tag mit genau diesem Schlüssel haben müssen.
  - Wert: Gibt den passenden Wert für das Tag an. Unterstützt Platzhalter, sodass der Wert Sample jedem Wert entspricht, der mit der Zeichenfolge Sample endet.
- Fn: :AND: Ein JSON-Array von JSON-Objekten. Jedes Objekt folgt denselben Regeln wie der Filter-Konfigurationsblock. Dies gibt an, dass der Filter mit jeder Ressource übereinstimmt, die allen Unterfiltern entspricht.
- Fn: :OR: Ein JSON-Array von JSON-Objekten. Jedes Objekt folgt denselben Regeln wie der Filter-Konfigurationsblock. Dies gibt an, dass der Filter mit jeder Ressource übereinstimmt, die einem der Unterfilter entspricht.
- Fn: :NOT: Ein JSON-Objekt, das denselben Regeln folgt wie der Filter-Konfigurationsblock. Dies gibt an, dass der Filter explizit keiner Ressource entspricht, die dem Unterfilter entspricht. Verwenden Sie dies, um Ausnahmen für Ihre Tagging-Regeln anzugeben.

Tags: Die Tags, die auf die entsprechenden Ressourcen angewendet werden sollen. (Siehe Konventionen zur Benennung und Verwendung von Tags.) Dieses Feld ist ein Array von Schlüssel-Wert-Paaren:

- Schlüssel: Der Schlüssel des Tags, das angewendet werden soll.
- Wert: Der Wert des Tags, das angewendet werden soll.

> **Note**
>
> Von Resource Tagger angewendete Tags haben immer Schlüssel, die mit ams:rt: beginnen. Wenn Sie dieses Präfix nicht in Ihrem Profil angeben, fügt Resource Tagger es für Sie ein. Auf diese Weise unterscheidet Resource Tagger die Tags, die es besitzt und verwaltet, von Tags, die von anderen Tools für andere Zwecke verwendet werden.

Resource Tagger-Anwendungsfälle in AMS Accelerate

In diesem Abschnitt werden häufig mit Resource Tagger ausgeführte Aktionen aufgeführt.

Anzeige der von Resource Tagger angewendeten Tags

Alle von Resource Tagger angewendeten Tags haben das key prefix ams:rt:. Die folgende Tag-Definition führt beispielsweise zu einem Tag mit dem Schlüssel ams:rt:SampleKey und dem Wert SampleValue. Alle Tags mit diesem Präfix werden als Teil von Resource Tagger behandelt.

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> Wenn Sie manuell ein eigenes Tag mit dem Präfix ams:rt: erstellen, gilt es als von Resource Tagger verwaltet. Das heißt, wenn die Ressource von Resource Tagger verwaltet wird, die Konfigurationsprofile aber nicht angeben, dass das Tag angewendet werden sollte, dann entfernt Resource Tagger Ihr manuell hinzugefügtes Tag. Wenn Sie Ressourcen, die von Resource Tagger verwaltet werden, manuell taggen, verwenden Sie nicht das ams:rt: -Präfix für Tag-Schlüssel.

Verwenden Sie Resource Tagger, um Tags zu erstellen

Der AMS Accelerate Resource Tagger ist eine Komponente, die während des AMS Accelerate-Onboardings in Ihrem Konto bereitgestellt wird. Resource Tagger verfügt über ein konfigurierbares Regelwerk, das definiert, wie Ihre Ressourcen gekennzeichnet werden sollen. Anschließend setzt es diese Regeln durch und fügt automatisch Tags zu Ressourcen hinzu und entfernt sie, um sicherzustellen, dass sie Ihren Regeln entsprechen.

Wenn Sie den Resource Tagger verwenden möchten, um Ihre Ressourcen zu taggen, finden Sie weitere Informationen unter. Beschleunigen Sie Resource Tagger

Im Folgenden finden Sie ein Beispiel für einen Resource Tagger-Konfigurationsausschnitt, der allen Amazon-Instances das Tag ams:rt:ams-managed mit dem Wert true hinzufügt. EC2 Mit dem ams:rt:ams-managed Tag stimmen Sie der Überwachung Ihrer Ressourcen durch AMS Accelerate zu.

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
```

```
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Seien Sie vorsichtig, wenn Sie den Namen für Ihre neue Konfiguration angeben (`SampleConfigurationBlock`im bereitgestellten Beispiel), da Sie versehentlich die AMS-verwaltete Konfiguration mit demselben Namen überschreiben könnten.

Verhindern, dass Resource Tagger Ressourcen verändert

Resource Tagger kann in einen schreibgeschützten Modus versetzt werden, der verhindert, dass Tags zu Ihren Ressourcen hinzugefügt oder entfernt werden. Dies ist nützlich, wenn Sie Ihren eigenen Tagging-Mechanismus bereitstellen möchten.

Im schreibgeschützten Modus untersucht Resource Tagger weiterhin die Tagging-Regeln, die in den Konfigurationsprofilen für Verwaltung und Kunden angegeben sind, und sucht nach Ressourcen, die diese Tagging-Regeln nicht erfüllen. Alle Ressourcen, die den Anforderungen nicht entsprechen, werden angezeigt. AWS Config Die AWS-Config-Regeln , nach denen Sie suchen können, haben das `AMSResourceTagger-` Präfix. Die `AMSResourceTagger-EC2Instance` AWS Config Regel bewertet beispielsweise, ob auf der Grundlage des Konfigurationsprofils geeignete Tags für `AWS::EC2::Instance` Ressourcen erstellt wurden.

Resource Tagger stoppt an diesem Punkt und nimmt keine Änderungen an Ihren Ressourcen vor (fügt keine Tags hinzu oder entfernt sie).

Sie können den Nur-Lese-Modus aktivieren, indem Sie das Kundenkonfigurationsprofil so ändern, dass der ReadOnlySchlüssel in den Optionsblock aufgenommen wird. Der folgende Ausschnitt aus dem Konfigurationsprofil zeigt beispielsweise, wie das aussehen könnte:

```
{
    "Options": {
        "ReadOnly": true
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger würde auf diese neue Konfiguration reagieren, sobald die Bereitstellung abgeschlossen ist, und das Hinzufügen und Entfernen von Tags zu Ressourcen beenden.

> **Note**
>
> Um die Tag-Änderung wieder zu aktivieren, ändern Sie den ReadOnlyWert auf False oder entfernen Sie den Schlüssel ganz, da der Standardwert False ist.

Weitere Informationen zur Einstellung „Optionen“ finden Sie im nächsten Syntax und Struktur Abschnitt.

Beispiel für ein Konfigurationsprofil

Das folgende Beispiel-Profildokument gibt an, dass alle EC2 Windows-Instanzen, die Teil eines CloudFormation Stack-*-Stacks sind, von AMS Accelerate verwaltet werden. Eine bestimmte EC2 Instanz mit der ID i-00000000000000001 wird jedoch explizit ausgeschlossen.

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
```

```
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
            "Tags": [
                {
                "Key": "ams:rt:ams-managed",
                "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Seien Sie vorsichtig, wenn Sie den Namen für Ihre neue Konfiguration angeben (`SampleConfigurationBlock`im bereitgestellten Beispiel), da Sie versehentlich die von AMS verwaltete Konfiguration mit demselben Namen überschreiben könnten.

Zusammenführen der Standardkonfiguration

Das Standardkonfigurationsprofil wird von AMS Accelerate zum Zeitpunkt der Kontoeröffnung bereitgestellt. Dieses Profil enthält Standardregeln, die in Ihrem Konto bereitgestellt werden.

Sie können das Standardkonfigurationsprofil zwar nicht ändern, aber Sie können die Standardeinstellungen überschreiben, indem Sie in Ihrem Anpassungskonfigurationsprofil einen Konfigurationsblock mit derselben ConfigurationID wie der Standardkonfigurationsblock angeben. Wenn Sie dies tun, überschreibt Ihr Konfigurationsblock den Standardkonfigurationsblock.

Betrachten Sie zum Beispiel das folgende Standardkonfigurationsdokument:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
```

```
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Um den hier angewendeten Tagwert von `SampleValueA` bis zu zu `SampleValueB` ändern und das Tag auf alle Instanzen, nicht nur auf Windows-Instanzen, anzuwenden, würden Sie das folgende Anpassungskonfigurationsprofil angeben:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> Denken Sie daran, Ihre Konfigurationsänderungen zu implementieren, nachdem Sie sie vorgenommen haben. Weitere Informationen finden Sie unter Konfigurationsänderungen werden bereitgestellt. In SSM AppConfig müssen Sie nach der Erstellung eine neue Version der Konfiguration bereitstellen.

Deaktivierung der Standardkonfiguration

Sie können eine Standardkonfigurationsregel deaktivieren, indem Sie Ihrem Anpassungskonfigurationsprofil einen Konfigurationsblock mit derselben ConfigurationID hinzufügen und dem Feld Enabled den Wert false zuweisen.

Zum Beispiel, wenn die folgende Konfiguration im Standardkonfigurationsprofil vorhanden wäre:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Sie könnten diese Tagging-Regel deaktivieren, indem Sie Folgendes in Ihr Anpassungskonfigurationsprofil aufnehmen:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> Denken Sie daran, Ihre Konfigurationsänderungen zu implementieren, nachdem Sie sie vorgenommen haben. Weitere Informationen finden Sie unterKonfigurationsänderungen werden bereitgestellt. In SSM AppConfig müssen Sie nach der Erstellung eine neue Version der Konfiguration bereitstellen.

Entfernen von Tags, die von Resource Tagger angewendet wurden

Alle Tags mit dem Präfix ams:rt werden von Resource Tagger entfernt, wenn die Tags nicht in den Konfigurationsprofilen vorhanden sind oder, falls sie existieren, wenn der Filter nicht übereinstimmt. Das bedeutet, dass Sie von Resource Tagger angewendete Tags entfernen können, indem Sie einen der folgenden Schritte ausführen:

- Ändern Sie den Abschnitt mit der Anpassungskonfiguration, der das Tag definiert.
- Es wurde eine Ausnahme für die spezifischen Ressourcen hinzugefügt, sodass sie nicht mehr dem Filter entsprechen.

Zum Beispiel: Wenn eine Linux-Instanz die folgenden Tags hat:

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
}]
```

Und Sie stellen das folgende Resource Tagger-Konfigurationsprofil bereit:

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
    }
}
```

Resource Tagger reagiert auf die neuen Konfigurationsänderungen, und das einzige Tag auf der Instanz lautet:

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

> **Warning**
>
> Seien Sie vorsichtig, wenn Sie den Namen für Ihre neue Konfiguration angeben (`SampleConfigurationBlock`im bereitgestellten Beispiel), da Sie versehentlich die von AMS verwaltete Konfiguration mit demselben Namen überschreiben könnten.

> **Important**
>
> Denken Sie daran, Ihre Konfigurationsänderungen zu implementieren, nachdem Sie sie vorgenommen haben. Weitere Informationen finden Sie unter. Konfigurationsänderungen werden bereitgestellt In SSM AppConfig müssen Sie nach der Erstellung eine neue Version der Konfiguration bereitstellen.

Die Resource Tagger-Konfiguration anzeigen oder Änderungen daran vornehmen

Die beiden JSON-Konfigurationsprofile, AMSManagedTags und CustomerManagedTags, die AppConfig beim Onboarding für Ihr Konto in AWS bereitgestellt werden und sich in der AMSResource Tagger-Anwendung und in der AMSInfrastructureUmgebung befinden, können über AppConfig die API überprüft werden. GetConfiguration

Im Folgenden finden Sie ein Beispiel für diesen Aufruf: GetConfiguration

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

Anwendung: AppConfig logische Einheit zur Bereitstellung von Funktionen, für den Resource Tagger ist dies AMSResource Tagger.

- Umgebung:. AMSInfrastructure
- Konfiguration: Um die Standard-Tag-Definitionen von AMS Accelerate anzuzeigen, lautet der Wert AMSManaged Tags. Für die Anzeige von Kunden-Tag-Definitionen lautet der Wert CustomerManagedTags.
- Client-ID: Die eindeutige Kennung der Anwendungsinstanz, dies kann eine beliebige Zeichenfolge sein.
- Die Tag-Definitionen können dann in der angegebenen Ausgabedatei angezeigt werden, in diesem Fall outfile.json.

Die Alarmdefinitionen können dann in der angegebenen Ausgabedatei angezeigt werden, in diesem Fall outfile.json.

Sie können anhand der vergangenen Bereitstellungen in der Umgebung sehen, welche Version der Konfiguration für Ihr Konto bereitgestellt wurde. AMSInfrastructure

So überschreiben Sie Tag-Regeln:

Jede der vorhandenen Tag-Regeln kann außer Kraft gesetzt werden, indem das Anpassungsprofil entweder mit CloudFormation by Bereitstellen eines Konfigurationsprofils mit CloudFormation for Accelerate oder oder oder direkt über die API AppConfig von CreateHostedConfigurationVersionusing aktualisiert wird. Die Verwendung derselben ConfigurationID als Standardregel für Konfigurations-Tags überschreibt die Standardregel und wendet stattdessen die benutzerdefinierte Regel an.

So stellen Sie die am Dokument vorgenommenen Änderungen bereit: CustomerManagedTags

Nachdem Sie Änderungen am Anpassungskonfigurationsprofil vorgenommen haben, müssen Sie die Änderungen für sie bereitstellen. Um die neuen Änderungen bereitzustellen, AppConfig muss die StartDeploymentAPI über die AWS AppConfig Konsole oder die CLI ausgeführt werden.

Konfigurationsänderungen werden bereitgestellt

Sobald die Anpassung abgeschlossen ist, müssen diese Änderungen über die AWS AppConfig StartDeploymentAPI bereitgestellt werden. Die folgenden Anweisungen zeigen, wie die Bereitstellung mit dem erfolgt AWS CLI. Darüber hinaus können Sie die verwenden AWS-Managementkonsole , um diese Änderungen vorzunehmen. Weitere Informationen finden Sie unter Schritt 5: Bereitstellen einer Konfiguration.

```
aws appconfig start-deployment
```

```
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- Anwendungs-ID: Die Anwendungs-ID des AMSResource Anwendungs-Taggers. Holen Sie sich das mit dem ListApplicationsAPI-Aufruf.
- Umgebungs-ID: Die Umgebungs-ID; diese erhalten Sie mit dem ListEnvironmentsAPI-Aufruf.
- Bereitstellungsstrategie-ID: Die ID der Bereitstellungsstrategie; diese erhalten Sie mit dem ListDeploymentStrategiesAPI-Aufruf.
- Konfigurationsprofil-ID: Die Konfigurationsprofil-ID von CustomerManagedTags; diese erhalten Sie mit dem ListConfigurationProfilesAPI-Aufruf.
- Konfigurationsversion: Die Version des Konfigurationsprofils, das Sie bereitstellen möchten.

> **Important**
>
> Resource Tagger wendet die in den Konfigurationsprofilen angegebenen Tags an. Alle manuellen Änderungen, die Sie (mit dem AWS-Managementkonsole, oder CloudWatch CLI/SDK) an den Resource Tags vornehmen, werden automatisch rückgängig gemacht. Stellen Sie also sicher, dass Ihre Änderungen über Resource Tagger definiert sind. Um zu wissen, welche Tags vom Resource Tagger erstellt wurden, suchen Sie nach Tag-Schlüsseln mit dem Präfix. `ams:rt:`

Beschränken Sie den Zugriff auf die Bereitstellung mit den StartDeploymentund den StopDeploymentAPI-Aktionen auf vertrauenswürdige Benutzer, die sich mit den Verantwortlichkeiten und Konsequenzen der Implementierung einer neuen Konfiguration für Ihre Ziele auskennen.

Weitere Informationen zur Verwendung von AWS AppConfig Funktionen zum Erstellen und Bereitstellen einer Konfiguration finden Sie in der Dokumentation unter Working with AWS AppConfig.

Terraform so konfigurieren, dass Resource Tagger-Tags ignoriert werden

Wenn Sie Terraform für die Bereitstellung Ihrer Ressourcen verwenden und Resource Tagger verwenden möchten, um Ihre Ressourcen zu taggen, können die Resource Tagger-Tags von Terraform als Drift identifiziert werden.

Sie können Terraform so konfigurieren, dass alle Resource Tagger-Tags ignoriert werden, indem Sie den Lebenszyklus-Konfigurationsblock oder den globalen Konfigurationsblock ignore_tags verwenden. Weitere Informationen finden Sie in der Terraform-Dokumentation zum Resource Tagging unter Resource Tagging.

Das folgende Beispiel zeigt, wie Sie eine globale Konfiguration erstellen, um alle Tags zu ignorieren, die mit dem Resource Tagger-Tag-Präfix beginnen: `ams:rt:`

```
provider "aws" {
  # ... potentially other configuration ...

  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

Die Anzahl der von Resource Tagger verwalteten Ressourcen anzeigen

Resource Tagger sendet jede Stunde Metriken im `AMS/ResourceTagger` Namespace an Amazon CloudWatch. Metriken werden nur für Ressourcentypen ausgegeben, die von Resource Tagger unterstützt werden.

Metrikname	Dimensionen	Beschreibung
ResourceCount	Komponente, ResourceType	Anzahl der Ressourcen (des angegebenen Ressourcentyps), die in dieser Region bereitgestellt wurden. Einheiten: Anzahl
ResourcesMissingManagedTags	Komponente, ResourceType	Anzahl der Ressourcen (des angegebenen Ressourcentyps), für die gemäß den Konfigurationsprofilen verwaltete Tags erforderlich sind, die jedoch noch nicht von Resource Tagger markiert wurden. Einheiten: Anzahl
UnmanagedResources	Komponente, ResourceType	Anzahl der Ressourcen (des angegebenen Ressourcentyps) ohne verwaltete Tags, die vom

Metrikname	Dimensionen	Beschreibung
		Resource Tagger angewendet wurden. In der Regel entsprachen diese Ressourcen keinem Resource Tagger-Konfigurationsblock oder sind ausdrücklich aus Konfigurationsblöcken ausgeschlossen. Einheiten: Anzahl
MatchingResourceCount	Komponente, ResourceType ConfigClauseName	Anzahl der Ressourcen (des angegebenen Ressourcentyps), die dem Resource Tagger-Konfigurationsblock entsprechen. Damit eine Ressource dem Konfigurationsblock entspricht, muss der Block aktiviert sein und die Ressource muss dem Filter des Blocks entsprechen. Einheiten: Anzahl

Diese Metriken können auch als Grafiken im AMS-Resource-Tagger-Reporting-Dashboard angezeigt werden. Um das Dashboard aufzurufen, wählen Sie in der Amazon CloudWatch Management Console AMS-Resource-Tagger-Reporting-Dashboard aus. In den Diagrammen in diesem Dashboard werden standardmäßig die Daten für den Zeitraum der letzten 12 Stunden angezeigt.

AMS Accelerate sendet CloudWatch Alarme an Ihr Konto, um einen deutlichen Anstieg der Anzahl nicht verwalteter Ressourcen zu erkennen, z. B. Ressourcen, die durch AMS Resource Tagger von der Verwaltung ausgeschlossen wurden. AMS Operations untersucht die Zunahme nicht verwalteter Ressourcen, die Folgendes übersteigen: entweder drei Ressourcen desselben Typs oder einen Anstieg von 50% gegenüber allen Ressourcen desselben Typs. Wenn die Änderung nicht beabsichtigt zu sein scheint, wird AMS Operations Sie möglicherweise kontaktieren, um die Änderung zu überprüfen.

Verwenden CloudFormation , um Tags für AMS Accelerate zu erstellen

Sie können CloudFormation sie verwenden, um Tags auf Stack-Ebene (siehe CloudFormation Dokumentation, Resource-Tag) oder auf individueller Ressourcenebene (z. B. unter Tagging Ihrer EC2 Amazon-Ressourcen) anzuwenden.

> **Important**
>
> Für einige AMS Accelerate-Servicekomponenten sind Tags mit dem Präfix ams:rt: erforderlich. Resource Tagger geht davon aus, dass es Eigentümer dieser Tags ist, und löscht sie, wenn keine Resource Tagger-Konfigurationsregeln sie zulassen. Sie müssen immer ein Resource Tagger-Konfigurationsprofil für diese Tags bereitstellen, auch wenn Sie Terraform verwenden CloudFormation .

CloudFormation Anwendungsfälle für AMS Accelerate

In diesem Abschnitt werden häufig ausgeführte Aktionen mit aufgeführt CloudFormation.

Themen

Eine EC2 Instanz mit CloudFormation for Accelerate taggen

Im Folgenden finden Sie ein Beispiel dafür, wie Sie das Tag ams:rt:ams-managed mit dem Wert true auf eine Amazon-Instance anwenden können, die von verwaltet wird. EC2 CloudFormation Mit dem Tag ams:rt:ams-managed stimmen Sie zu, dass Ihre Ressourcen von AMS Accelerate überwacht werden.

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Eine AutoScaling Gruppe (ASG) mit CloudFormation for Accelerate taggen

Im Folgenden finden Sie ein Beispiel dafür, wie Sie das Tag ams:rt:ams-managed mit dem Wert true auf eine Auto Scaling Scaling-Gruppe anwenden können, die von verwaltet wird. CloudFormation Beachten Sie, dass die Auto Scaling Scaling-Gruppe ihre Tags an EC2 Amazon-Instances weitergibt, die von ihr erstellt wurden. Mit dem Tag ams:rt:ams-managed stimmen Sie zu, dass Ihre Ressourcen von AMS Accelerate überwacht werden.

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Bereitstellen eines Konfigurationsprofils mit CloudFormation for Accelerate

Wenn Sie Ihr `CustomerManagedTags` Konfigurationsprofil mithilfe von bereitstellen möchten CloudFormation, können Sie die folgenden CloudFormation Vorlagen verwenden. Geben Sie Ihre gewünschte JSON-Konfiguration in das `AMSResourceTaggerConfigurationVersion.Content` Feld ein.

Wenn Sie die Vorlagen in einem CloudFormation Stack oder Stack-Set bereitstellen, schlägt die Bereitstellung der `AMSResourceTaggerDeployment` Ressource fehl, wenn Sie das erforderliche JSON-Format für die Konfiguration nicht eingehalten haben. Einzelheiten Syntax und Struktur zum erwarteten Format finden Sie unter.

Hilfe zur Bereitstellung dieser Vorlagen als CloudFormation Stack oder Stack-Set finden Sie in der entsprechenden AWS CloudFormation Dokumentation unten:

- Einen Stack auf der AWS CloudFormation Konsole erstellen
- Einen Stack erstellen mit AWS CLI
- Ein Stack-Set erstellen

> **Note**
>
> Wenn Sie eine Konfigurationsversion mithilfe einer dieser Vorlagen bereitstellen und anschließend den CloudFormation Stack/das Stack-Set löschen, bleibt die Version der Vorlagenkonfiguration die aktuell bereitgestellte Version, und es erfolgt keine weitere Bereitstellung. Wenn Sie zu einer Standardkonfiguration zurückkehren möchten, müssen Sie entweder manuell eine leere Konfiguration bereitstellen (also nur{}) oder Ihren Stack auf eine leere Konfiguration aktualisieren, anstatt den Stack zu löschen.

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
```

```
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

Verwenden von Terraform zur Erstellung von Tags für AMS Accelerate

Wenn Sie AMS Accelerate Resource Tagger nicht verwenden möchten, können Sie mithilfe von Terraform Ihre eigenen Tags anwenden. Wenn Sie Resource Tagger jedoch nicht verwenden möchten, weil es von Ihren Terraform-Definitionen abweicht, gibt es eine Möglichkeit, den Resource Tagger zu verwenden und die dadurch verursachte Abweichung zu ignorieren; siehe. Terraform so konfigurieren, dass Resource Tagger-Tags ignoriert werden

> **Important**
>
> Einige AMS Accelerate-Dienstkomponenten benötigen Tags mit dem Präfix ams:rt:. Resource Tagger geht davon aus, dass es Eigentümer dieser Tags ist, und löscht sie, wenn keine Resource Tagger-Konfigurationsregeln sie zulassen. Sie müssen ein Resource Tagger-Konfigurationsprofil für diese Tags bereitstellen, auch wenn Sie Terraform verwenden. CloudFormation

Im Folgenden finden Sie ein Beispiel dafür, wie Sie das Tag ams:rt:ams-managed mit dem Wert true auf eine von Terraform verwaltete Amazon-Instance anwenden können. EC2 Mit dem Tag ams:rt:ams-managed stimmen Sie zu, dass Ihre Ressourcen von AMS Accelerate überwacht werden.

```
  resource "aws_instance" "sample_linux_instance" {
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Im Folgenden finden Sie ein Beispiel dafür, wie Sie das Tag ams:rt:ams-managed mit dem Wert true auf eine von Terraform verwaltete Auto Scaling Scaling-Gruppe anwenden können. Beachten Sie, dass die Auto Scaling Scaling-Gruppe ihre Tags an die EC2 Amazon-Instances weitergibt, die von ihr erstellt wurden. Mit dem Tag ams:rt:ams-managed stimmen Sie zu, dass Ihre Ressourcen von AMS Accelerate überwacht werden.

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Eine Beschreibung der Verwaltung von von Terraform erstellten Ressourcen-Tags finden Sie unter. Terraform so konfigurieren, dass Resource Tagger-Tags ignoriert werden

Vorfallberichte, Serviceanfragen und Fragen zur Abrechnung in AMS Accelerate

Mit AMS Accelerate können Sie jederzeit Hilfe bei betrieblichen Problemen und Anfragen über das AWS Support Center in der anfordern AWS-Managementkonsole. Die Betriebsingenieure von AMS Accelerate stehen zur Verfügung round-the-clock, um auf Ihre Vorfälle und Serviceanfragen zu reagieren. Für den Service gelten Service Level Agreements (SLAs) zur Reaktionszeit. Die Betriebsingenieure von AMS Accelerate benachrichtigen Sie mithilfe derselben Mechanismen proaktiv über wichtige Warnmeldungen und Fragen.

AMS Accelerate bietet eine Reihe von Betriebsdienstleistungen, die Sie dabei unterstützen, betriebliche Exzellenz zu AWS erreichen. Einen schnellen Überblick darüber, wie AMS Ihren Teams dabei hilft, AWS Cloud mit einigen unserer wichtigsten operativen Funktionen, darunter round-the-clock Helpdesk, proaktive Überwachung, Sicherheit, Patching, Protokollierung und Backup, allgemeine betriebliche Exzellenz zu erreichen, finden Sie in den AMS-Referenzarchitekturdiagrammen.

Themen

Vorfallmanagement in AMS Accelerate

In AMS Accelerate verwenden Sie die, AWS Support Center Consoleum Vorfallberichte einzureichen. Bei Vorfällen handelt es sich um AWS-Service Leistungsprobleme, die sich auf Ihre verwaltete Umgebung auswirken. Diese werden von AMS Accelerate oder Ihnen festgestellt. Vorfälle, die vom AMS Accelerate-Team identifiziert wurden, werden zunächst als Ereignisse empfangen (eine Änderung des Systemstatus, die durch die Überwachung erfasst wird). Wenn ein konfigurierter Schwellenwert überschritten wird, löst das Ereignis einen Alarm aus, der auch als Warnung bezeichnet wird. Das AMS Accelerate Operations Team bestimmt, ob das Ereignis keine Auswirkungen hat oder ob es sich um einen Vorfall (eine Betriebsunterbrechung oder -verschlechterung) oder um ein Problem (die zugrunde liegende Ursache für einen oder mehrere Vorfälle) handelt.

> **Note**
>
> Das AMS Accelerate-Team empfängt auch Vorfälle, die Sie programmgesteuert mithilfe der AWS-Support-API mit Servicecode erstellt haben. `service-ams-operations-report-incident`

Informationen zur Verwendung finden Sie Support unter Erste Schritte mit. Support

Was ist Incident Management?

Incident Management ist der Prozess, den AMS verwendet, um aktive Vorfälle aufzuzeichnen, darauf zu reagieren, den Fortschritt zu kommunizieren und darüber zu informieren.

Das Ziel des Incident-Management-Prozesses besteht darin, sicherzustellen, dass der normale Betrieb Ihres Managed Services so schnell wie möglich wiederhergestellt wird, die Auswirkungen auf das Geschäft minimiert werden und alle betroffenen Parteien auf dem Laufenden gehalten werden.

Beispiele für Vorfälle sind unter anderem der Verlust oder die Verschlechterung der Netzwerkkonnektivität, ein Prozess oder eine API, die nicht reagiert, oder eine geplante Aufgabe, die nicht ausgeführt wird (z. B. ein fehlgeschlagenes Backup).

Die folgende Grafik zeigt den Arbeitsablauf eines Vorfalls, den Sie AMS gemeldet haben.

Diese Grafik zeigt den Arbeitsablauf eines Vorfalls, der Ihnen von AMS gemeldet wurde.

Priorität des Vorfalls

Incidents, die im AWS Support Center, in der Konsole oder in der Support API (SAPI) erstellt wurden, haben andere Klassifizierungen als Incidents, die in der AMS-Konsole erstellt wurden.

- Niedrig: Nicht kritische Funktionen Ihres Geschäftsservices oder Ihrer Anwendung, die sich auf AWS- oder AMS-Ressourcen beziehen, sind betroffen.
- Mittel: Ein Unternehmensservice oder eine Anwendung, die sich auf AWS and/or AMS-Ressourcen bezieht, ist mäßig beeinträchtigt und funktioniert in einem heruntergestuften Zustand.
- Hoch: Ihr Unternehmen ist erheblich beeinträchtigt. Kritische Funktionen Ihrer Anwendung im Zusammenhang mit AWS and/or AMS-Ressourcen sind nicht verfügbar. Reserviert für die kritischsten Ausfälle, die Produktionssysteme betreffen.

> **Note**
>
> Die AWS-Supportkonsole bietet fünf Prioritätsstufen für Vorfälle, die wir in die drei AMS-Stufen übersetzen.

So funktionieren die Reaktion auf Vorfälle und deren Lösung

AMS Accelerate verwendet bewährte Methoden für das IT-Servicemanagement (ITSM) für das Incident-Management, um den Service bei Bedarf so schnell wie möglich wiederherzustellen.

Wir bieten rund um die Uhr follow-the-sun Support über Betriebszentren auf der ganzen Welt, wobei engagierte Mitarbeiter die Überwachungs-Dashboards und Warteschlangen für Zwischenfälle aktiv beobachten.

Unsere Betriebstechniker verwenden interne Tools zur Vorfallverfolgung, um Vorfälle zu identifizieren, zu protokollieren, zu kategorisieren, zu priorisieren, zu diagnostizieren, zu lösen und zu schließen. Über das AWS Support Center und die Support-API informieren wir Sie über alle diese Aktivitäten auf dem Laufenden AWS . Unsere Mitarbeiter nutzen eine Vielzahl interner AWS Support-Tools, um sie bei all diesen Aktivitäten zu unterstützen. Diese Betreiber sind mit der von AMS Accelerate unterstützten Infrastruktur bestens vertraut und verfügen über technische Fähigkeiten auf Expertenniveau, um festgestellte Support-Probleme zu lösen. Für den Fall, dass unsere Mitarbeiter Hilfe benötigen, stehen die Premium-Support- und AWS Serviceteams zur Verfügung.

Nachdem Ihr Vorfall beim AMS Accelerate Operations Team eingegangen ist, überprüfen wir in Zusammenarbeit mit Ihnen die Priorität und Klassifizierung, falls weitere Erläuterungen erforderlich sind. Wenn der Vorfallbericht beispielsweise besser als Serviceanfrage eingestuft ist, wird er neu klassifiziert und das AMS Accelerate Service Request-Team übernimmt die Arbeit, und Sie werden benachrichtigt. Wenn der Vorfall vom empfangenden Mitarbeiter behoben werden kann, werden Maßnahmen ergriffen, um den Vorfall schnell zu lösen. Die Mitarbeiter von AMS Accelerate suchen nach einer Lösung in der internen Dokumentation und leiten den Vorfall bei Bedarf an andere Support-Mitarbeiter weiter, bis der Vorfall behoben ist. Nach der Lösung dokumentiert das AMS Accelerate Operations Team den Vorfall und die Lösung für die future Verwendung.

In Fällen, in denen sich Vorfälle mit kritischem Schweregrad auf Ihre kritischen Workloads auswirken, empfiehlt AMS Accelerate möglicherweise eine Wiederherstellung der Infrastruktur. Oft besteht ein Kompromiss zwischen der Behebung eines Problems und der einfachen Wiederherstellung aus einem bekannten funktionierenden Backup. Dabei sind Ihre Risiken und Auswirkungen von

Serviceausfällen ausschlaggebend. Wenn Sie Zeit haben, sich der Problembehebung zu widmen, hilft Ihnen AMS Accelerate, und Ihr Cloud Service Delivery Manager (CSDM) wird möglicherweise eingeschaltet. Wenn die Wiederherstellung jedoch dringend ist, kann AMS Accelerate sofort eine Wiederherstellung einleiten.

Arbeiten mit Vorfällen in AMS Accelerate

Vom AWS Support Center aus können Sie die folgenden Aufgaben ausführen:

- Einen Vorfall melden und aktualisieren. Um einen AMS Accelerate-Vorfall zu melden, wählen Sie AMS Operations — Vorfall melden aus dem Menü Services.
- Sie erhalten eine Liste mit allen von Ihnen eingereichten Vorfällen und detaillierte Informationen zu diesen.
- Grenzen Sie Ihre Suche nach Vorfällen nach Status und anderen Filtern ein.
- Fügen Sie Mitteilungen und Dateianhänge zu Ihren Vorfällen hinzu und fügen Sie E-Mail-Empfänger für die Fallkorrespondenz hinzu.
- Initiieren Sie einen Live-Chat oder fordern Sie einen Rückruf zu Ihrem Vorfall an.

> **Note**
>
> Die Live-Chat-Funktion ist nicht für Sicherheitsereignisse vorgesehen. Erstellen Sie bei Sicherheitsproblemen eine Support-Anfrage mit hoher Priorität (P1 oder P2).

- Beheben Sie Vorfälle.
- Bewerten Sie die Kommunikation bei Vorfällen.

In den folgenden Beispielen wird beschrieben, wie Sie mithilfe des Support Centers einen Vorfall einreichen können. Nach der Übermittlung arbeitet das AMS Accelerate-Team mit Ihnen zusammen, um den Vorfall gemäß der AMS Accelerate-Standard-SLA zu lösen.

Einen Vorfall für Accelerate einreichen

Informationen zum Melden eines Vorfalls über das Support Center finden Sie in der Support-Dokumentation: Support-Fall erstellen

Um einen Vorfall über das Support Center zu melden:

1. Klicken Sie auf Fall erstellen. Die Seite „Incident-Fall erstellen“ wird geöffnet.

2. Öffnen Sie das Menü für den Problemtyp des technischen Supports und wählen Sie AMS Operations — Vorfall melden aus. Geben Sie Informationen zu Ihrem Vorfall ein und wählen Sie Erstellen aus.
3. Um bei jedem Schritt des Vorfallbehebungsprozesses per E-Mail informiert zu werden, müssen Sie unbedingt die Option CC-E-Mails ausfüllen. Wenn Sie die Verbindung über einen Verbund herstellen, melden Sie sich an, bevor Sie dem Link in der E-Mail folgen, die AMS Accelerate Ihnen über den Vorfall sendet.

> **Note**
>
> Die Beschreibung sollte so detailliert wie möglich sein. Schließen Sie relevante Ressourceninformationen zusammen mit allen weiteren Daten ein, die uns bei Ihrem Problem von Nutzen sein können. Für die Fehlersuche bei der Leistung sind beispielsweise Zeitstempel und Protokolle nützlich. Für Anforderungen von Funktionen oder allgemeine Anleitungsfragen, schließen Sie eine Beschreibung der Umgebung und des Zwecks mit ein. Befolgen Sie in allen Fällen die Description Guidance (Beschreibungsanleitung), welche in Ihrem Einreichformular des Falls erscheint.
> Wenn Sie so viele Details wie möglich angeben, erhöhen Sie die Chancen, dass Ihr Fall schnell behoben werden kann.

Sie können auch die AWS-Support-API mit Servicecode verwenden`service-ams-operations-report-incident`, um einen Vorfall zu melden.

Überwachung und Aktualisierung eines Accelerate-Vorfalls

Sie können Vorfallberichte und Serviceanfragen, beides sogenannte Fälle, mithilfe des Support Centers oder programmgesteuert mithilfe des Support API-Vorgangs aktualisieren, `DescribeCases`überwachen und überprüfen.

Gehen Sie wie folgt vor, um einen Fall, einen Vorfall oder eine Serviceanfrage mithilfe Support des Centers zu überwachen.

1. Navigieren Sie in der AWS Management-Konsole zu Support.
2. Wählen Sie in der linken Navigationsleiste Ihre Supportfälle aus, suchen Sie nach einem Fall und klicken Sie auf den Link Betreff, um eine Detailseite mit dem aktuellen Status und den Korrespondenzen zu öffnen.

Wenn Sie zu diesem Zeitpunkt Telefon oder Chat verwenden möchten, klicken Sie im Support Center auf Kundenvorgang öffnen, um die Seite Kundenvorgang erstellen im Support Center zu öffnen, die automatisch mit dem AMS-Servicetyp gefüllt wird.

Wenn ein gemeldeter Vorfall oder eine Serviceanfrage vom Accelerate Operations Team aktualisiert wird, erhalten Sie eine E-Mail und einen Link zu dem Vorfall im Support Center, damit Sie antworten können.

> **Note**
>
> Sie können auf die Fallkorrespondenz nicht antworten, indem Sie auf die E-Mail antworten.

Wenn das Dashboard viele Fälle enthält, können Sie die Option Filter verwenden:

- Betreff: Verwenden Sie diesen Filter, um nach Schlüsselwörtern im Betreff des Falls zu suchen.
- Schweregrad: Verwenden Sie diese Option, um Fälle nach Schweregrad zu filtern, indem Sie einen Schweregrad aus der Liste auswählen.
- Falltyp: Verwenden Sie diese Option, um alle Fälle eines bestimmten Falltyps anzuzeigen. Accelerate Incidents und Serviceanfragen werden zusammen mit allen servicespezifischen Fällen unter dem Falltyp Technischer Support angezeigt.
- Status: Verwenden Sie diese Option, um Anfragen nach Status zu filtern, indem Sie einen bestimmten Status aus der Liste auswählen.

3. Um den aktuellen Status zu überprüfen, aktualisieren Sie die Seite.
4. Wenn es so viele Korrespondenzen gibt, dass nicht alle auf der Seite angezeigt werden, wählen Sie „Mehr laden“.
5. Um den Status des Falls zu aktualisieren, wählen Sie Antworten, geben Sie die neue Korrespondenz ein und klicken Sie dann auf Absenden.
6. Um den Fall abzuschließen, nachdem er zu Ihrer Zufriedenheit gelöst wurde, wählen Sie Fall schließen.

   Achten Sie darauf, den Service anhand von 1-5 Sternen zu bewerten, damit AMS weiß, wie es uns geht.

Verwaltung von Accelerate-Vorfällen mit der Support-API

Sie können die Support API verwenden, um Vorfälle zu erstellen und während der Untersuchung Ihrer Probleme Korrespondenz mit Support Mitarbeitern hinzuzufügen. Die Support API modelliert einen Großteil des Verhaltens des AWS Support Centers.

Informationen darüber, wie Sie diesen AWS Support-Service nutzen können, finden Sie unter Programmieren der Lebensdauer eines AWS Support-Falls.

> **Note**
>
> Das AMS Accelerate-Team empfängt Vorfälle, die Sie programmgesteuert mithilfe des Servicecodes with erstellt haben. `service-ams-operations-report-incident`

Reaktion auf einen von AMS Accelerate generierten Vorfall

AMS Accelerate überwacht Ihre Ressourcen proaktiv. Weitere Informationen finden Sie unter Überwachung und Eventmanagement in AMS Accelerate. Manchmal identifiziert und erstellt AMS Accelerate einen Vorfall, meistens, um Sie über ein Ereignis zu informieren. Wenn Ihrerseits Maßnahmen zur Lösung eines Vorfalls erforderlich sind, sendet das AMS Accelerate-Team eine Benachrichtigung an die Kontaktinformationen, die Sie für das Konto angegeben haben. Sie reagieren auf diese Benachrichtigung genauso wie auf jeden anderen Vorfall — in der Regel über das Support Center, in einigen Fällen ist jedoch eine Kontaktaufnahme per E-Mail oder Telefon erforderlich.

> **Important**
>
> Um Benachrichtigungen über Statusänderungen für einen Vorfall oder eine Serviceanfrage zu erhalten, geben Sie eine E-Mail-Adresse in das Adressfeld ein.

Sieh dir Akshays Video an, um mehr zu erfahren (4:15)

Verwaltung von Serviceanfragen in Accelerate

Themen

AMS Accelerate nutzt das Service Request Management, um aktive Serviceanfragen aufzuzeichnen, darauf zu reagieren, den Fortschritt zu kommunizieren und Benachrichtigungen darüber bereitzustellen.

Das Ziel des Prozesses zur Verwaltung von Serviceanfragen besteht darin, sicherzustellen, dass Ihr verwalteter Service das bietet, was Sie benötigen.

Für abrechnungsbezogene Anfragen erstellen Sie eine Serviceanfrage.

> **Note**
>
> Das AMS Accelerate-Team empfängt Serviceanfragen, die Sie programmgesteuert mithilfe der AWS-Support-API mit Servicecode erstellt haben. `service-ams-operations-service-request`

Mit dem AWS Support Center können Sie die folgenden Aufgaben ausführen:

- Eine Serviceanfrage melden und aktualisieren. Wählen Sie für eine AMS Accelerate-Serviceanfrage im Menü Dienste die Option AMS Operation — Serviceanfrage aus.
- Sie erhalten eine Liste mit allen von Ihnen eingereichten Serviceanfragen und detaillierte Informationen zu diesen.
- Grenzen Sie Ihre Suche nach Serviceanfragen nach Status und anderen Filtern ein.
- Fügen Sie Ihren Anfragen Mitteilungen und Dateianhänge hinzu und fügen Sie E-Mail-Empfänger für die Fallkorrespondenz hinzu.
- Bearbeiten Sie Serviceanfragen.
- Bewerten Sie die Kommunikation mit Serviceanfragen.

Wann sollte eine Serviceanfrage für Accelerate verwendet werden

Die folgenden Beispiele beschreiben eine Serviceanfrage. Nachdem Sie eine Serviceanfrage eingereicht haben, arbeitet das AMS Accelerate-Team mit Ihnen zusammen, um die Anfrage gemäß Ihrem AMS-SLA zu lösen.

- AMS oder AWS allgemeine Hinweise
- Fragen im Zusammenhang mit Patch MW
- Fragen zum Backup-Zeitplan
- Fragen zur Funktionalität von AWS Diensten

Im Folgenden finden Sie Beispiele dafür, was in einer Serviceanfrage nicht angesprochen werden sollte:

- Probleme beim Zugriff
- Patch-Fehler
- Backup-Fehler

So funktioniert die Verwaltung von Serviceanfragen in Accelerate

Serviceanfragen werden vom AMS Accelerate Operations Team auf Abruf bearbeitet.

Nachdem Ihre Serviceanfrage beim AMS Accelerate Operations Team eingegangen ist, wird sie überprüft, um sicherzustellen, dass sie ordnungsgemäß als Serviceanfrage oder Vorfall eingestuft wurde. Wenn es als Vorfall neu klassifiziert wird, beginnt der AMS Accelerate-Incident-Management-Prozess und Sie erhalten eine Benachrichtigung.

Wenn der AMS Accelerate-Mitarbeiter die Serviceanfrage lösen kann, werden sofort entsprechende Schritte unternommen. Wenn es sich bei der Serviceanfrage beispielsweise um Architekturberatung oder andere Informationen handelt, verweist der Betreiber Sie auf die entsprechenden Ressourcen oder beantwortet die Frage direkt.

Wenn bei der Analyse Ihrer Serviceanfrage ein Fehler oder eine Funktionsanfrage festgestellt wird, sendet AMS Ihnen im Rahmen der Serviceanfrage eine Benachrichtigung. Da es keine voraussichtliche Ankunftszeit für Funktionsanfragen oder Bugfixes gibt, ist die ursprüngliche Serviceanfrage geschlossen. Wenden Sie sich an Ihren CSDM, wenn Sie weitere Fragen zur ursprünglichen Serviceanfrage haben.

Wenn die Serviceanfrage außerhalb des Geltungsbereichs von AMS Accelerate Operations liegt, sendet der Betreiber die Anfrage entweder an Ihren Cloud Service Delivery Manager, damit dieser mit Ihnen kommunizieren kann, oder an das entsprechende AWS Support-Team, zusammen mit einer E-Mail an Sie, welche Schritte unternommen werden.

Die Serviceanfrage ist erst gelöst, wenn Sie angegeben haben, dass Sie mit dem Ergebnis zufrieden sind.

> **Note**
>
> Wir empfehlen Ihnen, in jedem Fall eine Kontakt-E-Mail-Adresse, einen Namen und eine Telefonnummer anzugeben, um die Kommunikation zu erleichtern.

Eine Serviceanfrage in Accelerate erstellen

Gehen Sie folgendermaßen vor, um eine Serviceanfrage zu erstellen:

1. Navigieren Sie in der AMS Accelerate-Konsole zu Dashboard.
2. Wählen Sie Serviceanfrage öffnen. AMS — Serviceanfrage ist vorausgewählt.
3. Wählen Sie eine Kategorie.
4. Wählen Sie den Schweregrad (nur Plus- oder Premium-Stufen).
5. Geben Sie Informationen ein für:
   - Betreff: Ein beschreibender Titel für die Serviceanfrage.
   - Beschreibung: Eine umfassende Beschreibung der Serviceanfrage, der betroffenen Systeme und des erwarteten Ergebnisses einer Lösung.
6. Um eine Anlage hinzuzufügen, wählen Sie Dateien anhängen, suchen Sie nach der gewünschten Anlage und wählen Sie Öffnen. Um den Anhang zu löschen, wählen Sie das Löschsymbol
7. Kontaktieren Sie uns: Der Standardkontakt mit AMS über das Internet. Um andere Optionen auszuwählen:
   - Bevorzugte Kontaktsprache: Englisch ist die unterstützte Sprache für AMS Accelerate-Serviceanfragen.

- Web: Ihre Serviceanfrage wird über das Internet eingereicht und vom AMS Operations Team bearbeitet.
- Chat: Chatten Sie online mit einem Mitarbeiter von AMS Accelerate Operations. Diese Option fügt Sie der Chat-Warteschlange hinzu.
- Telefon: Ein Mitarbeiter von AMS Operations ruft Sie zurück. Geben Sie gegebenenfalls Ihre AWS-Region, Telefonnummer und Durchwahl ein.
- Zusätzliche Kontakte: Geben Sie alle zusätzlichen E-Mail-Adressen ein, die Sie in Ihre Serviceanfrage übernehmen möchten.

8. Wählen Sie Absenden aus.

   Es wird eine Seite mit den Falldetails mit Informationen zur Serviceanfrage geöffnet, z. B. Typ, Betreff, Erstellt, ID und Status. Außerdem wird ein Bereich „Korrespondenz“ angezeigt, der die Beschreibung der von Ihnen erstellten Anfrage enthält.

   Um einen Korrespondenzbereich zu öffnen und zusätzliche Informationen oder Statusaktualisierungen bereitzustellen, wählen Sie Antworten.

   Nachdem die Serviceanfrage gelöst wurde, wählen Sie „Fall lösen“.

   Wenn es so viele Korrespondenzen gibt, dass nicht alle auf der Seite angezeigt werden, wählen Sie „Mehr laden“.

   Achten Sie darauf, den Service anhand der 1-5 Sterne zu bewerten, damit AMS weiß, wie es uns geht.

> **Note**
>
> Wenn Sie die Funktionalität für Serviceanfragen testen möchten, empfehlen wir Ihnen, dem Betreff Ihrer Serviceanfrage eine Meldung hinzuzufügen, dass keine Maßnahmen ergriffen wurden, z. B. `AMSTestNoOpsActionRequired` Dann können Sie testen, ohne den Prozess zur Lösung von Serviceanfragen zu starten.
> Das AMS Accelerate-Team empfängt Serviceanfragen, die Sie programmgesteuert mithilfe der AWS-Support-API mit Servicecode erstellt haben. `service-ams-operations-service-request`

Überwachung und Aktualisierung einer Serviceanfrage für Accelerate

Gehen Sie wie folgt vor, um einen Fall, einen Vorfall oder eine Serviceanfrage mithilfe Support des Centers zu überwachen.

1. Navigieren Sie in der AWS Management-Konsole zu Support.
2. Wählen Sie in der linken Navigationsleiste Ihre Supportfälle aus, suchen Sie nach einem Fall und klicken Sie auf den Link Betreff, um eine Detailseite mit dem aktuellen Status und den Korrespondenzen zu öffnen.

   Wenn Sie zu diesem Zeitpunkt Telefon oder Chat verwenden möchten, klicken Sie im Support Center auf Kundenvorgang öffnen, um die Seite Kundenvorgang erstellen im Support Center zu öffnen, die automatisch mit dem AMS-Servicetyp gefüllt wird.

   Wenn ein gemeldeter Vorfall oder eine Serviceanfrage vom Accelerate Operations Team aktualisiert wird, erhalten Sie eine E-Mail und einen Link zu dem Vorfall im Support Center, damit Sie antworten können.

   > **Note**
   >
   > Sie können auf die Fallkorrespondenz nicht antworten, indem Sie auf die E-Mail antworten.

   Wenn das Dashboard viele Fälle enthält, können Sie die Option Filter verwenden:

   - Betreff: Verwenden Sie diesen Filter, um nach Schlüsselwörtern im Betreff des Falls zu suchen.
   - Schweregrad: Verwenden Sie diese Option, um Fälle nach Schweregrad zu filtern, indem Sie einen Schweregrad aus der Liste auswählen.
   - Falltyp: Verwenden Sie diese Option, um alle Fälle eines bestimmten Falltyps anzuzeigen. Accelerate Incidents und Serviceanfragen werden zusammen mit allen servicespezifischen Fällen unter dem Falltyp Technischer Support angezeigt.
   - Status: Verwenden Sie diese Option, um Anfragen nach Status zu filtern, indem Sie einen bestimmten Status aus der Liste auswählen.
3. Um den aktuellen Status zu überprüfen, aktualisieren Sie die Seite.

4. Wenn es so viele Korrespondenzen gibt, dass nicht alle auf der Seite angezeigt werden, wählen Sie „Mehr laden“.
5. Um den Status des Falls zu aktualisieren, wählen Sie Antworten, geben Sie die neue Korrespondenz ein und klicken Sie dann auf Absenden.
6. Um den Fall abzuschließen, nachdem er zu Ihrer Zufriedenheit gelöst wurde, wählen Sie Fall schließen.

   Achten Sie darauf, den Service anhand von 1-5 Sternen zu bewerten, damit AMS weiß, wie es uns geht.

Verwaltung von Serviceanfragen mit der Support-API für Accelerate

Sie können die AWS Support-API verwenden, um Serviceanfragen zu erstellen und ihnen während der Untersuchung Ihrer Probleme und Interaktionen mit AWS Support-Mitarbeitern Korrespondenz hinzuzufügen. Die AWS Support-API modelliert einen Großteil des Verhaltens des AWS Support Centers.

Das AMS-Team empfängt auch Serviceanfragen, die von Ihnen programmgesteuert mithilfe der AWS-Support-API mit dem Servicecode service-ams-operations-service -request erstellt wurden.

Weitere Informationen darüber, wie Sie diesen AWS Support-Service nutzen können, finden Sie unter Programmieren der Lebensdauer eines AWS Support-Falls.

Beantwortung einer von AMS Accelerate generierten Serviceanfrage

AMS Accelerate überwacht Ihre Ressourcen proaktiv. Weitere Informationen finden Sie unter. Überwachung und Eventmanagement in AMS Accelerate Manchmal erstellt AMS Accelerate eine Serviceanfrage oder eine Servicebenachricht für Sie, in der Regel, wenn zur Lösung einer Serviceanfrage Maßnahmen Ihrerseits erforderlich sind. In diesem Fall sendet das AMS Accelerate-Team eine Benachrichtigung an den Kontakt, den Sie für das Konto angegeben haben. Sie beantworten diese Serviceanfrage auf die gleiche Weise wie jeden anderen Fall — in der Regel über das Support Center, in einigen Fällen ist jedoch E-Mail- oder Telefonkorrespondenz erforderlich.

> **Important**
>
> Um Benachrichtigungen über Statusänderungen für eine Serviceanfrage oder einen Vorfall zu erhalten, müssen Sie eine E-Mail-Adresse in das Adressfeld eingegeben haben.

Benachrichtigungen werden nur an die E-Mail-Adresse gesendet, die dem Fall bei der Erstellung hinzugefügt wurde.

Der Link in der Benachrichtigungs-E-Mail funktioniert nur, wenn Sie einen E-Mail-Server in Ihrem AMS Accelerate-Verbundnetzwerk verwenden. Andernfalls können Sie auf die Korrespondenz antworten, indem Sie Ihre AMS Accelerate-Konsole aufrufen und die Seite mit den Falldetails verwenden.

Note

AMS Accelerate sendet Mitteilungen an Ihre primäre E-Mail-Adresse in Ihrem AWS Konto. Wir empfehlen, einen alternativen E-Mail-Alias für den Betriebskontakt hinzuzufügen, um den request/notification Servicemanagementprozess zu vereinfachen. Dies wird während des Onboarding-Prozesses von AMS Accelerate und in der zugehörigen Onboarding-Dokumentation behandelt.

Testen von Vorfallberichten und Serviceanfragen in Accelerate

Wenn Sie Vorfallberichte oder Serviceanfragen testen, bitten wir Sie, AMSTestNoOpsActionRequiredden Betreff mit anzugeben. Dadurch wird AMS darüber informiert, dass der Vorfall oder die Anfrage nur zu Testzwecken dient. Wenn die Betriebstechniker von AMS dies sehen, werden sie in keiner Weise darauf reagieren.

Fragen zur Abrechnung für AMS Accelerate

Gehen Sie wie folgt vor, um eine abrechnungsbezogene Frage einzureichen:

1. Öffnen Sie das AWS Support Center zu Hause #/. https://console.aws.amazon.com/support/
2. Wählen Sie Konto und Abrechnung.
3. Wählen Sie Create case (Fall erstellen) aus.
4. Wählen Sie Konto und Abrechnung und folgen Sie dann den Anweisungen, um Ihren Fall einzureichen.

Verwaltung geplanter Ereignisse in AWS Managed Services

AWS Managed Services (AMS) Planned Event Management (PEM) ist ein AMS-Serviceangebot. PEM engagiert, koordiniert und unterstützt Kundenveranstaltungen und Projekte mithilfe von AMS-Services. Das PEM hilft bei der Koordination einer Reihe verwandter Aktivitäten, die dem vereinbarten Umfang und Zeitplan der PEM-Veranstaltung oder des PEM-Projekts entsprechen.

AMS PEM-Kriterien

Eine geplante Veranstaltung ist ein umfangs- und zeitgebundenes Projekt. AMS verwendet die von Ihnen bereitgestellten Informationen (einschließlich Plan und Umfang, erwartete Ergebnisse und Änderungen, die der AMS-Betrieb voraussichtlich vornehmen wird), um Sie während der PEM-Aktivitäten effektiv zu unterstützen. Ihre Cloud-Architekten (CAs) überprüfen und bewerten dann die PEM-Aktivität auf Vollständigkeit, technische Implementierung und Einsatz des AMS Operations. Nach der Überprüfung durch CA überprüft AMS Operations die Pläne und stimmt sich mit Ihrem Cloud Service Delivery Manager (CSDM) über die Einbindung des Betriebsteams ab.

Arten von PEM

Im Folgenden sind die verfügbaren PEM-Typen aufgeführt:

- Spieltage
  - Operational Gameday: Ein szenariobasierter Spielansatz zur operativen Reaktion, der darauf abzielt, die Integration von Prozessen, Personen und Systemen zu validieren.
  - Security Gameday: Eine Strategie zur Reaktion auf Sicherheitsvorfälle, die einen szenariobasierten Spielansatz verwendet, um die Integration von Systemen, Prozessen und Personal zu bewerten.
- Sicherheitsereignis für Kunden: Geplante Sicherheitsereignisse. Zum Beispiel Penetrationstests.
- Migrationsunterstützung: Support für geplante Onboarding- und Migrationsaktivitäten.

Dieser Workflow erleichtert die Zusammenarbeit mit AMS bei der Koordination von geplanten Veranstaltungen und Migrationsaktivitäten im Zusammenhang mit der AMS-Unterstützung. Wenn Sie Unterstützung bei Ihren spezifischen Anforderungen benötigen, wenden Sie sich an Ihren CSDM.

Der AMS PEM-Prozess

Der PEM-Prozess besteht aus den folgenden Phasen:

- PEM-Initiierung: Sie arbeiten mit Ihrem CSDM zusammen, um Ihr Ziel für die geplante Veranstaltung zu definieren und zu ermitteln, was von AMS Operations benötigt wird. AMS CAs überprüft die technischen Aspekte des PEM-Plans. Die CAs Zusammenarbeit mit AMS Security and Operations befasst sich mit der Einhaltung von Vorschriften, der Optimierung und Automatisierung der Ausführung sowie der Definition von Aufgaben und Ergebnissen für die Ausführung vor dem PEM. Anschließend erstellt Ihr CSDM das PEM-Ticket und stellt AMS die Projektinformationen und technischen Details zur Verfügung. AMS benötigt eine Vorlaufzeit von 14 Kalendertagen, damit das AMS Operations Team Zeit für die Planung, technische Überprüfung und Zuweisung von Ressourcen hat.
- PEM-Überprüfung: Das AMS Operations Team prüft die PEM-Anfrage und überprüft gemeinsam mit Ihrem CSDM, ob die Informationen im PEM-Plan korrekt und vollständig sind.
- PEM-Akzeptanz: AMS überprüft die bereitgestellten Informationen und teilt dem CSDM mit, in welchem Umfang der Support während der PEM-Aktivität angeboten wird. Wenn das PEM vollständige Informationen enthält und Ihr CSDM dem Umfang der Arbeit zustimmt, ist das PEM genehmigt.
- Vorbereitung und Ausführung: AMS stellt sicher, dass die vor Beginn des PEM erforderlichen Aufgaben erledigt werden, und erleichtert die interne Kommunikation und die Kundenkommunikation. AMS stellt sicher, dass der PEM-Plan ordnungsgemäß ausgeführt wird, und erstellt Status- und Fortschrittsberichte.

PEM FAQs

Wie kontaktiere ich AMS über Cases: Service Request (SRs) /Incident während einer PEM-Veranstaltung?

- Verwenden Sie die von Ihrem CSDM geteilte PEM-ID in der RFC/SR Betreffzeile des Formats. *PEM-ID*

  Gegebenenfalls können Sie die Live-Kontaktoption verwenden.
- Sie können auch eine Serviceanfrage (SR) erstellen, um Ihre Anwendungsfälle zu besprechen oder Fragen zu Ihrer geplanten Veranstaltung zu stellen. Wenn Sie eine SR verwenden, muss die PEM nicht gültig sein.

Welche Validierungen werden durchgeführt, wenn ein PEM-bezogener Fall eingereicht wird?

- Überprüfung, ob die Konto-ID auf dem PEM aufgeführt ist.
- Überprüfung, ob der PEM-Status zwischen den angegebenen Start- und Enddaten genehmigt und aktiv ist.
- AMS-Technikern wird intern ein Link zu den PEM-Details zur Verfügung gestellt.

Gibt es SLAs oder SLOs für PEM-Anfragen?

- PEMs sind nicht mit SLAs oder SLOs verknüpft.
- SLAs und SLOs für PEM-bezogene Arbeitsaufgaben (Service Request, Incidents) werden von AMS definiert. SLOs

  Weitere Informationen finden Sie unter Vorfallberichte, Serviceanfragen und Fragen zur Abrechnung in AMS Accelerate.

Können wir ein PEM über eine Serviceanfrage (SR) erstellen?

- Nein, die PEM-Erstellung muss vom Cloud Service Delivery Manager (CSDM) verwaltet werden.

Betrieb auf Abruf

Operations on Demand (OOD) ist eine Funktion von AWS Managed Services (AMS), die den Standardumfang Ihres AMS-Betriebsplans erweitert, indem sie Betriebsdienste bereitstellt, die derzeit nicht nativ in den AMS-Betriebsplänen oder AWS angeboten werden. Nach der Auswahl wird das Katalogangebot durch eine Kombination aus Automatisierung und hochqualifizierten AMS-Ressourcen bereitgestellt. Es gibt keine langfristigen Verpflichtungen oder zusätzlichen Verträge, sodass Sie Ihr bestehendes AMS sowie Ihre AWS Betriebsabläufe und Kapazitäten nach Bedarf erweitern können. Sie erklären sich damit einverstanden, monatliche Stundenblöcke (OOD-Blöcke), 20 Stunden pro Block, zu erwerben.

Sie können aus dem Katalog der standardisierten Angebote auswählen und über eine Serviceanfrage ein neues OOD-Engagement einleiten. Zu den OOD-Angeboten gehören beispielsweise die Unterstützung bei der Wartung von Amazon EKS, dem Betrieb und der AWS Control Tower Verwaltung von SAP-Clustern. Je nach Nachfrage und den am häufigsten auftretenden betrieblichen Anwendungsfällen werden regelmäßig neue Katalogangebote hinzugefügt.

OOD ist sowohl für die Betriebspläne AMS Advanced als auch für AMS Accelerate verfügbar und in allen Ländern verfügbar, in AWS-Regionendenen AMS verfügbar ist.

AMS führt das Kundensicherheitsrisikomanagement (CSRM) durch und implementiert gleichzeitig die von Ihnen gewünschten Änderungen. Weitere Informationen zum CSRM-Prozess finden Sie unter Sicherheitsüberprüfungen für Änderungsanträge.

Angebotskatalog für Operations on Demand

Operations on Demand (OOD) bietet Ihnen die in der folgenden Tabelle beschriebenen Dienste.

> **Note**
>
> Definitionen der wichtigsten Begriffe finden Sie in der AWS Managed Services Services-Dokumentation Wichtige Begriffe.

Betriebsplan	Titel	Beschreibung	Erwartete Ergebnisse

AMS Accelerate	Wartung des Amazon EKS-Clusters	AMS entlastet Ihre Container-Entwickler, indem es die laufende Wartung Ihrer Amazon Elastic Kubernetes Service (Amazon EKS) -Bereitstellungen übernimmt. AMS führt die zur Aktualisierung eines Clusters erforderlichen end-to-end Verfahren durch und adressiert dabei die Komponenten der Kontrollebene, der Add-Ons und der Knoten. AMS führt die Aktualisierung der verwalteten Knotentypen sowie eines kuratierten Satzes von Amazon EKS- und Kubernetes-Add-Ons durch.	Kundenteams halfen bei den zugrunde liegenden Betriebsarbeiten zur Aktualisierung von Amazon EKS-Clustern.

AMS Accelerate	AMI-Gebäude und Verkauf	AMS bietet seinen Kunden die laufende Verwaltung des Aufbaus und Verkaufs von AMI. Unsere Techniker führen monatliche Releases von abonnierten AMIs, On-Demand-Releases AMIs für neue Patch-Aktivitäten durch, verwalten Änderungen mithilfe von Runbooks und überwachen AMI-Builds mithilfe von Monitoring. CloudWatch Wir bieten auch Unterstützung bei der Fehlerbehebung und detaillierte Berichte für alle Benutzer, die in bestimmten Konten AMIs verwendet werden. Für dieses Angebot müssen AMI-Build-Pipelines über EC2 Image Builder bereitgestellt werden. AMS unterstützt keine anderen Automatisierungen oder Dienste, die mit EC2 Image Builder interagieren.	Die Sicherheitslage der Kunden verbesserte sich und der Zeitaufwand der Kunden für Gebäude und Verkauf wurde AMIs reduziert.

AMS Accelerate	Kuratierte Ausführung von Änderungen	Arbeiten Sie mit unseren erfahrenen Betriebsingenieuren zusammen, um Ihre Geschäftsanforderungen in validierte Änderungsanforderungen umzusetzen, die sicher in Ihrer AWS Umgebung ausgeführt werden können. Nutzen Sie unseren einzigartigen Automatisierungsansatz und unser Wissen über bewährte betriebliche Verfahren (z. B. Folgenabschätzung, Rollbacks, Zwei-Personen-Regel), unabhängig davon, ob es sich um eine einfache Änderung im großen Maßstab oder um eine komplexe Maßnahme mit nachgelagerten Auswirkungen handelt.	Kunden halfen uns bei der Definition, Erstellung und Ausführung von individuellen Änderungsanforderungen. Änderungen können manuell oder automatisiert (CloudFormation, SSM) erfolgen. Beinhaltet bei Bedarf eine Beratung Support zur Konfiguration. Nicht für Änderungen am Anwendungscode, für die Installation/Bereitstellung von Anwendungen, für die Datenmigration oder für Änderungen der Betriebssystemkonfiguration vorgesehen.

AMS Accelerate	AWS Network Firewall Operationen	AMS arbeitet mit Ihnen zusammen, um Ihre Firewall zu integrieren und die Richtlinien und Regeln für den laufenden Firewall-Betrieb zu implementieren und zu verwalten. Zu diesem Zweck nutzen unsere Techniker unsere betrieblichen Best Practices und Automatisierung, um standardisierte Richtlinien und Regeln zu konfigurieren, und indem sie die Überwachung aktivieren, um Änderungen zu erkennen, die außerhalb des Automatisierungsprozesses vorgenommen wurden. AMS benachrichtigt Sie schnell über unerwünschte Änderungen und bietet Optionen, um diese auf Anfrage einzubeziehen oder das Konto auf eine frühere Konfiguration zurückzusetzen, um die Gesamtstabilität Ihrer Systeme zu gewährleisten.	Die Kundenteams halfen bei der Reduzierung des Verwaltungsaufwands, indem sie unbeabsichtigte Änderungen an der Netzwerk-Firewall schnell erkannten, was zu einer verbesserten Problembehebung und einer kürzeren Ursachenanalyse sowohl für erwartete als auch für unerwartete Probleme führte.

AMS Accelerate	AWS Control Tower Betriebsabläufe	Kontinuierlicher Betrieb und Verwaltung Ihrer AWS Control Tower landing zone, einschließlich AWS Transit Gateway, und AWS Organizations Bereitstellung einer umfassenden Landezonenlösung. Wir kümmern uns um den Verkauf von Konten, das SCP- und OU-Management, die Behebung von Störungen, die SSO-Benutzerverwaltung und AWS Control Tower Upgrades mit unserer Bibliothek an benutzerdefinierten Steuerungen und Leitplanken.	Die Kundenteams helfen bei einigen der zugrunde liegenden Betriebsarbeiten wie Management AWS Control Tower, AWS Transit Gateway und AWS Organizations.

AMS Accelerate	AWS landing zone Beschleunigen Sie den Betrieb	AMS sorgt für den laufenden Betrieb der AWS Landezonen, die über den AWS Landing Zone Accelerator (LZA) eingerichtet wurden. Unsere Techniker kümmern sich um Änderungen an Konfigurationsdateien, das AWS Control Tower (CT) -Umgebungsmanagement (Kontoverkauf, OU-Erstellung, CT-Guardrails), die Verwaltung der Service Control Policy (SCP), die Erkennung und Behebung von CT-Driften, das Netzwerkkonfigurationsmanagement sowie Updates für CT und das LZA-Framework. AWS LZA bietet die Möglichkeit, eine sichere AWS Umgebung mit mehreren Konten einzurichten und zu verwalten. Dabei kommen bewährte betriebliche Verfahren und Dienste zum Einsatz, wie z. AWS Control Tower	Die Kundenteams unterstützten den laufenden Betrieb und die Verwaltung der AWS Landing Zone Accelerator-Lösung.

AMS Accelerate	SAP-Cluster-Assistent	Dedizierte Alarmierung, Überwachung, Cluster-Patching, Sicherung und Behebung von Zwischenfällen für Ihre SAP-Cluster. Mit diesem Katalogelement können Sie Ihrem SAP-Betriebsteam einen Teil der laufenden operativen Arbeit abnehmen, sodass es sich auf das Kapazitätsmanagement und die Leistungsoptimierung konzentrieren kann.	SAP-Teams von Kunden oder Partnern haben uns bei einigen der zugrunde liegenden Betriebsarbeiten unterstützt. Der Kunde muss jedoch weitere SAP-Funktionen wie Kapazitätsmanagement, Leistungsoptimierung, DBA und SAP-Basisadministration bereitstellen.

AMS Accelerate	SQL Server im laufenden Betrieb EC2	AMS arbeitet mit Ihnen zusammen, um den laufenden Betrieb Ihrer auf EC2 Instances bereitgestellten SQL Server-Datenbanken zu integrieren, zu implementieren und zu verwalten. Unsere Techniker nutzen unsere betrieblichen Best Practices und Automatisierung, um Ihre Datenbankteams zu entlasten, indem sie Aufgaben wie Backup und Patching übernehmen, den AMS-Betriebssupport auf SQL Server-Patching ausweiten, um clusterfähige fortlaufende Updates, Sicherungs- und Wiederherstellungsservices im Einklang mit unserer Ransomware-Abwehrstrategie und die Überwachung der Einhaltung der vom Kunden bereitgestellten Sicherungs- und Patchkontrollen zu überwachen.	SQL Server-Kunden halfen beim Auslagern von Patching- und Backup-Datenbankoperationen, um die Ausfallsicherheit und den Sicherheitsstatus ihrer Workloads zu verbessern und zusätzlich die Lizenzkosten zu optimieren, indem sie ihre eigenen Lizenzen (BYOL) einführten EC2.

AMS Advanced	Wartung des Amazon EKS-Clusters	AMS entlastet Ihre Container-Entwickler, indem es sich um die laufende Wartung und Integrität Ihrer Amazon Elastic Kubernetes Service (Amazon EKS) -Bereitstellungen kümmert. AMS führt die zur Aktualisierung eines Clusters erforderlichen end-to-end Verfahren durch und adressiert dabei die Komponenten der Kontrollebene, der Add-Ons und der Knoten. AMS führt die Aktualisierung der verwalteten Knotentypen sowie eines kuratierten Satzes von Amazon EKS- und Kubernetes-Add-Ons durch.	Kundenteams halfen bei den zugrunde liegenden Betriebsarbeiten zur Aktualisierung von Amazon EKS-Clustern.
AMS für Fortgeschrittene	Vorrangige RFC-Ausführung	Eigene Kapazität eines AMS Operations Engineers, der die Ausführung Ihrer Änderungsanträge (RFC) priorisiert. Alle Einsendungen erhalten eine höhere Anzahl an Antworten, und die Prioritätsreihenfolge kann angepasst werden, indem Sie über einen Amazon Chime Chime-Besprechungsraum direkt mit den Technikern interagieren.	Kunden erhalten eine Antwort innerhalb von 8 Stunden für RFCs.

AMS Advanced und AMS Accelerate	Upgrade eines älteren Betriebssystems	Vermeiden Sie eine Instanzmigration, indem Sie Instanzen auf eine unterstützte Betriebssystemversion aktualisieren. Wir können ein direktes Upgrade für Ihre ausgewählten Instanzen durchführen und dabei die Automatisierungs- und Upgrade-Funktionen der Softwareanbieter nutzen (z. B. Microsoft Windows 2008 R2 auf Microsoft Windows 2012 R2). Dieser Ansatz ist ideal für ältere Anwendungen, die nicht einfach auf einer neuen Instanz neu installiert werden können, und bietet zusätzlichen Schutz vor bekannten und nicht abgemilderten Sicherheitsbedrohungen auf älteren Betriebssystemversionen. Die folgenden Betriebssysteme werden für direkte Upgrades unterstützt: • Microsoft Windows 2012 R2 auf Microsoft Windows 2016 und höher • Microsoft Windows 2016 bis Microsoft Windows 2022 und höher • Von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 • Von Red Hat Enterprise Linux 8 auf Red Hat Enterprise Linux 9 • Von Oracle Linux 7 auf Oracle Linux 8	Diese Lösung wird für Anwendungen bereitgestellt, die nicht mehr auf einer neuen Instance neu installiert werden können (z. B. verlorener Quellcode, ausgefallener ISV usw.). Sie können fehlgeschlagene Upgrades in ihren ursprünglichen Zustand zurückversetzen. Aus betrieblicher Sicht ist ein Rollback vorzuziehen, da dadurch die Instance in einen Zustand versetzt wird, der mit den neuesten Sicherheitspatches besser unterstützt werden kann.

Themen

AMS Operations on Demand anfordern

AWS Managed Services (AMS) Operations on Demand (OOD) ist für alle verfügbar AWS-Konten , die bei AMS integriert wurden. Um Operations on Demand nutzen zu können, fordern Sie zusätzliche Informationen von Ihrem Cloud Service Delivery Manager (CSDM), Solutions Architect (SA), Account Manager oder Cloud Architect (CA) an. Die verfügbaren OOD-Angebote sind in der vorherigen Tabelle des Operations on Demand-Angebotskatalogs aufgeführt. Reichen Sie nach Abschluss des Auftragsumfangs eine Serviceanfrage an AMS Operations ein, um einen Auftrag für OOD einzuleiten.

Jede OOD-Serviceanfrage muss die folgenden detaillierten Informationen zum Auftrag enthalten:

- Die angeforderten spezifischen OOD-Angebote und für jedes spezifische OOD-Angebot:
  - Die Anzahl der Blöcke (ein Block entspricht 20 Stunden Betriebsressourcenzeit in einem bestimmten Kalendermonat, die zum jeweils aktuellen Standardtarif für AWS das jeweilige Operations on Demand-Angebot berechnet werden), die dem jeweiligen OOD-Angebot zugewiesen werden sollen.
  - Die Konto-ID für jedes AWS Managed Services Services-Konto, für das das spezifische OOD-Angebot angefordert wird.

OOD-Serviceanfragen müssen von Ihnen über einen der folgenden Kanäle eingereicht werden:

- Das AWS Managed Services Services-Konto, das die entsprechenden Operations on Demand-Angebote erhält, oder
- Ein AWS Managed Services Services-Konto, bei dem es sich um ein AWS Organizations Verwaltungskonto im Modus mit allen Funktionen handelt, und zwar im Namen aller Mitgliedskonten, bei denen es sich um AWS Managed Services Services-Konten handelt.

Nach Eingang der OOD-Serviceanfrage überprüft AMS Operations die Konten und aktualisiert sie mit deren Genehmigung, teilweiser Genehmigung oder Ablehnung.

Sobald die Serviceanfrage für das OOD-Angebot genehmigt wurde, stimmen sich AMS und Sie ab, um mit dem Auftrag zu beginnen. Es werden keine OOD-Angebote initiiert, bis die Serviceanfrage genehmigt und ein Startdatum für den Auftrag vereinbart wurde.

AMS verwendet eine monatliche Abonnementzuweisung von OOD-Blöcken. Wir weisen die genehmigte Anzahl von Blöcken monatlich zu, beginnend mit dem Startdatum des Engagements, bis Sie mit einer neuen Serviceanfrage die Abmeldung beantragen. OOD-Blöcke sind für einen Kalendermonat gültig. Ungenutzte Blöcke oder Blockteile werden nicht auf future Monate übertragen oder übertragen.

Ihnen wird jeden Monat mindestens ein OOD-Block in Rechnung gestellt, unabhängig von der Anzahl der tatsächlich genutzten Stunden. Jeder zusätzliche zugewiesene OOD-Block, für den keine Stunden genutzt wurden, wird nicht in Rechnung gestellt.

Änderungen an den Operations on Demand-Angeboten vornehmen

Um Änderungen an laufenden Aufträgen für Operations on Demand (OOD) -Angebote zu beantragen, reichen Sie eine Serviceanfrage ein, die folgende Informationen enthält:

- Die angeforderte (n) Änderung (en) und
- Das Datum, an dem die Änderungen in Kraft treten sollen.

Nach Erhalt der OOD-Serviceanfrage prüft AMS Operations die Anfrage und gibt entweder deren Zustimmung oder bittet den zuständigen CSDM, gemeinsam mit Ihnen den Umfang und die Auswirkungen der Änderung zu ermitteln. Wenn festgestellt wird, dass für die Änderung eine Überprüfung des Umfangs mit dem CSDM erforderlich ist, müssen Sie eine zweite OOD-Serviceanfrage einreichen, um den geänderten Auftrag nach Abschluss der Scoping-Maßnahme einzuleiten.

Nach der Genehmigung wird und bleibt die zuletzt geänderte Blockzuweisung aktiv und ersetzt alle vorherigen Blockzuweisungen, sofern mit Ihnen nichts anderes vereinbart wurde. AWS

Berichte und Optionen

AWS Managed Services (AMS) sammelt Daten aus verschiedenen nativen AWS-Services, um Mehrwertberichte zu wichtigen AMS-Angeboten bereitzustellen.

AMS bietet zwei Arten von detaillierten Berichten:

- Berichte auf Anfrage: Sie können bestimmte Berichte ad hoc über Ihren Cloud Service Delivery Manager (CSDM) anfordern. Diese Berichte haben kein Limit, da Sie sie während des Onboardings oder bei kritischen Ereignissen möglicherweise mehrmals anfordern müssen. Beachten Sie jedoch, dass diese Berichte nicht so konzipiert sind, dass sie nach einem Zeitplan wie wöchentliche Berichte bereitgestellt werden. Um Ihre Bedürfnisse besser zu verstehen oder weitere Informationen zur Verwendung von Self-Service-Berichten zu erhalten, wenden Sie sich an Ihren CSDM.
- Self-Service-Berichte: Mit den Self-Service-Berichten von AMS können Sie Daten beliebig oft direkt abfragen und analysieren. Verwenden Sie Self-Service-Berichte, um von der AMS-Konsole aus auf Berichte zuzugreifen und Datensätze über S3-Buckets (ein Bucket pro Konto) zu melden. Auf diese Weise können Sie die Daten in Ihr bevorzugtes Business Intelligence (BI) -Tool integrieren, sodass Sie Berichte an Ihre Anforderungen anpassen können.

Themen

Berichte auf Anfrage

Themen

AMS sammelt Daten aus verschiedenen nativen AWS-Services, um Mehrwertberichte zu wichtigen AMS-Angeboten bereitzustellen. Eine Kopie dieser Berichte erhalten Sie bei Ihrem Cloud Service Delivery Manager (CSDM).

AMS-Host-Management-Berichte

Verfügbare Berichte

- Bericht über die Abdeckung durch SSM-Agenten

Bericht über die Abdeckung durch SSM-Agenten

Der Bericht zur Abdeckung des AMS SSM-Agenten informiert Sie darüber, ob auf den EC2 Instances im Konto der SSM-Agent installiert ist oder nicht.

Name des Felds	Definition
Name des Kunden	Kundenname für Situationen, in denen es mehrere Unterkunden gibt
Region der Ressource	AWS Region, in der sich die Ressource befindet
Account name (Kontoname)	Der Name des Kontos
AWS Konto-ID	Die ID des AWS Kontos
Ressourcen-ID	ID der EC2 Instanz
Ressourcenname	Name der EC2 Instanz
Konforme Flagge	Gibt an, ob auf der Ressource der SSM-Agent installiert ist („Compliant“) oder nicht („NON_COMPLIANT“)

AMS Backup-Berichte

Verfügbare Berichte

- Bericht über Erfolg- und Fehlschlag des Backup-Jobs

- Bericht „Backup-Zusammenfassung“
- Summary/Coverage Backup-Bericht

Bericht über Erfolg- und Fehlschlag des Backup-Jobs

Der Success/Failure Backup-Job-Bericht enthält Informationen über Backups, die in den letzten Wochen ausgeführt wurden. Um den Bericht anzupassen, geben Sie die Anzahl der Wochen an, für die Sie Daten abrufen möchten. Die Standardanzahl von Wochen ist 12. In der folgenden Tabelle sind die im Bericht enthaltenen Daten aufgeführt:

Name des Felds	Definition
AWS-Konto-ID	AWS-Konto-ID, zu der die Ressource gehört
Kontoname	AWS-Kontoname
Backup-Job-ID	Die ID des Backup-Jobs
Ressourcen-ID	Die ID der gesicherten Ressource
Ressourcentyp	Der Typ der Ressource, die gesichert wird
Region der Ressource	Die AWS Region der gesicherten Ressource
Backup-Status	Der Status des Backups. Weitere Informationen finden Sie unter Status von Backup-Jobs
ID des Wiederherstellungspunkts	Die eindeutige Kennung des Wiederher stellungspunkts
Statusmeldung	Beschreibung der Fehler oder Warnungen, die während des Backup-Jobs aufgetreten sind
Größe des Backup	Größe des Backups in GB
ARN für den Wiederherstellungspunkt	Der ARN des erstellten Backups
Alter des Wiederherstellungspunkts in Tagen	Anzahl der Tage, die seit der Erstellung des Wiederherstellungspunkts vergangen sind

Name des Felds	Definition
Weniger als 30 Tage alt	Indikator für Backups, die weniger als 30 Tage alt sind

Bericht „Backup-Zusammenfassung“

Name des Felds	Definition
Name des Kunden	Kundenname für Situationen, in denen mehrere Unterkunden
Backup-Monat	Monat des Backups
Jahr des Backup	Jahr des Backups
Ressourcentyp	Der Typ der Ressource, die gesichert wird
Anzahl der Ressourcen	Die Anzahl der Ressourcen, die gesichert wurden
Anzahl der Wiederherstellungspunkte	Anzahl der unterschiedlichen Schnappschüsse
Backups, die weniger als 30 Tage alt sind	Die Anzahl der Backups, die weniger als 30 Tage alt sind
Maximales Alter des Wiederherstellungspunkts	Das älteste Alter des Wiederherstellungspunkts seit Tagen
Mindestalter des Wiederherstellungspunkts	Das letzte Alter des Wiederherstellungspunkts in Tagen

Summary/Coverage Backup-Bericht

Der Summary/Coverage Backup-Bericht listet auf, wie viele Ressourcen derzeit durch keinen AWS Backup Plan geschützt sind. Besprechen Sie mit Ihrem CDSM einen geeigneten Plan, um die Abdeckung nach Möglichkeit zu erhöhen und das Risiko eines Datenverlusts zu verringern.

Name des Felds	Definition
Name des Kunden	Kundenname für Situationen, in denen mehrere Unterkunden
Region	AWS Region, in der sich die Ressource befindet
Account name (Kontoname)	Der Name des Kontos
AWS Konto-ID	Die ID des AWS Kontos
Ressourcentyp	Typ der Ressource. Ressourcen werden unterstützt von AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EFS EC2 FSx, RDS und S3)
ARN-Ressourcen	ARN der Ressource
Ressourcen-ID	ID der Ressource
Abdeckung	Gibt an, ob die Ressource abgedeckt ist oder nicht („COVERED“ oder „NOT_COVERED“)
Anzahl der Ressourcen	Anzahl der unterstützten Ressourcen im Konto
perc_coverage	Prozentsatz der unterstützten Ressourcen, für die in den letzten 30 Tagen ein Backup ausgeführt wurde.

AWS Config Bericht zur Einhaltung der Kontrollvorschriften

Der AWS Config Control Compliance-Bericht bietet einen detaillierten Einblick in die Ressourcen- und AWS Config Regelkonformität von AMS-Konten. Sie filtern den Bericht nach dem Schweregrad der Konfigurationsregel, um die wichtigsten Ergebnisse zu priorisieren. In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt:

field	Beschreibung
Datum	Datum des Berichts
Kundenname	Kundenname
AWS Konto-ID	Zugeordnete AWS Konto-ID für den Kunden
Quellen-ID	AWS Config eindeutige Quell-ID der Regel
Beschreibung der Regel	AWS Config Beschreibung der Regel
Regeltyp	AWS Config Art der Regel
Konformitätskennzeichnung	AWS Config Status der Regelkonformität
Ressourcentyp	AWS Art der Ressource
Ressourcenname	AWS Name der Ressource
Schweregrad	Von AMS definierter empfohlener Standards chweregrad für die AWS Config Regel
Kategorie „Problembehebung“	Zugeordnete Kategorie der Abhilfemaßnahme für eine Regel AWS Config
Beschreibung der Problembehebung	Erläuterung der Abhilfemaßnahme, damit die AWS Config Regel konform ist
Kundenaktion	Maßnahmen des Kunden sind erforderlich, um sicherzustellen, dass die AWS Config Regel konform ist
Bericht über Delta-Metriken	Änderungen im Hinblick auf die Einhaltung einer Regel zwischen den beiden angegebenen Terminen

Bericht zur Konfiguration der Antwort von AMS Config Rules

Der Bericht zur Antwortkonfiguration von AMS Config Rules bietet einen detaillierten Überblick darüber, wie Sie Accelerate derzeit so konfiguriert haben, dass es auf nicht konforme AMS-Konfigurationsregeln reagiert. Weitere Informationen zum Ändern der Antwort auf AMS-Konfigurationsregeln finden Sie unter AMS Accelerate Customized Findings Responses.

Dieser Bericht zeigt nur die Konfigurationen, die Sie geändert haben, und schließt die AMS-Standardkonfigurationen aus, die in der AMS Config Rules Library aufgeführt sind. Der Bericht enthält Daten zur Konfiguration von AMS-Konten mit Ressourcen- und AMS-Konfigurationsregeln, einschließlich der folgenden Daten:

- Die Liste der AWS Konten, für die Sie die Standardantwort für AMS-Konfigurationsregeln geändert haben.
- Die Liste der Tags, denen Sie eine Antwort für AMS-Konfigurationsregeln zugeordnet haben.
- Die Liste der Antwortkonfigurationen für jede Regel, jedes Konto und jedes Tag.
- Die Liste der Ressourcen, für die Sie die Standardantwort für AMS-Konfigurationsregeln geändert haben.

Bericht über die neuesten Antwortkonfigurationen

field	Beschreibung
Datum	Datum, an dem der Bericht erstellt wurde
Kundenname	Kundenname
AWS Konto-ID	Die der Konfiguration zugeordnete AWS Konto-ID
Kontoname	AWS Kontoname der Ressourcengruppe auf Kontoebene
Typ wird gesucht	Art des identifizierten Befundes. In diesem Fall AWS Config
Quellen-ID	AWS Config Eindeutiger Quellen-Identifier der Regel

field	Beschreibung
Ressourcengruppen-ID	Die Ressourcengruppen-ID, die der Antwortkonfiguration zugeordnet ist
Antwortaktion konfiguriert	Von AMS ausgelöster Aktionstyp
Mit SSM Runbook verknüpft	Das Remediation Runbook, das ausgeführt wird, falls vorhanden
Typ der Ressourcengruppe	Dies kann ein Konto oder ein Tag sein

Ressourcen mit benutzerdefinierter Standardantwort auf Konfigurationsregeln

Name des Felds	Definition
Name des Kunden	Kundenname
Datum	Datum, an dem der Bericht generiert wurde
AWS Kontoname	AWS Kontoname
Konto-ID	Zugeordnete AWS Konto-ID
AMS-Konfigurationsregel	AMS-Konfigurationsregel, die auf die Ressource abzielt und mit einer Konfiguration angewendet wird
Ressourcen-ID	Die Ressourcen-ID im Kundenkonto, auf das die AMS-Konfigurationsregel abzielt
Region der Ressource	Die AWS Region, in der die Konfiguration angewendet wird
Ressourcentyp	AWS Ressourcentyp
Ressourcengruppen-ID	Die Ressourcengruppen-ID, die der Antwortkonfiguration zugeordnet ist

Name des Felds	Definition
AMS-Flagge der Ressource	Wenn die AWS Ressource von AMS bereitgestellt wird, ist dieses Feld auf gesetzt `True`
Typ des Auslösers	Die Art der für die Ressource konfigurierten Antwort
Konformitätskennzeichnung	Konformitätsstatus der AMS-Konfigurationsregel

Berichte von Top Talkers zur Vermeidung von Vorfällen und Überwachung

Verfügbare Berichte

- Bericht über verhinderte Vorfälle
- Bericht „Monitoring Top Talkers“

Bericht über verhinderte Vorfälle

Der Bericht über verhinderte Vorfälle listet die CloudWatch Amazon-Alarme auf, die automatisch behoben wurden, wodurch ein möglicher Vorfall verhindert wurde. Weitere Informationen finden Sie unter Automatische Problembehebung. In der folgenden Tabelle sind die in diesem Bericht enthaltenen Informationen aufgeführt:

Name des Felds	Definition
execution_start_time_utc	Datum, an dem die Automatisierung ausgeführt wurde
Kundenname	Kundenname des Kontos
Konto_Bezeichnung	Der Name des Kontos
AwsAccountId	Die ID des AWS-Kontos
Dokumentname	Der Name des ausgeführten SSM-Dokuments oder der ausgeführten Automatisierung

Name des Felds	Definition
Dauer in Minuten	Die Länge der Automatisierung in Minuten
Region	AWS Region, in der sich die Ressource befindet
automation_execution_id	Die ID der Ausführung
automation_execution_status	Der Status der Ausführung

Bericht „Monitoring Top Talkers“

Der Bericht Monitoring Top Talkers zeigt die Anzahl der CloudWatch Amazon-Alerts, die in einem bestimmten Zeitraum generiert wurden, und bietet Visualisierungen der Ressourcen, die die meisten Alerts generieren. Dieser Bericht hilft Ihnen dabei, Ressourcen zu identifizieren, die die meisten Alerts generieren. Diese Ressourcen eignen sich möglicherweise für die Durchführung einer Ursachenanalyse zur Behebung des Problems oder zur Änderung der Alarmschwellenwerte, um unnötige Auslöser zu verhindern, wenn kein echtes Problem vorliegt. In der folgenden Tabelle sind die in diesem Bericht enthaltenen Informationen aufgeführt:

Name des Felds	Definition
Kundenname	Name des Kunden
AccountId	Die ID des AWS Kontos
Kategorie der Warnung	Die Art der ausgelösten Warnung
Beschreibung	Beschreibung der Warnung
Ressourcen-ID	ID der Ressource, die die Warnung ausgelöst hat
Ressourcenname	Name der Ressource, die die Warnung ausgelöst hat
Region	AWS Region, in der sich die Ressource befindet

Name des Felds	Definition
Status des Vorfalls	Aktueller Status des durch den Alarm ausgelöst en Vorfalls
Erstes Auftreten	Das erste Mal, dass die Warnung ausgelöst wurde
Jüngstes Ereignis	Der letzte Zeitpunkt, zu dem die Warnung ausgelöst wurde
Anzahl der Alarme	Anzahl der Alarme, die zwischen dem ersten und dem letzten Ereignis generiert wurden

Bericht „Einzelheiten zu Abrechnungsgebühren“

Der Bericht mit den Einzelheiten zu den Rechnungsgebühren von AWS Managed Services (AMS) enthält Einzelheiten zu den AMS-Abrechnungsgebühren mit verknüpften Konten und den jeweiligen AWS-Services, darunter:

- Gebühren auf AMS-Serviceebene, Prozentsätze zur Erhöhung der Gebühren, AMS-Servicestufen auf Kontoebene und AMS-Gebühren.
- Verknüpfte Konten und Nutzungsgebühren AWS

Name des Felds	Definition
Monat der Abrechnung	Der Monat und das Jahr, in dem der Service in Rechnung gestellt wurde
Konto-ID des Zahlers	Die 12-stellige ID, die das Konto identifiz iert, das für die Zahlung der AMS-Gebühren verantwortlich ist
ID des verknüpften Kontos	Die 12-stellige ID, die das AMS-Konto identifiz iert, das Dienste in Anspruch nimmt, die Kosten verursachen

Name des Felds	Definition
AWS Name des Dienstes	Der AWS Dienst, der verwendet wurde
AWS Gebühren	Die AWS Gebühren für den AWS unter Dienstname aufgeführten AWS Dienstnamen
Preisplan	Der Name des Preisplans, der mit dem verknüpften Konto verknüpft ist
Proportion erhöhen	Der Uplift-Prozentsatz (als Dezimalzahl V.WXYZ) basierend auf pricing_plan, SLA und AWS-Service
Angepasste Gebühren AWS	AWS Nutzung angepasst an AMS
Erhöhte AWS-Gebühren	Der Prozentsatz der AWS-Gebühren, die für AMS berechnet werden sollen; adjusted_ aws_charges * uplift_percent
EC2 Instances, die RDS ausgeben	Ausgaben für EC2 und RDS-Instances
AMS-Gebühren	AMS-Gebühren insgesamt für das Produkt; uplifted_aws_charges + instance_ec2_rds_s pend + uplifted_ris + uplifted_sp
Anteilige Mindestgebühr	Der Betrag, den wir berechnen, um den vertraglichen Mindestbetrag zu erreichen
Mindestgebühr	AMS-Mindestgebühren (falls zutreffend)
Gesamtbetrag der AMS-Gebühren für verknüpft e Konten	Summe aller Gebühren für das linked_account
AMS-Gebühren für das Konto des Zahlers	Summe aller Gebühren für das Konto des Zahlers

Trusted Remediator-Berichte

Verfügbare Berichte

- Bericht „Trusted Remediator Remediation — Zusammenfassung“
- Bericht mit der Zusammenfassung der Trusted Remediator-Konfiguration
- Trusted Advisor Überprüfen Sie den zusammenfassenden Bericht

Bericht „Trusted Remediator Remediation — Zusammenfassung“

Der Bericht „Trusted Remediator Remediation Status“ enthält Informationen zu den Behebungen, die während früherer Behebungszyklen durchgeführt wurden. Die Standardanzahl von Wochen ist 1. Um den Bericht anzupassen, geben Sie die Anzahl der Wochen auf der Grundlage Ihres Behebungszeitplans an.

Name des Felds	Definition
Datum	Das Datum, an dem die Daten gesammelt wurden.
Konto-ID	Die AWS Konto-ID, zu der die Ressource gehört
Kontoname	Der AWS Kontoname
Überprüfen Sie die Kategorie	Die AWS Trusted Advisor Scheck-Kategorie
Überprüfen Sie den Namen	Der Name der behobenen Prüfung Trusted Advisor
Prüf-ID	Die ID des korrigierten Schecks Trusted Advisor
Ausführungsmodus	Der Ausführungsmodus, der für die spezifische Trusted Advisor Prüfung konfiguriert wurde
OpsItem ID	Die ID der Datei, die von Trusted Advisor für die Behebung OpsItem erstellt wurde

Name des Felds	Definition
OpsItem Status	Der Status von „ OpsItem Erstellt von“ zum Trusted Advisor Zeitpunkt der Meldung
Ressourcen-ID	Der ARN der Ressource, die für die Problembehebung erstellt wurde

Bericht mit der Zusammenfassung der Trusted Remediator-Konfiguration

Der Bericht mit der Zusammenfassung der Trusted Remediator-Konfiguration enthält Informationen zu den aktuellen Trusted Remediator-Wiederherstellungskonfigurationen für jede Prüfung. Trusted Advisor

Name des Felds	Definition
Datum	Das Datum, an dem die Daten gesammelt wurden.
Konto-ID	Die AWS Konto-ID, für die die Konfiguration gilt
Kontoname	Der AWS Kontoname
Überprüfen Sie die Kategorie	Die AWS Trusted Advisor Scheck-Kategorie
Überprüfen Sie den Namen	Der Name der behebten Trusted Advisor Prüfung, für die die Konfiguration gilt
Prüf-ID	Die ID der standardisierten Trusted Advisor Prüfung, für die die Konfiguration gilt
Ausführungsmodus	Der Ausführungsmodus, der für die spezifische Trusted Advisor Prüfung konfiguriert wurde
Auf Automatisiert überschreiben	Das Tag-Muster, falls konfiguriert, um den Ausführungsmodus auf Automatisiert zu überschreiben

Name des Felds	Definition
Auf Manuell überschreiben	Das Tag-Muster, falls konfiguriert, um den Ausführungsmodus auf Manuell zu überschre iben

Trusted Advisor Überprüfen Sie den zusammenfassenden Bericht

Der Bericht „Zusammenfassung der Trusted Advisor Schecks“ enthält Informationen zu den aktuellen Trusted Advisor Prüfungen. In diesem Bericht werden Daten nach jedem wöchentlichen Behebungsplan gesammelt. Die Standardanzahl von Wochen ist 1. Um den Bericht anzupassen, geben Sie die Anzahl der Wochen an, die auf Ihrem Behebungszyklus basieren.

Name des Felds	Definition
Datum	Das Datum, an dem die Daten gesammelt wurden.
Konto-ID	Die AWS Konto-ID, für die die Konfiguration gilt
Name des Kunden	Der AWS Kontoname
Überprüfen Sie die Kategorie	Die AWS Trusted Advisor Scheck-Kategorie
Überprüfen Sie den Namen	Der Name der behebten Trusted Advisor Prüfung, für die die Konfiguration gilt
Prüf-ID	Die ID der standardisierten Trusted Advisor Prüfung, für die die Konfiguration gilt
Status	Der Warnungsstatus der Prüfung. Mögliche Status sind ok (grün), Warnung (gelb), Fehler (rot) oder not_available
Markierte Ressourcen	Die Anzahl der AWS Ressourcen, die durch den Scheck gekennzeichnet (aufgelistet) wurden. Trusted Advisor

Name des Felds	Definition
Ignorierte Ressourcen	Die Anzahl der AWS Ressourcen, die ignoriert wurden, Trusted Advisor weil Sie sie als unterdrückt markiert haben.
Ressourcen im kritischen Zustand	Die Anzahl der Ressourcen im kritischen Zustand
Ressourcen im Warnstatus	Die Anzahl der Ressourcen im Warnstatus

Self-Service-Berichte

Die Self-Service-Berichte (SSR) von AWS Managed Services (AMS) sind eine Funktion, die Daten von verschiedenen systemeigenen AWS Services sammelt und Zugriff auf Berichte zu wichtigen AMS-Angeboten bietet. SSR bietet Informationen, die Sie zur Unterstützung von Betrieb, Konfigurationsmanagement, Bestandsmanagement, Sicherheitsmanagement und Compliance verwenden können.

Verwenden Sie SSR, um über die AMS-Konsole auf die Berichte und Berichtsdatensätze über Amazon S3 S3-Buckets (ein Bucket pro Konto) zuzugreifen. Sie können die Daten in Ihr bevorzugtes Business Intelligence (BI) -Tool einbinden, um die Berichte an Ihre individuellen Bedürfnisse anzupassen. AMS erstellt diesen S3-Bucket (S3-Bucket-Name: (ams-reporting-data-a<Account_ID>) in Ihrer primären AWS Region, und die Daten werden von der AMS-Steuerebene gemeinsam genutzt, die in der Region us-east-1 gehostet wird.

Damit Ihre Benutzer AMS Accelerate-Berichte in der AMS-Konsole einsehen können, müssen Sie in AWS Identity and Access Management (IAM) explizite Berechtigungen zur Ausführung dieser Aktionen gewähren. Beispiele für IAM-Richtlinien finden Sie unter Berechtigungen zur Nutzung von AMS-Funktionen.

> **Important**
>
> Verwenden von benutzerdefinierten Schlüsseln mit AWS Glue
> Um Ihre AWS Glue Metadaten mit einem vom Kunden verwalteten KMS-Schlüssel zu verschlüsseln, müssen Sie die folgenden zusätzlichen Schritte ausführen, damit AMS Daten aus dem Konto aggregieren kann:

1. Öffnen Sie die AWS Key Management Service Konsole unter https://console.aws.amazon.com/kms und wählen Sie dann Customer Managed Keys aus.
2. Wählen Sie die Schlüssel-ID aus, die Sie zur Verschlüsselung der AWS Glue Metadaten verwenden möchten.
3. Wählen Sie die Registerkarte Aliase und dann Alias erstellen aus.
4. Geben Sie AmsReportingFlywheelCustomKeyin das Textfeld ein und wählen Sie dann Alias erstellen aus.

Themen

Interne API-Operationen

Wenn Sie API-Operationen überwachen, werden Ihnen möglicherweise Aufrufe der folgenden rein internen Operationen angezeigt:

- `GetDashboardUrl`
- `ListReportsV2`

Interner API-Vorgang: GetDashboardUrl

Dieser Vorgang erscheint in den Systemprotokollen, wenn er von der AMS-Konsole aufgerufen wird. Es gibt keinen anderen Anwendungsfall. Es ist nicht für Ihren direkten Gebrauch verfügbar.

Gibt die eingebettete Dashboard-URL für den entsprechenden Bericht zurück. Dieser Vorgang akzeptiert einen `dashboardName` zurückgegebenen Wert von`ListReports`.

Erforderliche Syntax

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
}
```

Elemente anfordern

`dashboardName`: Der Name des QuickSight Dashboards, für das die URL angefordert wird. Der Dashboard-Name wird in ListReports V2 zurückgegeben.

Typ: Zeichenfolge

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück. Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

`url`: Gibt die QuickSight URL für die angeforderte URL zurück`dashboardName`.

Typ: Zeichenfolge

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unter Häufige Fehler.

`BadRequestException`:

Die eingereichte Anfrage ist nicht gültig. Zum Beispiel, wenn die Eingabe unvollständig oder falsch ist. Einzelheiten finden Sie in der beigefügten Fehlermeldung.

HTTP Status Code: 400

`NotFoundException`:

Die angeforderte Ressource wurde nicht gefunden. Stellen Sie sicher, dass der Anfrage-URI korrekt ist.

HTTP Status Code: 404

`TooManyRequestsException`:

Die Anfrage hat ihr Drosselungslimit erreicht. Versuchen Sie es nach dem angegebenen Zeitraum erneut.

HTTP-Statuscode: 429

`UnauthorizedException`:

Die Anfrage wurde abgelehnt, da der Anrufer nicht über ausreichende Berechtigungen verfügt.

HTTP-Statuscode: 401

Interner API-Betrieb: ListReports V2

Diese API erscheint in den Systemprotokollen, wenn sie von der AMS-Konsole aufgerufen wird. Sie hat keinen anderen Anwendungsfall. Es ist nicht für Ihren direkten Gebrauch verfügbar.

Gibt eine Liste von Betriebsberichten zurück, die für ein bestimmtes Konto verfügbar sind.

Erforderliche Syntax

Die Anfrage hat keinen Anfragetext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
```

```
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück. Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

`reportsList`: Die Liste der verfügbaren Betriebsberichte.

Typ: Anordnung von Dashboard-Objekten

`reportsType`: Gibt an, ob ein Bericht für mehrere Konten aggregiert ist oder nicht.

Typ: Zeichenfolge

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unter Häufige Fehler.

`BadRequestException`:

Die eingereichte Anfrage ist nicht gültig. Beispielsweise ist die Eingabe unvollständig oder falsch. Einzelheiten finden Sie in der beigefügten Fehlermeldung.

HTTP Status Code: 400

`NotFoundException`:

Die angeforderte Ressource wurde nicht gefunden. Stellen Sie sicher, dass der Anfrage-URI korrekt ist.

HTTP Status Code: 404

`TooManyRequestsException`:

Die Anfrage hat ihr Drosselungslimit erreicht. Versuchen Sie es nach dem angegebenen Zeitraum erneut.

HTTP-Statuscode: 429

`UnauthorizedException`:

Die Anfrage wurde abgelehnt, da der Anrufer nicht über ausreichende Berechtigungen verfügt.

HTTP-Statuscode: 401

Patch-Bericht (täglich)

Verfügbare Berichte

- Zusammenfassung der Instanzdetails für AMS-Patching
- Einzelheiten zum Patch
- Instanzen, bei denen Patches ausgelassen wurden

Zusammenfassung der Instanzdetails für AMS-Patching

Dies ist ein informativer Bericht, anhand dessen alle in AMS Patching integrierten Instances, Kontostatus, Instanzdetails, Umfang des Wartungsfensters, Ausführungszeit des Wartungsfensters, Stack-Details und Plattformtyp identifiziert werden können.

Dieser Datensatz bietet:

- Daten zu den Produktions- und Nichtproduktionsinstanzen eines Kontos. Die Produktions- und Nichtproduktionsphase wird vom Kontonamen und nicht von den Instanz-Tags abgeleitet.
- Daten zur Verteilung der Instanzen nach Plattformtyp. Der Plattformtyp „N/A“ tritt auf, wenn AWS Systems Manager (SSM) die Plattforminformationen nicht abrufen kann.
- Daten zur Verteilung des Status der Instanzen, zur Anzahl der laufenden, angehaltenen oder beendeten Instanzen.

Name des Konsolenfeldes	Feldname des Datensatzes	Definition
Zugriffsbeschränkungen	access_restrictions	Regionen, auf die der Zugriff beschränkt ist
Konto-ID	aws_account_id	AWS Konto-ID, zu der die Instanz-ID gehört
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Kontoname	Konto_Bezeichnung	AWS Kontoname

Name des Konsolenfeldes	Feldname des Datensatzes	Definition
Status des Kontos	account_status	AMS-Kontostatus
	account_sla	Verpflichtung zum AMS-Konto service
Kontotyp	malz_role	MALZ-Rolle
Name der Auto-Scaling-Gruppe	instanz_asg_name	Name der Auto Scaling Group (ASG), die die Instance enthält
Instanz-ID	instance_id	ID der EC2 Instanz
Instance-Name	Instanzname	Name der Instanz EC2
Instanz-Patch-Gruppe	instance_patch_group	Name der Patch-Gruppe, die verwendet wird, um Instanzen zu gruppieren und dasselbe Wartungsfenster anzuwenden
Typ der Instanz-Patchgruppe	instance_patch_group_type	Typ der Patch-Gruppe
Plattformtyp der Instanz	instance_platform_type	Typ des Betriebssystems (OS)
Name der Instanzplattform	instance_platform_name	Name des Betriebssystems (OS)
Instance-Status	instance_state	Status innerhalb des Instanzlebenszyklus EC2
Instanz-Tags	ec2_tags	Die mit der EC2 Amazon-Instance-ID verknüpften Tags
Landezone	malz_flag	Flagge für ein Konto im Zusammenhang mit Malz

Name des Konsolenfeldes	Feldname des Datensatzes	Definition
Geltungsbereich des Wartungsfensters	mw_covered_flag	Wenn für eine Instanz mindestens ein Wartungsfenster mit einem future Ausführungsdatum aktiviert ist, gilt sie als abgedeckt, andernfalls als nicht abgedeckt
Wartungsfenster, Ausführungsdatum/Uhrzeit	früheste_window_execution_time	Das nächste Mal wird das Wartungsfenster voraussichtlich ausgeführt
Wartungsfenster, Ausführung, Datum/Uhrzeit	früheste_window_execution_time	Das nächste Mal wird das Wartungsfenster voraussichtlich ausgeführt
Produktionskonto	prod_account	Kennung der AMS-Prod- und Nicht-Prod-Konten, abhängig davon, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält.
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Stack-Name	instance_stack_name	Name des Stacks, der die Instanz enthält
Typ des Stapels	instance_stack_type	AMS-Stack (AMS-Infrastruktur innerhalb des Kundenkontos) oder Kunden-Stack (AMS-verwaltete Infrastruktur, die Kundenanwendungen unterstützt)

Einzelheiten zum Patch

Dieser Bericht enthält Patch-Details und deckt das Wartungsfenster für verschiedene Instanzen ab.

Dieser Bericht enthält:

- Daten zu Patchgruppen und ihren Typen.
- Daten zu Wartungsfenstern, Dauer, Stichtag, future Daten der Ausführung von Wartungsfenstern (Zeitplan) und betroffenen Instanzen in jedem Fenster.
- Daten zu allen Betriebssystemen unter dem Konto und Anzahl der Instanzen, auf denen das Betriebssystem installiert ist.

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Konto-ID	aws_account_id	AWS Konto-ID, zu der die Instanz-ID gehört
Kontoname	Konto_Bezeichnung	AWS Kontoname
Kontostatus	account_status	AMS-Kontostatus
Konform — Kritisch	compliant_critical	Anzahl der kompatiblen Patches mit dem Schweregrad „kritisch“
Konform — Hoch	compliant_high	Anzahl der kompatiblen Patches mit dem Schweregrad „hoch“
Konform — Mittel	compliant_medium	Anzahl der kompatiblen Patches mit dem Schweregrad „mittel“

Name des Felds	Feldname des Datensatzes	Definition
Konform — Niedrig	compliant_low	Anzahl der kompatiblen Patches mit dem Schweregrad „niedrig“
Konform — informativ	compliant_informational	Anzahl der kompatiblen Patches mit dem Schweregrad „informativ“
Konform — Nicht spezifiziert	compliant_nicht spezifiziert	Anzahl der kompatiblen Patches mit dem Schweregrad „nicht spezifiziert“
Konform — Insgesamt	compliant_total	Anzahl der kompatiblen Patches (alle Schweregrade)
Instanz-ID	instance_id	ID der EC2 Instanz
Instance-Name	Instanzname	Name der Instanz EC2
	account_sla	Dienststufe für AMS-Konten
Plattformtyp der Instanz	instance_platform_type	Typ des Betriebssystems (OS)
Name der Instanzplattform	instance_platform_name	Name des Betriebssystems (OS)

Name des Felds	Feldname des Datensatzes	Definition
Typ der Instanz-Patchgruppe	instance_patch_group_type	DEFAULT: Standard-Patchgruppe mit standardmäßigem Wartungsfenster, bestimmt durch das Tag:TRUE auf der Instanz AMSDefault PatchGroup KUNDE: Der Kunde hat die Patchgruppe erstellt NOT_ASSIGNED: Keine Patch-Gruppe zugewiesen
Instanz-Patch-Gruppe	instance_patch_group	Name der Patch-Gruppe, die verwendet wird, um Instanzen zu gruppieren und dasselbe Wartungsfenster anzuwenden
Instance-Status	instance_state	Status innerhalb des Instanzlebenszyklus EC2
Instanz-Tags	ec2_tags	Die mit der EC2 Amazon-Instance-ID verknüpften Tags
Wartungsfenster für die letzte Ausführung	last_execution_window	Der letzte Zeitpunkt, zu dem das Wartungsfenster ausgeführt wurde
ID des Wartungsfensters	Fenster-ID	Wartungsfenster-ID
Status des Wartungsfensters	window_state	Status des Wartungsfensters
Typ des Wartungsfensters	Fenstertyp	Typ des Wartungsfensters
Wartungsfenster: Datum und Uhrzeit der nächsten Ausführung	window_next execution_time	Beim nächsten Mal wird das Wartungsfenster voraussichtlich ausgeführt

Name des Felds	Feldname des Datensatzes	Definition
Dauer des Wartungsfensters (Stunden)	Dauer des Fensters	Die Dauer des Wartungsfensters in Stunden
Geltungsbereich des Wartungsfensters	mw_covered_flag	Wenn für eine Instanz mindestens ein Wartungsfenster mit einem future Ausführungsdatum aktiviert ist, gilt sie als abgedeckt , andernfalls als nicht abgedeckt
Nicht konform — Kritisch	noncompliant_critical	Anzahl der nicht konformen Patches mit dem Schweregrad „kritisch“
Nicht konform — Hoch	noncompliant_high	Anzahl der nicht konformen Patches mit dem Schweregrad „hoch“
Nicht konform — Mittel	noncompliant_medium	Anzahl der nicht konformen Patches mit dem Schweregrad „mittel“
Nicht konform — Niedrig	noncompliant_low	Anzahl der nicht konformen Patches mit dem Schweregrad „niedrig“
Nicht konform — Informativ	nicht konform _informativ	Anzahl der nicht konformen Patches mit dem Schweregrad „informativ“
Nicht konform — Nicht spezifiziert	nicht konform _nicht spezifiziert	Anzahl der nicht konformen Patches mit dem Schweregrad „nicht spezifiziert“
Nicht konform — Insgesamt	noncompliant_total	Anzahl der nicht konformen Patches (alle Schweregrade)

Name des Felds	Feldname des Datensatzes	Definition
Patch-Baseline-ID	Patch_Baseline_ID	Die Patch-Baseline ist derzeit an die Instanz angehängt
Patch-Status	Status des Patches	Allgemeiner Status der Patch-Konformität. Fehlt mindestens ein Patch, gilt die Instanz als nicht konform, andernfalls als konform.
Produktionskonto	prod_account	Kennung der AMS-Prod- und Nicht-Prod-Konten, abhängig davon, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält.
Typ des Stapels	instance_stack_type	AMS-Stack (AMS-Infrastruktur innerhalb des Kundenkontos) oder Kunden-Stack (AMS-verwaltete Infrastruktur, die Kundenanwendungen unterstützt)
	window_next_exec_yyyy	Jahr als Teil von window_next_execution_time
	window_next_exec_mm	Teil des Monats window_next_execution_time
	Window_Next_Exec_D	Teil des Tages von window_next_execution_time
	window_next _exec_HHMI	Stunde:Minute Teil von window_next_execution_time

Instanzen, bei denen Patches ausgelassen wurden

Dieser Bericht enthält Einzelheiten zu Instanzen, bei denen während der Ausführung des letzten Wartungsfensters Patches verpasst wurden.

Dieser Bericht enthält:

- Daten zu fehlenden Patches auf Patch-ID-Ebene.
- Daten zu allen Instances, bei denen mindestens ein Patch fehlt, und Attribute wie Schweregrad des Patches, Tage ohne Patches, Bereich und Veröffentlichungsdatum des Patches.

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung
Konto-ID	aws_account_id	AWS Konto-ID, zu der die Instanz-ID gehört
Kontoname	Konto_Bezeichnung	AWS Kontoname
Kundenname Elternteil	Kundenname_Elternteil	
Name des Kunden	Kundenname	
Produktionskonto	prod_account	Bezeichner der AMS-Prod- oder Non-Prod-Konten, je nachdem, ob der Kontoname den Wert „PROD“ oder „NONPROD“ enthält.
Status des Kontos	account_status	AMS-Kontostatus
Kontotyp	Kontotyp	
	account_sla	Dienststufe für AMS-Konten
Instanz-ID	instance_id	ID deiner EC2 Instanz

Name des Felds	Feldname des Datensatzes	Definition
Instance-Name	Instanzname	Name Ihrer Instanz EC2
Plattformtyp der Instanz	instance_platform_type	Typ des Betriebssystems (OS)
Instance-Status	instance_state	Status innerhalb des Instanzlebenszyklus EC2
Instanz-Tags	ec2_tags	Die mit der EC2 Amazon-Instance-ID verknüpften Tags
Patch-ID	Patch-ID	ID des veröffentlichten Patches
Schweregrad des Patch	patch_sev	Schweregrad des Patches pro Herausgeber
Patch-Klassifizierung	patch_class	Klassifizierung der Patches nach dem Patch-Herausgeber
Datum und Uhrzeit der Patch-Veröffentlichung (UTC)	release_dt_utc	Veröffentlichungsdatum des Patches pro Herausgeber
Status der Patch-Installation	Installationsstatus	Installieren Sie den Status des Patches auf der Instanz pro SSM
Tage ohne Patches	days_ungepatched	Anzahl der Tage, an denen die Instanz seit dem letzten SSM-Scan nicht gepatcht wurde
Zeitraum für Tage ohne Patches	days_unpatched_bucket	Ungepatchte Tage

Backup-Bericht (täglich)

Der Backup-Bericht deckt primäre und sekundäre (falls zutreffend) Regionen ab. Er deckt den Status der Backups (Erfolg/Fehlschlag) und Daten zu den erstellten Snapshots ab.

Dieser Bericht enthält:

- Status des Backup
- Anzahl der aufgenommenen Schnappschüsse
- Wiederherstellungspunkt
- Backup-Plan und Tresorinformationen

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Konto-ID	aws_account_id	AWS-Konto-ID, zu der die Instance-ID gehört
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Kontoname	Konto_Bezeichnung	AWS-Kontoname
Konto-SLA	account_sla	Verpflichtung zum AMS-Konto service
	malz_flag	Flagge für ein Konto im Zusammenhang mit Malz
	malz_role	MALZ-Rolle
	Zugangsbeschränkungen	Regionen, auf die der Zugriff beschränkt ist
Startdatum und Uhrzeit des geplanten Backup-Snapshots	start_by_dt_utc	Zeitstempel, zu dem der Start des Snapshots geplant ist

Name des Felds	Feldname des Datensatzes	Definition
Aktuelles Startdatum und Uhrzeit des Backup-Snapshots	creation_dt_utc	Zeitstempel, zu dem der Snapshot tatsächlich beginnt
Datum und Uhrzeit der Fertigstellung des Backup-Snapshots	completion_dt_utc	Zeitstempel, wenn der Snapshot abgeschlossen ist
Ablaufdatum/Uhrzeit des Backup-Snapshots	expiration_dt_utc	Zeitstempel, wenn der Snapshot abläuft
Status des Backup-Jobs	backup_job_status	Status des Snapshots
Art des Backup	Sicherungstyp	Art der Sicherung
ID des Backup-Auftrags	Backup_Job-ID	Die eindeutige Kennung des Backup-Jobs
Backup-Größe in Byte	backup_size_in_bytes	Die Backup-Größe in Byte
Backup-Plan ARN	backup_plan_arn	Der Backup-Plan ARN
ID des Backup-Plans	backup_plan_id	Eindeutige Kennung des Backup-Plans
Name des Sicherungsplans	backup_plan_name	Der Name des Backup-Plans
Version des Backup-Plans	backup_plan_version	Die Version des Backup-Plans
ID der Backup-Regel	backup_rule_id	Die ID der Backup-Regel
Backup-Tresor-ARN	backup_vault_arn	Backup-Tresor-ARN
Name des Sicherungstresors	Name des Backup-Tresors	Der Name des Backup-Tresors
IAM-Rolle ARN	iam_role_arn	Die IAM-Rolle ARN
Instanz-ID	instance_id	Eindeutige Instanz-ID

Name des Felds	Feldname des Datensatzes	Definition
Instance-Status	instance_state	Instance-Status
Instanz-Tags	ec2_tags	Die mit der Instanz-ID verknüpften EC2 Tags
ARN-Ressourcen	resource_arn	Der Name der Amazon-Ressource
Ressourcen-ID	resource_id	Die eindeutige Ressourcen-ID
Region der Ressource	resource_region	Die primären (und gegebenen falls sekundären) Regionen der Ressource.
Ressourcentyp	resource_type	Der Typ der Ressource
ARN für den Wiederherstellungspunkt	recovery_point_arn	Der ARN des Wiederherstellungspunkts
ID des Wiederherstellungspunkts	Wiederherstellungspunkt-ID	Die eindeutige Kennung des Wiederherstellungspunkts
Status des Wiederherstellungspunkts	recovery_point_status	Status des Wiederherstellungspunkts
Löschen des Wiederherstellungspunkts nach Tagen	recovery_point_delete_after_days	Löschen des Wiederherstellungspunkts nach Tagen
Der Erholungspunkt wird nach Tagen in den Kühlraum verschoben	recovery_point_move_to_cold_storage_after_days	Anzahl der Tage nach dem Fertigstellungsdatum, an denen der Backup-Snapshot in den Cold Storage verschoben wird
Verschlüsselungsstatus des Wiederherstellungspunkts	recovery_point_is_encrypted	Verschlüsselungsstatus des Wiederherstellungspunkts

Name des Felds	Feldname des Datensatzes	Definition
ARN für den Wiederherstellungspunkt-Verschlüsselungsschlüssel	recovery_point_encryption_key_arn	Verschlüsselungsschlüssel ARN für den Wiederherstellungspunkt
Stapel-ID	stack_id	Eindeutige Kennung für den Cloudformation-Stack
Stack-Name	stack_name	Stack-Name
Schlagwort: AMS-Standard-Patchgruppe	tag_ams_default_patch_group	Tag-Wert: AMS-Standard-Patchgruppe
Schlagwort: App-ID	tag_app_id	Tag-Wert: App-ID
Schlagwort: App-Name	tag_app_name	Tag-Wert: App-Name
Schlagwort: Backup	tag_backup	Tagwert: Backup
Schlagwort: Compliance-Framework	tag_compliance_framework	Tag-Wert: Compliance-Framework
Schlagwort: Kostenstelle	tag_cost_center	Tag-Wert: Kostenstelle
Schlagwort: Kunde	tag_customer	Tag-Wert: Kunde
Schlagwort: Datenklassifizierung	tag_data_classification	Tag-Wert: Datenklassifizierung
Tag: Umgebungstyp	tag_environment_type	Tag-Wert: Umgebungstyp
Tag: Öffnungszeiten	tag_hours_of_operation	Tag-Wert: Betriebsstunden
Schlagwort: Besitzerteam	tag_owner_team	Tag-Wert: Besitzerteam
Schlagwort: E-Mail des Eigentümerteams	tag_owner_team_email	Tag-Wert: E-Mail-Adresse des Eigentümerteams
Schlagwort: Patch-Gruppe	tag_patch_group	Tag-Wert: Patch-Gruppe

Name des Felds	Feldname des Datensatzes	Definition
Schlagwort: Support-Priorität	tag_support_priority	Tag-Wert: Support-Priorität
Status des Volumens	volume_state	Status des Volumens

Zwischenfallbericht (wöchentlich)

Dieser Bericht enthält die aggregierte Liste der Vorfälle zusammen mit ihrer Priorität, ihrem Schweregrad und ihrem aktuellen Status, einschließlich:

- Daten zu Supportfällen, die im verwalteten Konto als Vorfälle eingestuft wurden
- Vorfallinformationen, die zur Visualisierung der Vorfallkennzahlen für das verwaltete Konto erforderlich sind
- Daten zu den Kategorien von Vorfällen und zum Status der Behebung jedes Vorfalls

Sowohl Visualisierungen als auch Daten sind für den wöchentlichen Vorfallbericht verfügbar.

- Auf die Visualisierung kann über die AMS-Konsole im Konto über die Seite Berichte zugegriffen werden.
- Auf den Datensatz mit dem folgenden Schema kann über den S3-Bucket im verwalteten Konto zugegriffen werden.
- Verwenden Sie die bereitgestellten Datumsfelder, um Vorfälle nach Monat, Quartal, Woche oder and/or Tag zu filtern, an dem der Vorfall erstellt oder gelöst wurde.

Name des Felds	Feldname des Datensatzes	Definition
Datum/Uhrzeit melden	dataset_datetime	Das Datum und die Uhrzeit, zu der der Bericht generiert wurde.
Konto-ID	aws_account_id	AWS Konto-ID, zu der der Vorfall gehört.

Name des Felds	Feldname des Datensatzes	Definition
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Kontoname	Konto_Bezeichnung	AWS Kontoname.
Fallnummer	case_id	Die ID des Vorfalls.
Monat der Erstellung	erstellter_Monat	Der Monat, in dem der Vorfall erstellt wurde.
Priorität	priority	Die Priorität des Vorfalls.
Schweregrad	severity	Die Schwere des Vorfalls.
Status	Status	Der Status des Vorfalls.
Kategorie	yuma_category	Die Kategorie des Vorfalls.
Tag der Erstellung	erstellter_Tag	Der Tag, an dem der Vorfall im Format erstellt wurde. YYYY-MM-DD
Woche erstellt	created_wk	Die Woche, in der der Vorfall im Format YYYY-WW erstellt wurde. Sonntag bis Samstag werden als Anfang und Ende einer Woche gezählt. Die Woche dauert von 01 bis 52. Woche 01 ist immer die Woche, die den ersten Tag des Jahres enthält. Beispiels weise befinden sich 2023-12-31 und 2024-01-01 in Woche 2024-01.

Name des Felds	Feldname des Datensatzes	Definition
Quartal erstellt	created_qtr	Das Quartal, in dem der Vorfall im Format YYYY-Q erstellt wurde. 01/01 bis 03/31 sind als Q1 definiert usw.
Tag der Lösung	resolved_day	Der Tag, an dem der Vorfall im Format behoben wurde. YYYY-MM-DD
Gelöste Woche	resolved_wk	Die Woche, in der der Vorfall gelöst wurde, im Format YYYY-WW. Sonntag bis Samstag werden als Anfang und Ende einer Woche gezählt. Die Woche dauert von 01 bis 52. Woche 01 ist immer die Woche, die den ersten Tag des Jahres enthält. Beispiels weise befinden sich 2023-12-3 1 und 2024-01-01 in Woche 2024-01.
Monat, der gelöst wurde	Resolved_month	Der Monat, in dem der Vorfall behoben wurde, im Format YYYY-MM.
Quartal gelöst	resolved_qtr	Das Quartal, in dem der Vorfall gelöst wurde, im Format YYYY-Q. 01/01 bis 03/31 sind als Q1 definiert usw.
Gruppierungsregel wurde erstellt	grouping_rule	Die Gruppierungsregel, die für den Vorfall gilt. Entweder „no_grouping“ oder „instance _grouping“.

Name des Felds	Feldname des Datensatzes	Definition
Instanz IDs	instance_ids	Die mit dem Vorfall verknüpfte Instanz.
Anzahl der Alerts	Anzahl_der_Warnmeldungen	Die Anzahl der Warnmeldungen, die mit diesem Vorfall verknüpft sind. Wenn Sie die Gruppierung aktiviert haben, kann diese Zahl größer als 1 sein. Wenn Sie die Gruppierung nicht aktiviert haben, wird sie immer 1 sein.
Erstellt um	created_at	Der Zeitstempel, zu dem der Vorfall erstellt wurde.
Alarm ARNs	alarm_arns	Der Amazon-Ressourcenname („arn“) der Alarme, die mit Ihrem Vorfall verknüpft sind.
Verwandte Alarme	verwandte Alarme	Die für Menschen lesbaren Namen aller Alarme, die mit dem Vorfall in Verbindung stehen.

Abrechnungsbericht (monatlich)

Einzelheiten zu den Abrechnungsgebühren

Dieser Bericht enthält Einzelheiten zu den AMS-Abrechnungsgebühren für verknüpfte Konten und die jeweiligen AWS-Services.

Dieser Bericht enthält:

- Daten zu AMS-Gebühren auf Serviceniveau, prozentuale Erhöhungsquoten, AMS-Servicestufen auf Kontoebene und AMS-Gebühren.
- Daten zu verknüpften Konten und AWS-Nutzungsgebühren.

> **Important**
>
> Der monatliche Abrechnungsbericht ist nur in Ihrem Management Payer Account (MPA) oder Ihrem definierten Gebührenkonto verfügbar. Dies sind die Konten, an die Ihre monatliche AMS-Rechnung gesendet wird. Wenn Sie diese Konten nicht finden können, wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM), um Unterstützung zu erhalten.

Name des Felds	Feldname des Datensatzes	Definition
Rechnungsdatum	date	Monat und Jahr der abgerechneten Dienstleistung
Konto-ID des Zahlers	payer_account_id	Die 12-stellige ID, die das Konto identifiziert, das für die Zahlung der AMS-Gebühren verantwortlich ist
ID des verknüpften Kontos	linked_account_id	Die 12-stellige ID, die das AMS-Konto identifiziert, das Dienste in Anspruch nimmt, die zu hohen Kosten führen
AWS Name des Dienstes	product_name	Der AWS Dienst, der verwendet wurde
AWS Gebühren	aws_charges	Die AWS Gebühren für den AWS Dienstnamen in AWS Service Name
Preisplan	Preisplan	Der mit dem verknüpften Konto verknüpfte Preisplan
AMS Service Group	tier_uplifting_groups	Gruppencode für den AMS-Service, der den Prozentsatz der Erhöhung festlegt

Name des Felds	Feldname des Datensatzes	Definition
Verhältnis der Erhöhung	prozentualer Anstieg	Der prozentuale Anstieg (als Dezimalzahl V.WXYZ), basierend auf pricing_plan, SLA und Service AWS
Angepasste Gebühren AWS	adjusted_aws_usage	AWS Nutzung für AMS angepasst
Erhöhte Gebühren AWS	uplifted_aws_charges	Der Prozentsatz der Gebühren, die für AMS berechnet werden müssen AWS ; adjusted_aws_charges * uplift_percent
EC2 Instanzen, die RDS ausgeben	instances_ec2_rds_spend	Ausgaben für und RDS-Insta nces EC2
Gebühren für Reserved Instances	ris_charges	Gebühren für Reserved Instances
Die Gebühren für Reserved Instances wurden angehoben	uplifted_ris	Der Prozentsatz der Reserved Instance-Gebühren, die für AMS berechnet werden müssen; ris_charges * uplift_percent
Gebühren für den Savings Plan	sp_charges	SavingsPlan Nutzungsg ebühren
Erhöhte Sparplangebühren	uplifted_sp	Der Prozentsatz der Sparplangebühren, die für AMS berechnet werden müssen; sp_charges * uplift_percent

Name des Felds	Feldname des Datensatzes	Definition
AMS-Gebühren	ams_charges	Summe der AMS-Gebühren für das Produkt; uplifted_ aws_charges + instance_ ec2_rds_spend + uplifted_ris + uplifted_sp
Anteilige Mindestgebühr	anteiliges Minimum	Der Betrag, den wir berechnen , um den vertraglichen Mindestbetrag zu erreichen
Gesamter AMS-Betrag der Gebühren für verknüpfte Konten	linked_account_total ams_charges	Summe aller Gebühren für den Linked_Account
AMS-Gebühren insgesamt auf dem Konto des Zahlers	payer_account_total ams_charges	Summe aller Gebühren für das Konto des Zahlers
Mindestgebühr	Mindestgebühren	AMS-Mindestgebühren (falls zutreffend)
discount für Reserved Instance und Savings Plan	adj_ri_sp_charges	RI/SP discount to be applied against RI/SPGebühren (unter bestimmten Umständen anwendbar)

Aggregierte Berichte

Aggregierte Self-Service-Berichte (SSR) bieten Ihnen einen Überblick über bestehende Self-Service-Berichte, die auf Unternehmensebene kontenübergreifend aggregiert wurden. Auf diese Weise erhalten Sie Einblick in wichtige Betriebskennzahlen wie Patch-Compliance, Backup-Abdeckung und Vorfälle für alle Konten, die in Ihrem Unternehmen von AMS verwaltet werden. AWS Organizations

Aggregierte SSR ist in allen kommerziellen Bereichen verfügbar, in AWS-Regionen denen AWS Managed Services verfügbar sind. Eine vollständige Liste der verfügbaren Regionen finden Sie in der Regionentabelle.

Aktivieren Sie aggregierte Berichte

Sie müssen aggregiertes SSR von einem Verwaltungskonto aus verwalten. AWS Organizations Das Verwaltungskonto ist das AWS Konto, mit dem Sie Ihre Organisation erstellt haben.

Um Aggregated SSR für ein AWS Organizations Verwaltungskonto zu aktivieren, das in AMS integriert ist, greifen Sie auf Ihre AMS-Konsole zu und navigieren Sie zu Berichte. Wählen Sie in der top-right-hand Ecke Organization Access aus, um den Bereich AWS Managed Services Console: Organization View zu öffnen. In diesem Bereich können Sie die Aggregated SSR-Funktionalität verwalten.

AWS Organizations Verwaltungskonten, die nicht in AMS integriert sind, haben keinen Zugriff auf die AMS-Konsole. Um Aggregated SSR für ein AWS Organizations Verwaltungskonto zu aktivieren, das nicht bei AMS integriert ist, authentifizieren Sie sich zunächst bei Ihrem AWS-Konto, navigieren Sie dann zur AWS Konsole und suchen Sie nach Managed Services. Dadurch wird die AMS-Marketingseite geöffnet. Wählen Sie auf dieser Seite in der Navigationsleiste den Link Organization Access aus, um die AWS Managed Services Services-Konsole zu öffnen: Organization View, in der Sie die Aggregated SSR-Funktionalität verwalten können.

Wenn Sie zum ersten Mal auf die AWS Managed Services Console: Organization View zugreifen, führen Sie die folgenden Schritte aus:

1. Wenn Sie es noch nicht eingerichtet haben AWS Organizations, wählen Sie in Ihrer Konsole die Option Aktivieren AWS Organizations aus. Weitere Informationen zur Einrichtung AWS Organizations finden Sie im AWS Organizations Benutzerhandbuch. Sie können diesen Schritt überspringen, wenn Sie ihn bereits verwenden AWS Organizations.
2. Um den Aggregated Self-Service Reporting Service zu aktivieren, wählen Sie auf der Konsole die Option Vertrauenswürdigen Zugriff aktivieren aus.
3. (Optional) Registrieren Sie einen delegierten Administrator, um Lesezugriff für die Organisationsansicht zu erhalten.

Zeigen Sie als delegierter Administrator aggregierte Berichte an

Ein delegierter Administrator ist das Konto, das Sie für den Lesezugriff auf die aggregierten Berichte auswählen. Der delegierte Administrator muss ein bei AMS registriertes Konto sein und das einzige Konto sein, das Lesezugriff auf aggregierte Berichte hat.

Um einen delegierten Administrator auszuwählen, geben Sie die Konto-ID in Schritt 3 in der AWS Managed Services Console ein: Organization View. Sie können jeweils nur ein delegiertes

Administratorkonto registrieren. Beachten Sie, dass das delegierte Administratorkonto ein von AMS verwaltetes Konto sein muss.

Um ein delegiertes Administratorkonto zu aktualisieren, navigieren Sie zur AWS Managed Services Console: Organization View und wählen Sie Delegierten Administrator entfernen aus. Die Konsole fordert Sie auf, eine neue Konto-ID einzugeben, um sich als delegierter Administrator zu registrieren.

Lesen Sie aggregierte Berichte

Wenn Sie keinen delegierten Administrator registrieren und Ihr AWS Organizations Verwaltungskonto bei AMS angemeldet ist, erhält das AWS Organizations Verwaltungskonto standardmäßig Lesezugriff auf die aggregierten Berichte. Wenn das AWS Organizations Verwaltungskonto nicht von AMS verwaltet wird, müssen Sie ein delegiertes Administratorkonto wählen, um Lesezugriff auf die aggregierten Berichte zu haben.

Zu jedem Zeitpunkt hat nur ein einziges Konto, das bei AMS integriert ist, Lesezugriff auf die aggregierten Berichte, entweder das AWS Organizations Verwaltungskonto oder der registrierte delegierte Administrator. Alle anderen Mitgliedskonten in Ihrer Organisation (und bei AMS integriert) haben weiterhin nur Zugriff auf Einzelkontenberichte für jedes einzelne Konto.

Nachdem Sie Aggregated SSR aktiviert haben, navigieren Sie zu Ihren Berichten. Alle Ihre vorhandenen Self-Service-Berichte werden in diesem Abschnitt aufgeführt, und ein blaues Tag gibt an, dass sie aggregiert wurden. Beachten Sie, dass Sie von dem Konto aus auf die AMS-Konsole zugreifen müssen, das Sie für den Lesezugriff auf die aggregierten Berichte ausgewählt haben. Dies ist entweder das AWS Organizations Verwaltungskonto oder das delegierte Administratorkonto.

Nachdem Sie Aggregated SSR aktiviert haben, sind aggregierte Berichte ab dem nächsten Berichtszyklus verfügbar.

Deaktivieren Sie aggregierte Berichte

Um Aggregated SSR zu deaktivieren, öffnen Sie die AWS Managed Services Console: Organization View. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren aus. Nachdem Sie den vertrauenswürdigen Zugriff für Aggregated SSR deaktiviert haben, werden Ihre AMS-Selfservice-Berichte nicht mehr auf Organisationsebene kontenübergreifend aggregiert. Beachten Sie auch, dass die Deaktivierung ab dem nächsten Berichtszyklus wirksam wird.

Nach der Deaktivierung von Aggregated SSR dauert es eine Wartezeit, bis die Berichte in Ihrer AMS-Konsole als Einzelkonto-Berichte angezeigt werden. Diese Verzögerung ist darauf zurückzuführen, dass die Deaktivierung der Funktion ab dem nächsten Berichtszyklus wirksam wird.

Dashboards für AMS-Selfservice-Berichte

AMS Self-Service Reports bietet zwei Dashboards: und. Resource Tagger-Dashboard Dashboard „Regeln für Sicherheitskonfigurationen“

Resource Tagger-Dashboard

Das AMS Resource Tagger Dashboard bietet detaillierte Informationen zu den Ressourcen, die von Resource Tagger unterstützt werden, sowie zum aktuellen Status der Tags, die Resource Tagger so konfiguriert ist, dass sie auf diese Ressourcen angewendet werden.

Resource Tagger-Abdeckung nach Ressourcentyp

Dieser Datensatz besteht aus einer Liste von Ressourcen, deren Tags von Resource Tagger verwaltet werden.

Die Ressourcenabdeckung nach Ressourcentyp wird in Form von vier Liniendiagrammen visualisiert, die die folgenden Kennzahlen beschreiben:

- Ressourcenanzahl: Die Gesamtzahl der Ressourcen in der Region, aufgeschlüsselt nach Ressourcentyp.
- Ressourcen, denen verwaltete Tags fehlen: Die Gesamtzahl der Ressourcen in der Region, aufgeschlüsselt nach Ressourcentyp, für die verwaltete Tags erforderlich sind, die aber nicht von Resource Tagger markiert wurden.
- Nicht verwaltete Ressourcen: Die Gesamtzahl der Ressourcen in der Region, aufgeschlüsselt nach Ressourcentyp, auf die Resource Tagger keine verwalteten Tags angewendet hat. Dies bedeutet in der Regel, dass diese Ressourcen keiner Resource Tagger-Konfiguration entsprechen oder dass sie ausdrücklich von Konfigurationen ausgeschlossen sind.
- Verwaltete Ressourcen: Gegenstück zur Metrik „Nicht verwaltete Ressourcen“ (Anzahl der Ressourcen — Nicht verwaltete Ressourcen).

In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung (UTC-Zeit)

Feldname	Name des Datensatz-Felds	Definition
AWS-Konto ID	aws_account_id	AWS-Konto AUSWEIS
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Region	Region	AWS-Region
Ressourcentyp	resource_type	Dieses Feld identifiziert den Ressourcentyp. Es sind nur Ressourcentypen enthalten , die von Resource Tagger unterstützt werden.
Anzahl der Ressourcen	resource_count	Anzahl der Ressourcen (des angegebenen Ressource ntyps), die in dieser Region bereitgestellt werden.
ResourcesMissingMa nagedTags	resource_missing_m anaged_tags_count	Anzahl der Ressourcen (des angegebenen Ressource ntyps), für die gemäß den Konfigurationsprofilen verwaltete Tags erforderlich sind, die aber noch nicht von Resource Tagger markiert wurden.

Feldname	Name des Datensatz-Felds	Definition
UnmanagedResources	unmanaged_resource_count	Anzahl der Ressourcen (des angegebenen Ressource ntyps), auf die vom Resource Tagger keine verwalteten Tags angewendet wurden. In der Regel entsprachen diese Ressourcen keinem Resource Tagger-Konfigurati onsblock oder sind ausdrückl ich aus Konfigurationsblöcken ausgeschlossen.

Einhaltung der Resource Tagger-Konfigurationsregeln

Dieser Datensatz besteht aus einer Liste von Ressourcen in einem AWS-Region, sortiert nach Ressourcentyp, auf die ein bestimmtes Konfigurationsprofil angewendet wurde. Es wird als Liniendiagramm visualisiert.

In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung (UTC-Zeit)
AWS-Konto ID	aws_account_id	AWS-Konto AUSWEIS
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Region	Region	AWS-Region
Ressourcentyp	resource_type	Dieses Feld identifiziert den Ressourcentyp. Es sind nur

Feldname	Name des Datensatz-Felds	Definition
		Ressourcentypen enthalten , die von Resource Tagger unterstützt werden.
ID des Konfigurationsprofils	configuration_profile_id	Die ID des Resource Tagger-Konfigurationsprofils. Ein Konfigurationsprofil wird verwendet, um Richtlinien und Regeln zu definieren, die zum Taggen Ihrer Ressourcen verwendet werden.
MatchingResourceCount	resource_count	Anzahl der Ressourcen (des angegebenen Ressource ntyps), die der ID des Resource Tagger-Konfigurati onsprofils entsprechen. Damit eine Ressource dem Konfigurationsprofil entsprich t, muss das Profil aktiviert sein und die Ressource muss der Regel des Profils entsprechen.

Resource Tagger-konforme Ressourcen

Dieser Datensatz besteht aus einer Liste von Ressourcen, die für eine einzelne Resource Tagger-Konfiguration nicht konform sind. Bei diesen Daten handelt es sich um eine tägliche Momentaufnahme der Ressourcen-Compliance. Sie zeigen den Status der Kundenressourcen zum Zeitpunkt der Übermittlung dieser Berichte an die Kundenkonten (es gibt keine historische Ansicht). Es wird als Pivot-Tabelle visualisiert, die aus Ressourcen besteht, die für eine bestimmte Konfiguration nicht konform sind.

In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
Datum/Uhrzeit melden	dataset_datetime	Datum und Uhrzeit der Berichtsgenerierung (UTC-Zeit)
AWS-Konto ID	aws_account_id	AWS-Konto AUSWEIS
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Region	Region	AWS-Region
Ressourcentyp	resource_type	Dieses Feld identifiziert den Ressourcentyp. Es sind nur Ressourcentypen enthalten , die von Resource Tagger unterstützt werden.
Ressourcen-ID	resource_id	Die eindeutige Kennung für Ressourcen, die von Resource Tagger unterstützt werden.
Status der Abdeckung	Deckungsstatus	Dieses Feld gibt an, ob die Ressource anhand der Resource Tagger-Ko nfigurations-ID als konfiguriert gekennzeichnet ist.
ID des Konfigurationsprofils	configuration_profile_id	Die ID des Resource Tagger-Konfigurationsprofils. Ein Konfigurationsprofil wird verwendet, um Richtlinien und Regeln zu definieren, die zum Taggen Ihrer Ressourcen verwendet werden.

Dashboard „Regeln für Sicherheitskonfigurationen“

Das Security Config Rules Dashboard bietet einen detaillierten Einblick in die Ressourcen- und AWS Config Regelkonformität von AMS-Konten. Sie können den Bericht nach dem Schweregrad der Regel filtern, um die wichtigsten Ergebnisse zu priorisieren. In der folgenden Tabelle sind die in diesem Bericht enthaltenen Daten aufgeführt.

Feldname	Name des Datensatz-Felds	Definition
AWS-Konto ID	AWS-Konto AUSWEIS	Die Konto-ID, die mit verwandten Ressourcen verknüpft ist.
Admin-Konto-ID	aws_admin_account_id	Vertrauenswürdiges Konto, das von Ihnen aktiviert wurde. AWS Organizations
Datum/Uhrzeit melden	Datum des Berichts	Datum und Uhrzeit der Berichtsgenerierung.
Kundenname	Name des Kunden	Der Name des Kunden.
Konto_Bezeichnung	Kontoname	Der mit der Konto-ID verknüpfte Name
resource_id	Ressourcen-ID	Ein Bezeichner für eine Ressource.
resource_region	Region der Ressource	Der AWS-Region Ort, an dem sich die Ressource befindet.
resource_type	Ressourcentyp	Der Ressourcentyp AWS-Service oder.
Ressourcenname	Ressourcenname	Der Name der Ressource.
resource_ams_flag	AMS-Flagge der Ressource	Wenn die Ressource im Besitz von AMS ist, ist dieses Flag auf TRUE gesetzt. Wenn sich die Ressource im Besitz des

Feldname	Name des Datensatz-Felds	Definition
		Kunden befindet, ist dieses Flag auf FALSE gesetzt. Wenn der Eigentümer nicht bekannt ist, wird dieses Kennzeichen auf UNKNOWN gesetzt.
config_rule	Konfigurationsregel	Der nicht anpassbare Name für die Konfigurationsregel.
config_rule_description	Beschreibung der Konfigurationsregel	Eine Beschreibung der Konfigurationsregel.
source_identifier	Quellen-ID	Ein eindeutiger Bezeichner für die verwaltete Konfigurationsregel und kein Bezeichner für eine benutzerdefinierte Konfigurationsregel.
compliance_flag	Konformitätskennzeichnung	Zeigt an, ob die Ressourcen den Konfigurationsregeln entsprechen oder nicht.
rule_type	Regeltyp	Gibt an, ob die Regel vordefiniert oder benutzerdefiniert ist.

Feldname	Name des Datensatz-Felds	Definition
exception_flag	Ausnahme-Flag	Das Ausnahmerkennzeichen für Ressourcen zeigt die Risikobereitschaft gegenüber einer Ressource an, die den Vorschriften nicht entspricht. Wenn das Ausnahmerkennzeichen für eine Ressource den Wert TRUE hat, ist die Ressource ausgenommen. Wenn das Ausnahme-Flag NULL ist, ist die Ressource nicht ausgenommen.
cal_dt	Datum	Das Bewertungsdatum der Regel.
Beschreibung der Abhilfemaßnahme	Beschreibung der Problembehebung	Eine Beschreibung, wie die Einhaltung von Regeln behoben werden kann.
severity	Schweregrad	Der Schweregrad der Konfigurationsregel gibt die Auswirkungen einer Nichteinhaltung an.
customer_action	Aktion des Kunden	Maßnahmen, die Sie zur Behebung dieser Regel benötigen.
Empfehlung	Empfehlung	Eine Beschreibung dessen, wonach die Konfigurationsregel sucht.

Feldname	Name des Datensatz-Felds	Definition
remediation_category	Kategorie „Problembehebung“	Die Standardmaßnahmen, die AMS ergreift, wenn diese Regel nicht mehr konform ist.

Datenaufbewahrungsrichtlinie

AMS SSR hat für jeden Bericht eine Richtlinie zur Aufbewahrung von Daten eingeführt. Nach Ablauf des Berichtszeitraums werden die Daten gelöscht und sind nicht mehr verfügbar.

Name des Berichts	SSR-Konsole zur Datenspeicherung	Datenspeicherung SSR S3-Bucket
Zusammenfassung der Instanzdetails für AMS-Patching	2 Monate	2 Jahre
Einzelheiten zum Patch	2 Monate	2 Jahre
Instanzen, bei denen während der Ausführung des Wartungsfensters Patches übersehen wurden	2 Monate	2 Jahre
Einzelheiten zu den AMS-Abrechnungsgebühren	2 Jahre	2 Jahre
Täglicher Backup-Bericht	1 Monat	2 Jahre
Wöchentlicher Zwischenfallbericht	2 Monate	2 Jahre
Dashboard mit Regeln für Sicherheitskonfigurationen	3 Monate	2 Jahre
Resource Tagger-Dashboard	1 Jahr	2 Jahre

Offboard von SSR

Um den SSR-Dienst zu verlassen, erstellen Sie über die AMS-Konsole eine Serviceanfrage (SR). Nachdem Sie die SR eingereicht haben, hilft Ihnen ein Betriebstechniker von AMS bei der Auslagerung von SSR. Geben Sie in der SR den Grund an, aus dem Sie aussteigen möchten.

Um ein Konto auszulagern und die Ressourcen zu bereinigen, erstellen Sie über die AMS-Konsole eine SR. Nachdem Sie die SR eingereicht haben, hilft Ihnen ein AMS Operations Engineer beim Löschen des SSR Amazon S3 S3-Buckets.

Wenn Sie das Board von AMS verlassen, werden Sie automatisch von der AMS SSR-Konsole aus ausgebucht. AMS beendet automatisch das Senden von Daten an Ihr Konto. AMS löscht Ihren SSR S3-Bucket im Rahmen des Offboarding-Prozesses.

Zugriffsverwaltung in AMS Accelerate

Beim Zugriffsmanagement werden Ihre Ressourcen geschützt, indem nur autorisierter und authentifizierter Zugriff gewährt wird. Mit AMS Accelerate sind Sie für die Verwaltung des Zugriffs auf Ihre AWS-Konten und die ihnen zugrunde liegenden Ressourcen verantwortlich, z. B. für Zugriffsverwaltungslösungen, Zugriffsrichtlinien und verwandte Prozesse. Um Sie bei der Verwaltung Ihrer Zugriffslösung zu unterstützen, setzt AMS Accelerate AWS Config Regeln ein, die häufig auftretende IAM-Fehlkonfigurationen erkennen und anschließend Benachrichtigungen zur Behebung bereitstellen. Eine häufige IAM-Fehlkonfiguration besteht darin, dass der Root-Benutzer über Zugriffsschlüssel verfügt. Die `iam-root-access-key-check` Konfigurationsregel prüft, ob der Root-Benutzerzugriffsschlüssel verfügbar und konform ist oder ob der Zugriffsschlüssel nicht existiert. Eine Liste der von AMS bereitgestellten Konfigurationsregeln finden Sie in der AWS Config AMS-Regelbibliothek.

Themen

Erhalten Sie Zugriff auf die Accelerate-Konsole

Wenn Sie Accelerate nutzen, haben Sie automatisch Zugriff auf die Accelerate-Konsole. Sie können auf die Konsole zugreifen, indem Sie in Ihrer AWS-Managementkonsole nach Managed Services suchen. Die Accelerate-Konsole bietet Ihnen einen zusammengefassten Überblick über die Funktionen, die Ihnen Accelerate bietet. Diese Ansicht umfasst einzelne Komponenten, die auf dem Dashboard und den Konfigurationsseiten dargestellt werden.

Berechtigungen zur Nutzung von AMS-Funktionen

Damit Ihre Benutzer AMS Accelerate-Funktionen lesen und konfigurieren können, z. B. den Zugriff auf die AMS-Konsole oder die Konfiguration von Backups, müssen Sie ihren IAM-Rollen explizite Berechtigungen zur Ausführung dieser Aktionen gewähren. Die folgende CloudFormation Vorlage enthält die Richtlinien, die zum Lesen und Konfigurieren der mit AMS verbundenen Dienste

erforderlich sind, sodass Sie sie Ihren IAM-Rollen zuweisen können. Sie sind so konzipiert, dass sie eng an die allgemeinen Aufgabenbereiche in der IT-Branche angepasst sind, wo Administrator- oder Nur-Lese-Berechtigungen erforderlich sind. Wenn Sie Benutzern jedoch unterschiedliche Berechtigungen gewähren müssen, können Sie die Richtlinie bearbeiten, um bestimmte Berechtigungen ein- oder auszuschließen. Zudem können Sie eine eigene benutzerdefinierte Richtlinie erstellen.

Die Vorlage enthält zwei Richtlinien. Die `AMSAccelerateAdminAccess` Richtlinie soll für die Einrichtung und den Betrieb der AMS Accelerate-Komponenten verwendet werden. Diese Richtlinie wird in der Regel von einem IT-Administrator übernommen und gewährt Berechtigungen zur Konfiguration von AMS-Funktionen wie Patching und Backups. Die `AMSAccelerateReadOnly` gewährt die erforderlichen Mindestberechtigungen für die Anzeige von AMS Accelerate-bezogenen Ressourcen.

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies

Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
```

```
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
```

```
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
          ]
        },
        {
          "Sid": "AmsChangeRecordS3WritePolicy",
          "Effect": "Allow",
          "Action": [
            "s3:PutObject",
            "s3:PutObjectLegalHold",
            "s3:PutObjectRetention"

          ],
          "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
          ]
        },
        {
          "Sid": "MaciePolicy",
          "Effect": "Allow",
          "Action": [
            "macie2:GetFindingStatistics"
          ],
          "Resource": "*"
        },
        {
          "Sid": "GuardDutyPolicy",
          "Effect": "Allow",
          "Action": [
            "guardduty:GetFindingsStatistics",
            "guardduty:ListDetectors"
          ],
          "Resource": "*"
        },
        {
          "Sid": "SupportPolicy",
          "Effect": "Allow",
          "Action": "support:*",
          "Resource": "*"
        },
        {
          "Sid": "ConfigPolicy",
          "Effect": "Allow",
          "Action": [
```

```
                "config:Get*",
                "config:Describe*",
                "config:Deliver*",
                "config:List*",
                "config:StartConfigRulesEvaluation"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigReadPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:List*",
                "appconfig:Get*"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:StartDeployment",
                "appconfig:StopDeployment",
                "appconfig:CreateHostedConfigurationVersion",
                "appconfig:ValidateConfiguration"
              ],
              "Resource": [
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
              ]
            },
```

```
            {
              "Sid": "CloudFormationStacksPolicy",
              "Effect": "Allow",
              "Action": [
                "cloudformation:DescribeStacks"
              ],
              "Resource": "*"
            },
            {
              "Sid": "EC2Policy",
              "Action": [
                "ec2:DescribeInstances"
              ],
              "Effect": "Allow",
              "Resource": "*"
            },
            {
              "Sid": "SSMPolicy",
              "Effect": "Allow",
              "Action": [
                "ssm:AddTagsToResource",
                "ssm:CancelCommand",
                "ssm:CancelMaintenanceWindowExecution",
                "ssm:CreateAssociation",
                "ssm:CreateAssociationBatch",
                "ssm:CreateMaintenanceWindow",
                "ssm:CreateOpsItem",
                "ssm:CreatePatchBaseline",
                "ssm:DeleteAssociation",
                "ssm:DeleteMaintenanceWindow",
                "ssm:DeletePatchBaseline",
                "ssm:DeregisterPatchBaselineForPatchGroup",
                "ssm:DeregisterTargetFromMaintenanceWindow",
                "ssm:DeregisterTaskFromMaintenanceWindow",
                "ssm:Describe*",
                "ssm:Get*",
                "ssm:List*",
                "ssm:PutConfigurePackageResult",
                "ssm:RegisterDefaultPatchBaseline",
                "ssm:RegisterPatchBaselineForPatchGroup",
                "ssm:RegisterTargetWithMaintenanceWindow",
                "ssm:RegisterTaskWithMaintenanceWindow",
                "ssm:RemoveTagsFromResource",
                "ssm:SendCommand",
```

```
                "ssm:StartAssociationsOnce",
                "ssm:StartAutomationExecution",
                "ssm:StartSession",
                "ssm:StopAutomationExecution",
                "ssm:TerminateSession",
                "ssm:UpdateAssociation",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateMaintenanceWindow",
                "ssm:UpdateMaintenanceWindowTarget",
                "ssm:UpdateMaintenanceWindowTask",
                "ssm:UpdateOpsItem",
                "ssm:UpdatePatchBaseline"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AmsPatchRestrictAMSResources",
            "Effect": "Deny",
            "Action": [
                "ssm:DeletePatchBaseline",
                "ssm:UpdatePatchBaseline"
            ],
            "Resource": [
                "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/ams:resourceOwner": "*"
                }
            }
        },
        {
            "Sid": "AmsPatchRestrictAmsTags",
            "Effect": "Deny",
            "Action": [
                "ssm:AddTagsToResource",
                "ssm:RemoveTagsFromResource"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:TagKeys": [
                        "AMS*",
                        "Ams*",
```

```
                "ams*"
              ]
            }
          }
        },
        {
          "Sid": "TagReadPolicy",
          "Effect": "Allow",
          "Action": [
            "tag:GetResources",
            "tag:GetTagKeys"
          ],
          "Resource": "*"
        },
        {
          "Sid": "CloudtrailReadPolicy",
          "Effect": "Allow",
          "Action": [
            "cloudtrail:DescribeTrails",
            "cloudtrail:GetTrailStatus",
            "cloudtrail:LookupEvents"
          ],
          "Resource": "*"
        },
        {
          "Sid": "EventBridgePolicy",
          "Effect": "Allow",
          "Action": [
            "events:Describe*",
            "events:List*",
            "events:TestEventPattern"
          ],
          "Resource": "*"
        },
        {
          "Sid": "IAMReadOnlyPolicy",
          "Action": [
              "iam:ListRoles",
              "iam:GetRole"
          ],
          "Effect": "Allow",
          "Resource": "*"
        },
        {
```

```
                "Sid": "AmsResourceSchedulerPassRolePolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
            {
               "Sid": "AmsBackupPolicy",
               "Effect": "Allow",
               "Action": [
                 "backup:Describe*",
                 "backup:Get*",
                 "backup:List*"
```

```
            ],
            "Resource": "*"
        },
        {
            "Action": [
                "rds:DescribeDBSnapshots",
                "rds:ListTagsForResource",
                "rds:DescribeDBInstances",
                "rds:describeDBSnapshots",
                "rds:describeDBEngineVersions",
                "rds:describeOptionGroups",
                "rds:describeOrderableDBInstanceOptions",
                "rds:describeDBSubnetGroups",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBInstanceAutomatedBackups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "dynamodb:ListBackups",
                "dynamodb:ListTables"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticfilesystem:DescribeFilesystems"
            ],
            "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:describeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
```

```
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
```

```
            "Action": [
                "iam:ListRoles",
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:DescribeOrganization",
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
        {
            "Action": "fsx:DescribeFileSystems",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:file-system/*"
        },
        {
            "Action": "ds:DescribeDirectories",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordKMSPolicy",
          "Effect": "Allow",
          "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": [
            "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
          ],
          "Condition": {
            "ForAnyValue:StringLike": {
              "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
            }
          }
        },
```

```
            {
              "Sid": "AmsChangeRecordAthenaReadPolicy",
              "Effect": "Allow",
              "Action": [
                "athena:BatchGetNamedQuery",
                "athena:Get*",
                "athena:List*",
                "athena:StartQueryExecution",
                "athena:UpdateWorkGroup",
                "glue:GetDatabase*",
                "glue:GetTable*",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AmsChangeRecordS3ReadPolicy",
              "Effect": "Allow",
              "Action": [
                "s3:Get*",
                "s3:List*"
              ],
              "Resource": [
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
              ]
            },
            {
              "Sid": "AmsChangeRecordS3WritePolicy",
              "Effect": "Allow",
              "Action": [
                "s3:PutObject",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention"
              ],
              "Resource": [
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
              ]
            },
            {
```

```
            "Sid": "MaciePolicy",
            "Effect": "Allow",
            "Action": [
              "macie2:GetFindingStatistics"
            ],
            "Resource": "*"
          },
          {
            "Sid": "GuardDutyReadPolicy",
            "Effect": "Allow",
            "Action": [
              "guardduty:GetFindingsStatistics",
              "guardduty:ListDetectors"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SupportReadPolicy",
            "Effect": "Allow",
            "Action": "support:Describe*",
            "Resource": "*"
          },
          {
            "Sid": "ConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "config:Get*",
              "config:Describe*",
              "config:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AppConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "appconfig:List*",
              "appconfig:Get*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudFormationReadPolicy",
            "Effect": "Allow",
```

```
            "Action": [
              "cloudformation:DescribeStacks"
            ],
            "Resource": "*"
          },
          {
            "Sid": "EC2ReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ec2:DescribeInstances"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SSMReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ssm:Describe*",
              "ssm:Get*",
              "ssm:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "TagReadPolicy",
            "Effect": "Allow",
            "Action": [
              "tag:GetResources",
              "tag:GetTagKeys"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudtrailReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudtrail:DescribeTrails",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
          },
          {
            "Sid": "EventBridgePolicy",
```

```
            "Effect": "Allow",
            "Action": [
              "events:Describe*",
              "events:List*",
              "events:TestEventPattern"
            ],
            "Resource": "*"
          }
        ]
      }
```

Warum und wann AMS auf Ihr Konto zugreift

AMS Accelerate (Accelerate) -Operatoren können unter bestimmten Umständen auf Ihre Kontokonsole und Ihre Instances zugreifen, um Ihre Ressourcen zu verwalten. Diese Zugriffsereignisse sind in Ihren AWS CloudTrail (CloudTrail) Protokollen dokumentiert. Einzelheiten dazu, wie Sie die Aktivitäten des AMS Accelerate Operations Teams und AMS Accelerate Automation in Ihrem Konto überprüfen können, finden Sie unterÄnderungen in Ihren AMS Accelerate-Konten verfolgen.

Warum, wann und wie AMS auf Ihr Konto zugreift, wird in den folgenden Themen erklärt.

Auslöser für den Zugriff auf das AMS-Kundenkonto

Die Aktivität beim Zugriff auf AMS-Kundenkonten wird durch Auslöser gesteuert. Die Auslöser sind heute die AWS Tickets, die in unserem Problemmanagementsystem als Reaktion auf Alarme und Ereignisse von Amazon CloudWatch (CloudWatch) erstellt wurden, sowie auf von Ihnen eingereichte Vorfallberichte oder Serviceanfragen. Für jeden Zugriff können mehrere Serviceanrufe und Aktivitäten auf Host-Ebene durchgeführt werden.

Die Begründung des Zugriffs, die Auslöser und der Initiator des Triggers sind in der folgenden Tabelle aufgeführt.

Auslöser für den Zugriff

Zugriff	Initiator	Auslöser
Patchen	AMS	Problem mit dem Patch

Zugriff	Initiator	Auslöser
Untersuchung interner Probleme	AMS	Problemproblem (ein Problem, das als systemisch eingestuft wurde)
Untersuchung und Behebung von Warnmeldungen	AMS	Operative Arbeitselemente (SSM OpsItems) von AWS Systems Manager
Untersuchung und Behebung von Vorfällen	Sie	Eingehender Support-Fall (ein Vorfall oder eine Serviceanfrage, die Sie einreichen)
Bearbeitung eingehender Serviceanfragen	Sie	

Zugriff auf das AMS-Kundenkonto (IAM-Rollen)

AMS-Betreiber benötigen die folgenden Rollen, um Ihr Konto zu verwalten.

> **Note**
>
> AMS-Zugriffsrollen ermöglichen AMS-Operatoren den Zugriff auf Ihre Ressourcen, um AMS-Funktionen bereitzustellen (siehe Service description (Service-Beschreibung)). Eine Änderung dieser Rollen kann uns daran hindern, diese Funktionen bereitzustellen. Wenn Sie die AMS-Zugriffsrollen ändern müssen, wenden Sie sich an Ihren Cloud-Architekten.

IAM-Rollen für den AMS-Zugriff auf Kundenkonten

Name der Rolle	Beschreibung
ams-access-admin	Diese Rolle hat vollen administrativen Zugriff auf Ihr Konto ohne Einschränkungen. AMS-Dienste verwenden diese Rolle mit restriktiven Sitzungsr ichtlinien, die den Zugriff auf die Bereitstellung der AMS-Infrastruktur und den Betrieb Ihres Kontos einschränken.

Name der Rolle	Beschreibung
ams-access-admin-operations	Diese Rolle gewährt AMS-Betreibern Administr atorberechtigungen für den Betrieb Ihres Kontos. Diese Rolle gewährt keine Lese-, Schreib- oder Löschberechtigungen für Kundeninhalte in AWS Diensten, die üblicherweise als Datenspeicher verwendet werden, wie Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift und Amazon. ElastiCache Diese Rolle können nur qualifizierte AMS-Betreiber übernehmen, die über fundierte Kenntniss e und Erfahrungen im Bereich der Zugriffsverwaltung verfügen. Diese Operatoren dienen als Eskalatio nsstelle bei Problemen mit der Zugriffsverwaltung und greifen auf Ihre Konten zu, um Probleme mit dem Zugriff auf AMS-Betreiber zu beheben.
ams-access-management	Wird während des Onboardings manuell eingesetzt. Das AMS Access-System benötigt diese Rolle für die Verwaltung `ams-access-roles` und `ams-acces s-managed-policies` Stapelung.
ams-access-operations	Diese Rolle ist berechtigt, administrative Aufgaben in Ihren Konten auszuführen. Diese Rolle hat keine Lese-, Schreib- oder Löschberechtigungen für Kundeninhalte in AWS Diensten, die üblicherweise als Datenspeicher verwendet werden, wie Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift und Amazon. ElastiCache Berechtigungen zur Ausführung von AWS Identity and Access Management Schreibvo rgängen sind ebenfalls von dieser Rolle ausgeschl ossen. Mitarbeiter und Cloud-Architekten (CAs) von AMS Accelerate Operations können diese Rolle übernehmen.

Name der Rolle	Beschreibung
ams-access-read-only	Diese Rolle hat nur Lesezugriff auf Ihr Konto. Mitarbeiter und Cloud-Architekten (CAs) von AMS Accelerate Operations können diese Rolle übernehmen. Leseberechtigungen für Kundeninhalte in AWS Diensten, die üblicherweise als Datenspeicher verwendet werden, wie Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift und ElastiCache, erhalten diese Rolle nicht.
ams-access-security-analyst	Diese AMS-Sicherheitsrolle verfügt über Berechtigungen in Ihrem AMS-Konto, um spezielle Sicherheitswarnungen zu überwachen und Sicherheitsvorfälle zu behandeln. Nur sehr wenige ausgewählte AMS Security-Mitarbeiter können diese Rolle übernehmen.
ams-access-security-analyst-nur lesbar	Diese AMS-Sicherheitsrolle ist auf Leseberechtigungen in Ihrem AMS-Konto beschränkt, um spezielle Sicherheitswarnungen zu überwachen und Sicherheitsvorfälle zu behandeln.

> **Note**
>
> Dies ist die Vorlage für die ams-access-management Rolle. Es ist der Stack, den Cloud-Architekten (CAs) beim Onboarding manuell in Ihrem Konto bereitstellen: management-role.yaml.
> Dies ist die Vorlage für die verschiedenen Zugriffsrollen für die verschiedenen Zugriffsebenen:,,,: accelerate-roles.yaml. ams-access-read-only ams-access-operations ams-access-admin-operations ams-access-admin

So greift AMS auf Ihr Konto zu

AMS Accelerate-Betreiber können unter bestimmten Umständen auf Ihre Kontokonsole und Ihre Instances zugreifen.

AMS-Betreiber nutzen den internen AMS Accelerate Access Service, um auf sichere und geprüfte Weise auf Ihre Konten zuzugreifen. Für den Zugriff auf Ihre Instances verwenden AMS-Betreiber denselben internen AMS-Zugriffsdienst wie der Broker. Nachdem der Zugriff gewährt wurde, verwenden AMS Accelerate-Betreiber den SSM-Sitzungsmanager, um mithilfe von Sitzungsdaten Zugriff zu erhalten. Der RDP-Zugriff für Windows-Instances wird bereitgestellt, indem eine Portweiterleitung zur Instance eingerichtet und ein lokaler Benutzer mithilfe von SSM erstellt wird. Die lokalen Benutzeranmeldeinformationen werden für den RDP-Zugriff verwendet und am Ende der Sitzung entfernt.

Wie und wann benutzt man das Root-Benutzerkonto in AMS

Der Root-Benutzer ist der Superuser in Ihrem AWS Konto. AMS überwacht die Root-Nutzung. Wir empfehlen Ihnen, Root nur für die wenigen Aufgaben zu verwenden, für die es erforderlich ist, z. B.: Änderung Ihrer Kontoeinstellungen, Aktivierung des AWS Identity and Access Management (IAM-) Zugriffs auf Abrechnung und Kostenmanagement, Änderung Ihres Root-Passworts und Aktivierung der Multi-Faktor-Authentifizierung (MFA). Weitere Informationen finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind AWS Identity and Access Management .

Rooten Sie mit AMS Accelerate:

AMS verbietet Ihnen nicht, Ihr Root-Benutzerkonto zu verwenden. AMS Operations and Security behandelt ihre Nutzung jedoch als ein Problem, das untersucht werden muss, und wir werden uns bei jeder Nutzung an Ihr Sicherheitsteam wenden.

Wir empfehlen Ihnen, sich vierundzwanzig Stunden im Voraus mit Ihrem CSDM und Ihrer CA in Verbindung zu setzen, um sie über die Root-Zugriffsarbeiten zu informieren, die Sie durchführen möchten.

AMS-Betrieb und Sicherheitsreaktion bei Root-Nutzung:

AMS erhält einen Alarm, wenn das Root-Benutzerkonto verwendet wird. Wenn die Verwendung der Root-Anmeldeinformationen außerplanmäßig erfolgt, wenden sie sich an das AMS-Sicherheitsteam und Ihr Account-Team, um zu überprüfen, ob es sich um eine erwartete Aktivität handelt. Wenn es sich nicht um eine erwartete Aktivität handelt, arbeitet AMS mit Ihrem Sicherheitsteam zusammen, um das Problem zu untersuchen.

Sicherheitsmanagement in AMS Accelerate

AWS Managed Services verwendet mehrere Kontrollen, um Ihre Informationsressourcen zu schützen und Ihnen zu helfen, Ihre AWS Infrastruktur zu schützen. AMS Accelerate unterhält eine Sammlung von Maßnahmen AWS-Config-Regeln und Problembehebungsmaßnahmen, um sicherzustellen, dass alle Ihre Konten den Industriestandards für Sicherheit und Betriebsintegrität entsprechen. AWS-Config-Regeln verfolgt kontinuierlich die Konfigurationsänderung Ihrer aufgezeichneten Ressourcen. Wenn eine Änderung gegen Regelbedingungen verstößt, meldet AMS die Ergebnisse und ermöglicht es Ihnen, Verstöße je nach Schweregrad des Verstoßes automatisch oder auf Anfrage zu beheben. AWS-Config-Regeln die Einhaltung der Standards erleichtern, die vom Center for Internet Security (CIS), dem National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), dem Health Insurance Portability and Accountability Act (HIPAA) und dem Payment Card Industry (PCI) Data Security Standard (DSS) festgelegt wurden.

Darüber hinaus nutzt AMS Amazon, GuardDuty um potenziell unautorisierte oder böswillige Aktivitäten in Ihrer AWS Umgebung zu identifizieren. AMS überwacht die GuardDuty Ergebnisse rund um die Uhr. AMS arbeitet mit Ihnen zusammen, um die Auswirkungen der Ergebnisse zu verstehen und auf der Grundlage von Best-Practice-Empfehlungen Abhilfemaßnahmen zu ermitteln. AMS verwendet Amazon Macie auch, um Ihre sensiblen Daten wie persönliche Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII) und Finanzdaten zu schützen.

> **Note**
>
> Amazon Macie ist ein optionaler Service und standardmäßig nicht aktiviert.

AMS Accelerate bietet eine Reihe von Betriebsdienstleistungen, die Sie dabei unterstützen, betriebliche Exzellenz zu AWS erreichen. Weitere Informationen darüber, wie AMS Ihren Teams hilft, AWS Cloud mit den wichtigsten operativen Funktionen von AMS, einschließlich Helpdesk rund um die Uhr, proaktive Überwachung, Sicherheit, Patching, Protokollierung und Backup, allgemeine betriebliche Exzellenz zu erreichen, finden Sie in den AMS-Referenzarchitekturdiagrammen.

Themen

- AWS Identity and Access Management in AMS Accelerate
- Reaktion auf Sicherheitsvorfälle in AMS
- Protokollierung und Überwachung von Sicherheitsereignissen in Accelerate
- Konformität mit der Konfiguration in Accelerate
- Reaktion auf Vorfälle in Accelerate
- Resilienz bei Accelerate
- Sicherheitskontrolle für end-of-support Betriebssysteme
- Bewährte Sicherheitsmethoden in Accelerate
- Sicherheitsüberprüfungen für Änderungsanfragen
- Häufig gestellte Fragen zur Sicherheit

Verwenden Sie das Log4j SSM-Dokument, um Ereignisse in Accelerate zu entdecken

Das AWS Systems Manager Log4j-Dokument (SSM-Dokument) unterstützt Sie bei der Suche nach der Apache Log4j2-Bibliothek in aufgenommenen Workloads. Das Automatisierungsdokument enthält einen Bericht über die Prozess-ID der Java-Anwendung (en), in denen die Log4j2-Bibliothek aktiv ist.

Der Bericht enthält Informationen über die Java-Archive (JAR-Dateien), die sich in der angegebenen Umgebung befinden, die die Klasse enthält. JndiLookup Es hat sich bewährt, die erkannten Bibliotheken auf die neueste verfügbare Version zu aktualisieren. Dieses Upgrade verringert die in CVE-2021-44228 identifizierte Remote Code Execution (RCE). Laden Sie die neueste Version der Log4j-Bibliothek von Apache herunter. Weitere Informationen finden Sie unter Apache Log4j 2 herunterladen.

Das Dokument wird allen Regionen zur Verfügung gestellt, die bei Accelerate, registriert sind. Gehen Sie wie folgt vor, um auf das Dokument zuzugreifen:

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Dokumente aus.
3. Wählen Sie Mit mir geteilt.
4. Geben Sie in das Suchfeld AWSManagedServices-GatherLog4JInformation ein.

5. Verwenden Sie die Geschwindigkeitssteuerung, um das Dokument maßstabsgetreu zu bearbeiten.

Das AWSManagedServices-GatherLog 4JInformationsdokument erfasst die folgenden Parameter:

- InstanceId: (Erforderlich) ID Ihrer Instanz. EC2
- S3Bucket: (Optional) Die vorsignierte S3-URL oder S3-URI (s3://BUCKET_NAME), in die die Ergebnisse hochgeladen werden sollen.
- AutomationAssumeRole: (Erforderlich) Der ARN der Rolle, die es der Automatisierung ermöglicht, Aktionen in Ihrem Namen auszuführen.

Es hat sich bewährt, dieses Dokument mithilfe der Ratensteuerung auszuführen. Sie können den Parameter für die Preissteuerung auf den InstanceIdWert festlegen und ihm entweder eine Liste von Instanzen zuweisen oder eine Tag-Tastenkombination anwenden, um alle EC2 Instanzen mit einem bestimmten Tag als Ziel auszuwählen. AWS Managed Services empfiehlt außerdem, dass Sie einen Amazon Simple Storage Service (Amazon S3) -Bucket bereitstellen, in den Sie die Ergebnisse hochladen können, sodass Sie einen Bericht aus den in S3 gespeicherten Daten erstellen können. Ein Beispiel für die Zusammenfassung der Ergebnisse in S3 finden Sie unter EC2 Instance Stack | Log4j-Informationen sammeln.

Wenn Sie das Paket nicht aktualisieren können, befolgen Sie die Richtlinien im Abschnitt AWS Sicherheit unter Verwendung von AWS Sicherheitsdiensten zum Schutz vor der Log4j-Sicherheitslücke, zur Erkennung und zur Reaktion darauf. Um Sicherheitslücken zu minimieren, indem Sie die JndiLookup Klassenfunktionalität entfernen, führen Sie den Log4j-Hotpatch direkt mit Ihren Java-Anwendungen aus. Weitere Informationen zum Hotpatch finden Sie unter Hotpatch für Apache Log4j.

Wenn Sie Fragen zur Leistung der Automatisierung oder zur weiteren Vorgehensweise bei weiteren Abhilfemaßnahmen haben, senden Sie eine Serviceanfrage.

Überwachung der Infrastruktursicherheit in AMS

Wenn Sie AMS Accelerate nutzen, AWS setzt AMS Accelerate die folgende AWS Config Basisinfrastruktur und das folgende Regelwerk ein. AMS Accelerate verwendet diese Regeln, um Ihre Konten zu überwachen.

- AWS Config serviceverknüpfte Rolle: AMS Accelerate stellt die benannte serviceverknüpfte Rolle bereit AWSServiceRoleForConfig, die von verwendet wird, AWS Config um den Status anderer Dienste abzufragen. AWS Die AWSServiceRoleForConfigdienstbezogene Rolle vertraut darauf, dass der AWS Config Dienst die Rolle übernimmt. Die Berechtigungsrichtlinie für die AWSServiceRoleForConfigRolle umfasst nur Lese- und Schreibberechtigungen für Ressourcen und nur Leseberechtigungen für AWS Config Ressourcen in anderen Diensten, die diese Funktion unterstützen. AWS Config Wenn Sie bereits eine Rolle mit AWS Config Recorder konfiguriert haben, überprüft AMS Accelerate, ob an die bestehende Rolle eine verwaltete AWS Config-Richtlinie angehängt ist. Wenn nicht, ersetzt AMS Accelerate die Rolle durch die serviceverknüpfte Rolle. AWSServiceRoleForConfig
- AWS Config Rekorder und Bereitstellungskanal: AWS Config verwendet den Konfigurationsrekorder, um Änderungen an Ihren Ressourcenkonfigurationen zu erkennen und diese Änderungen als Konfigurationselemente zu erfassen. AMS Accelerate stellt den Konfigurationsrekorder in allen Diensten bereit AWS-Regionen, wobei alle Ressourcen kontinuierlich aufgezeichnet werden. AMS Accelerate erstellt auch den Config Delivery Channel, einen Amazon S3 S3-Bucket, der verwendet wird, um Änderungen an Ihren AWS Ressourcen aufzuzeichnen. Der Config Recorder aktualisiert den Konfigurationsstatus über den Lieferkanal. Der Konfigurationsrekorder und der Bereitstellungskanal sind erforderlich AWS Config , damit sie funktionieren. AMS Accelerate erstellt den gesamten AWS-Regionen Rekorder und einen Lieferkanal in einem einzigen AWS-Region. Wenn Sie bereits einen Rekorder und einen Übertragungskanal in einem haben AWS-Region, löscht AMS Accelerate die vorhandenen AWS Config Ressourcen nicht. Stattdessen verwendet AMS Accelerate Ihren vorhandenen Rekorder und Lieferkanal, nachdem überprüft wurde, ob sie ordnungsgemäß konfiguriert sind. Weitere Informationen zur AWS Config Kostensenkung finden Sie unterReduzieren Sie die AWS Config Kosten in Accelerate.
- AWS Config Regeln: AMS Accelerate verfügt über eine Sammlung von Maßnahmen AWS-Config-Regeln und Abhilfemaßnahmen, die Sie bei der Einhaltung der Industriestandards für Sicherheit und Betriebsintegrität unterstützen. AWS-Config-Regeln verfolgt kontinuierlich die Konfigurationsänderungen Ihrer aufgezeichneten Ressourcen. Wenn eine Änderung gegen Regelbedingungen verstößt, meldet AMS die Ergebnisse und ermöglicht es Ihnen, Verstöße je nach Schweregrad des Verstoßes automatisch oder auf Anfrage zu beheben. AWS-Config-Regeln die Einhaltung der Standards erleichtern, die vom Center for Internet Security (CIS), dem National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), dem Health Insurance Portability and Accountability Act (HIPAA) und dem Payment Card Industry (PCI) Data Security Standard (DSS) festgelegt wurden.

- AWS Config Aggregator-Autorisierung: Ein Aggregator ist ein AWS Config Ressourcentyp, der AWS Config Konfigurations- und Compliance-Daten aus mehreren Konten und mehreren Regionen sammelt. AMS Accelerate verknüpft Ihr Konto mit einem Konfigurationsaggregator, aus dem AMS Accelerate die Informationen zur Ressourcenkonfiguration und die Konformitätsdaten der Konfiguration Ihres Kontos zusammenfasst und den Compliance-Bericht generiert. Wenn in dem AMS-eigenen Konto bereits Aggregatoren konfiguriert sind, stellt AMS Accelerate einen zusätzlichen Aggregator bereit und der bestehende Aggregator wird nicht geändert.

> **Note**
>
> Der Config-Aggregator ist nicht in Ihren Konten eingerichtet, sondern in AMS-eigenen Konten eingerichtet, und Ihre Konten sind darin integriert.

Weitere Informationen dazu finden Sie unter: AWS Config

- AWS Config: Was ist Config?
- AWS-Config-Regeln: Ressourcen anhand von Regeln auswerten
- AWS-Config-Regeln: Dynamische Konformitätsprüfung: AWS-Config-Regeln — Dynamische Konformitätsprüfung für Cloud-Ressourcen
- AWS Config Aggregator: Datenaggregation mit mehreren Konten und mehreren Regionen

Informationen zu Berichten finden Sie unter. AWS Config Bericht zur Einhaltung der Kontrollvorschriften

Verwenden von serviceverknüpften Rollen für AMS Accelerate

AMS Accelerate verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle (SLR) ist eine einzigartige Art von IAM-Rolle, die direkt mit AMS Accelerate verknüpft ist. Serviceverknüpfte Rollen sind von AMS Accelerate vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von AMS Accelerate, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AMS Accelerate definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur AMS Accelerate seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und

Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Diensten, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Serviceverknüpfte Rollen nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rolle im Deployment Toolkit für AMS Accelerate

AMS Accelerate verwendet die benannte serviceverknüpfte Rolle (SLR) AWSServiceRoleForAWSManagedServicesDeploymentToolkit— diese Rolle stellt die AMS Accelerate-Infrastruktur in Kundenkonten bereit.

> **Note**
>
> Diese Richtlinie wurde kürzlich aktualisiert; Einzelheiten finden Sie unter. Beschleunigen Sie die Aktualisierung von serviceverknüpften Rollen

AMS Accelerate Deployment Toolkit (SLR)

Die AWSService RoleFor AWSManaged ServicesDeploymentToolkit dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `deploymenttoolkit.managedservices.amazonaws.com`

Die genannte Richtlinie AWSManagedServicesDeploymentToolkitPolicyermöglicht AMS Accelerate, Aktionen für die folgenden Ressourcen durchzuführen:

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

Diese SLR gewährt Amazon S3 Berechtigungen zur Erstellung und Verwaltung des Deployment-Buckets, der von AMS verwendet wird, um Ressourcen wie CloudFormation Vorlagen oder Lambda-Asset-Bundles in das Konto für Komponentenbereitstellungen hochzuladen. Diese SLR gewährt CloudFormation Berechtigungen zur Bereitstellung des CloudFormation Stacks, der die Deployment-

Buckets definiert. Weitere Informationen oder zum Herunterladen der Richtlinie finden Sie unter. AWSManagedServices_DeploymentToolkitPolicy

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Dienstbezogene Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen eines Bereitstellungs-Toolkits (SLR) für AMS Accelerate

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie in der AWS-Managementkonsole, der oder der AWS API bei AMS AWS CLI einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese dienstbezogene Rolle kann in Ihrem Konto erscheinen, wenn Sie den AMS Accelerate-Dienst vor dem 09. Juni 2022 genutzt haben, als er begann, serviceverknüpfte Rollen zu unterstützen, dann hat AMS Accelerate die AWSService RoleFor AWSManaged ServicesDeploymentToolkit Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie bei AMS einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle erneut für Sie.

Bearbeitung eines Implementierungs-Toolkits (SLR) für AMS Accelerate

AMS Accelerate erlaubt Ihnen nicht, die AWSService RoleFor AWSManaged ServicesDeploymentToolkit serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen eines Deployment Toolkits (SLR) für AMS Accelerate

Sie müssen die Rolle nicht manuell löschen. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Wenn Sie in der AWS-Managementkonsole, der oder der AWS API ein

Offboard von AMS ausführen AWS CLI, bereinigt AMS Accelerate die Ressourcen und löscht die serviceverknüpfte Rolle für Sie.

Sie können auch die IAM-Konsole, die AWS CLI oder die AWS API verwenden, um die dienstverknüpfte Rolle manuell zu löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

> **Note**
>
> Wenn der AMS Accelerate-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AMS Accelerate-Ressourcen zu löschen, die von der AWSService RoleFor AWSManaged ServicesDeploymentToolkit serviceverknüpften Rolle verwendet werden

Löschen Sie den `ams-cdk-toolkit` Stack aus allen Regionen, in denen Ihr Konto in AMS integriert war (möglicherweise müssen Sie die S3-Buckets zuerst manuell leeren).

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die serviceverknüpfte Rolle zu löschen. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Löschen einer serviceverknüpften Rolle.

Detective kontrolliert die dienstbezogene Rolle für AMS Accelerate

AMS Accelerate verwendet die serviceverknüpfte Rolle (SLR) mit dem Namen AWSServiceRoleForManagedServices_DetectiveControlsConfig— AWS Managed Services verwendet diese serviceverknüpfte Rolle, um Config-Recorder, Konfigurationsregeln und S3-Bucket Detective-Kontrollen bereitzustellen.

Der AWSServiceRoleForManagedServices_DetectiveControlsConfigserviceverknüpften Rolle ist die folgende verwaltete Richtlinie beigefügt: _. AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy Aktualisierungen dieser Richtlinie finden Sie unter Beschleunigen Sie die Aktualisierung AWS verwalteter Richtlinien.

Berechtigungen für Detective Controls SLR for AMS Accelerate

Die AWSServiceRoleForManagedServices_DetectiveControlsConfig dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `detectivecontrols.managedservices.amazonaws.com`

Dieser Rolle ist die `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS verwaltete Richtlinie beigefügt (siehe AWS verwaltete Richtlinie: _ AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy Der Dienst verwendet die Rolle, um AMS Detective Controls in Ihrem Konto zu konfigurieren), was die Bereitstellung von Ressourcen wie S3-Buckets, Konfigurationsregeln und einem Aggregator erfordert. Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine dienstverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Dienstbezogene Rollenberechtigungen im AWS Identity and Access Management-Benutzerhandbuch.

Die Erstellung eines Detektivs steuert SLR für AMS Accelerate

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie in der AWS-Managementkonsole, der oder der AWS API bei AMS AWS CLI einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie den AMS Accelerate-Dienst vor dem 09. Juni 2022 genutzt haben. Als er begann, serviceverknüpfte Rollen zu unterstützen, hat AMS Accelerate die AWSServiceRoleForManagedServices_DetectiveControlsConfig Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie bei AMS einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle erneut für Sie.

Die Bearbeitung eines Detektivs steuert SLR für AMS Accelerate

AMS Accelerate erlaubt Ihnen nicht, die AWSServiceRoleForManagedServices_DetectiveControlsConfig serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Das Löschen eines Detektivs steuert SLR für AMS Accelerate

Sie müssen die AWSServiceRoleForManagedServices_DetectiveControlsConfig Rolle nicht manuell löschen. Wenn Sie in der AWS-Managementkonsole, der oder der AWS API ein Offboard von AMS ausführen AWS CLI, bereinigt AMS Accelerate die Ressourcen und löscht die serviceverknüpfte Rolle für Sie.

Sie können auch die IAM-Konsole, die AWS CLI oder die AWS API verwenden, um die dienstverknüpfte Rolle manuell zu löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

> **Note**
>
> Wenn der AMS Accelerate-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AMS Accelerate-Ressourcen zu löschen, die von der AWSServiceRoleForManagedServices_DetectiveControlsConfig serviceverknüpften Rolle verwendet werden

Löschen `ams-detective-controls-config-rules-cdk` und `ams-detective-controls-infrastructure-cdk` Stapel aus allen Regionen`ams-detective-controls-config-recorder`, in denen Ihr Konto in AMS integriert war (möglicherweise müssen Sie zuerst die S3-Buckets manuell leeren).

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API, um die AWS CLI serviceverknüpfte Rolle zu löschen. AWSServiceRoleForManagedServices_DetectiveControlsConfig Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Rolle im Zusammenhang mit dem Amazon EventBridge Rule Service für AMS Accelerate

AMS Accelerate verwendet die benannte serviceverknüpfte Rolle (SLR). AWSServiceRoleForManagedServices_Events Diese Rolle vertraut darauf, dass einer der AWS Managed Services Service Principals (events.managedservices.amazonaws.com) die Rolle für Sie übernimmt. Der Service verwendet die Rolle, um eine von Amazon EventBridge verwaltete Regel zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem AWS-Konto erforderlich ist, um Informationen zur Änderung des Alarmstatus von Ihrem Konto an AWS Managed Services zu übermitteln.

Berechtigungen für EventBridge SLR für AMS Accelerate

Die AWSServiceRoleForManagedServices_Events dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `events.managedservices.amazonaws.com`

Dieser Rolle ist die `AWSManagedServices_EventsServiceRolePolicy` AWS verwaltete Richtlinie zugeordnet (siheAWS verwaltete Richtlinie: AWSManagedServices_EventsServiceRolePolicy). Der Dienst verwendet die Rolle, um Informationen über die Änderung des Alarmstatus von Ihrem Konto an AMS zu übermitteln. Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im AWS Identity and Access Management - Benutzerhandbuch.

Sie können die JSON-Datei AWSManagedServices_EventsServiceRolePolicy in dieser ZIP-Datei herunterladen: EventsServiceRolePolicy.zip.

Eine EventBridge Spiegelreflexkamera für AMS Accelerate erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie in der AWS-Managementkonsole, der oder der AWS API bei AMS AWS CLI einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie den AMS Accelerate-Dienst vor dem 7. Februar 2023 genutzt haben. Als er begann, serviceverknüpfte Rollen zu unterstützen, hat AMS Accelerate die AWSServiceRoleForManagedServices_Events Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie bei AMS einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle erneut für Sie.

Eine EventBridge Spiegelreflexkamera für AMS Accelerate bearbeiten

AMS Accelerate erlaubt es Ihnen nicht, die AWSServiceRoleForManagedServices_Events serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer EventBridge Spiegelreflexkamera für AMS Accelerate

Sie müssen die AWSServiceRoleForManagedServices_Events Rolle nicht manuell löschen. Wenn Sie in der AWS-Managementkonsole, der oder der AWS API ein Offboard von AMS ausführen AWS CLI, bereinigt AMS Accelerate die Ressourcen und löscht die serviceverknüpfte Rolle für Sie.

Sie können auch die IAM-Konsole, die AWS CLI oder die AWS API verwenden, um die dienstverknüpfte Rolle manuell zu löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

> **Note**
>
> Wenn der AMS Accelerate-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AMS Accelerate-Ressourcen zu löschen, die von der AWSServiceRoleForManagedServices_Events serviceverknüpften Rolle verwendet werden

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForManagedServices_Events serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Serviceverknüpfte Kontakte-Rolle für AMS Accelerate

AMS Accelerate verwendet die Service-Linked Role (SLR) mit dem Namen AWSServiceRoleForManagedServices_Contacts— Diese Rolle ermöglicht automatische Benachrichtigungen bei Vorfällen, indem sie dem Service ermöglicht, die vorhandenen Tags der betroffenen Ressource zu lesen und die konfigurierte E-Mail der entsprechenden Kontaktstelle abzurufen.

Dies ist der einzige Dienst, der diese serviceverknüpfte Rolle verwendet.

Der AWSServiceRoleForManagedServices_Contactsdienstbezogenen Rolle ist die folgende verwaltete Richtlinie beigefügt:. AWSManagedServices_ContactsServiceRolePolicy Aktualisierungen dieser Richtlinie finden Sie unter Beschleunigen Sie die Aktualisierung AWS verwalteter Richtlinien.

Berechtigungen für Contacts SLR for AMS Accelerate

Die AWSServiceRoleForManagedServices_Contacts dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `contacts-service.managedservices.amazonaws.com`

Dieser Rolle ist die von `AWSManagedServices_ContactsServiceRolePolicy` AWS verwaltete Richtlinie beigefügt (sieheAWS verwaltete Richtlinie: AWSManagedServices_ContactsServiceRolePolicy). Der Service verwendet die Rolle, um die Tags auf einer beliebigen AWS Ressource zu lesen und die im Tag enthaltene E-Mail der entsprechenden Kontaktperson für den Fall zu finden, dass Vorfälle auftreten. Diese Rolle ermöglicht automatische Benachrichtigungen bei Vorfällen, indem AMS das Tag auf einer betroffenen Ressource lesen und die E-Mail abrufen kann. Weitere Informationen finden Sie unter Dienstbezogene Rollenberechtigungen im AWS Identity and Access Management-Benutzerhandbuch.

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. AMS verwendet Tags, um Ihnen Verwaltungsdienste zur Verfügung zu stellen. Tags sind nicht für private oder vertrauliche Daten gedacht.

Die genannte Richtlinie für Rollenberechtigungen AWSManagedServices_ContactsServiceRolePolicy ermöglicht AMS Accelerate, die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- Aktion: Ermöglicht dem Contacts Service, die Tags zu lesen, die speziell für die E-Mail eingerichtet wurden, damit AMS Benachrichtigungen über Vorfälle an jede AWS-Ressource senden kann.

Sie können die JSON-Datei AWSManagedServices_ContactsServiceRolePolicy in dieser ZIP-Datei herunterladen: ContactsServicePolicy.zip.

Eine Spiegelreflexkamera für Kontakte für AMS Accelerate erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie in der AWS-Managementkonsole, der oder der AWS API bei AMS AWS CLI einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie den AMS Accelerate-Dienst vor dem 16. Februar 2023 genutzt haben. Als er begann, serviceverknüpfte Rollen zu unterstützen, hat AMS Accelerate die AWSServiceRoleForManagedServices_Contacts Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie bei AMS einsteigen, erstellt AMS Accelerate die serviceverknüpfte Rolle erneut für Sie.

Eine Spiegelreflexkamera für Kontakte für AMS Accelerate bearbeiten

AMS Accelerate erlaubt es Ihnen nicht, die AWSServiceRoleForManagedServices_Contacts serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer Kontakt-Spiegelreflexkamera für AMS Accelerate

Sie müssen die AWSServiceRoleForManagedServices_Contacts Rolle nicht manuell löschen. Wenn Sie in der AWS-Managementkonsole, der oder der AWS API ein Offboard von AMS ausführen AWS CLI, bereinigt AMS Accelerate die Ressourcen und löscht die serviceverknüpfte Rolle für Sie.

Sie können auch die IAM-Konsole, die AWS CLI oder die AWS API verwenden, um die dienstverknüpfte Rolle manuell zu löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

> **Note**
>
> Wenn der AMS Accelerate-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AMS Accelerate-Ressourcen zu löschen, die von der AWSServiceRoleForManagedServices_Contacts serviceverknüpften Rolle verwendet werden

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForManagedServices_Contacts serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für dienstverknüpfte AMS Accelerate-Rollen

AMS Accelerate unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS -Regionen und -Endpunkte.

Beschleunigen Sie die Aktualisierung von serviceverknüpften Rollen

Hier finden Sie Informationen zu Aktualisierungen der mit dem Dienst Accelerate verknüpften Rollen, die seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Accelerate-Seite, um automatische Benachrichtigungen über Änderungen an dieser Dokumentenverlauf für AMS Accelerate User Guide Seite zu erhalten.

Änderungen	Beschreibung	Datum

Aktualisierte Richtlinie — Deployment Toolkit	• Diese neuen Berechtigungen wurden für die Ressource `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` hinzugefügt:
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4. April 2024

Aktualisierte Richtlinie — Deployment Toolkit	• Diese neuen Berechtigungen wurden für die Ressource `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` hinzugefügt:
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Diese neuen Berechtigungen wurden für die Ressource hinzugefügt`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
		09. Mai 2023

Änderungen	Beschreibung	Datum

	<pre>ecr:SetRepositoryPolicy
	ecr:TagResource
	ecr:UntagResource</pre>
	• Außerdem wurden einige bestehende Aktionen mit Platzhaltern auf einzelne Aktionen beschränkt:
	<pre>- s3:DeleteObject*
	+ s3:DeleteObject
	+ s3:DeleteObjectTagging
	+ s3:DeleteObjectVersion
	+ s3:DeleteObjectVersionTagging
	
	- s3:GetObject*
	+ s3:GetObject
	+ s3:GetObjectAcl
	+ s3:GetObjectAttributes
	+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProt
	ection</pre>	

Aktualisierte Richtlinie — Detective Controls	• Die CloudFormation Maßnahmen wurden nach Bestätigung durch das Sicherheits- und Zugangsteam weiter eingegrenzt • Die Lambda-Aktionen wurden aus der Richtlinie entfernt, da sie sich nicht auf das Boarding auswirken onboarding/off	10. April 2023

Änderungen	Beschreibung	Datum
Aktualisierte Richtlinie — Detective Controls	Die Richtlinie wurde aktualisiert und die Richtlinie zur Begrenzung der Zugriffsrechte hinzugefügt.	21. März 2023
Neue dienstbezogene Rolle — Contacts SLR	Accelerate hat eine neue dienstbezogene Rolle für den Dienst Contacts hinzugefügt. Diese Rolle ermöglicht automatische Benachrichtigungen bei Vorfällen, indem sie dem Dienst ermöglicht, die vorhandenen Tags der betroffenen Ressource zu lesen und die konfigurierte E-Mail der entsprechenden Kontaktstelle abzurufen.	16. Februar 2023
Neue dienstbezogene Rolle — EventBridge	Accelerate hat eine neue serviceverknüpfte Rolle für eine EventBridge Amazon-Regel hinzugefügt. Diese Rolle vertraut darauf, dass einer der AWS Managed Services Service Principals (events.managedservices.amazonaws.com) die Rolle für Sie übernimmt. Der Service verwendet die Rolle, um eine von Amazon EventBridge verwaltete Regel zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem AWS-Konto erforderlich ist, um Informationen zur Änderung des Alarmstatus von Ihrem Konto an AWS Managed Services zu übermitteln.	07. Februar 2023

Änderungen	Beschreibung	Datum
Die serviceverknüpfte Rolle wurde aktualisiert — Deployment Toolkit	Beschleunigen Sie die Aktualisierung AWSService RoleFor AWSManaged ServicesDeploymentToolkit mit neuen S3-Berechtigungen. Diese neuen Berechtigungen wurden hinzugefügt: `"s3:GetLifecycleConfiguration", "s3:GetBucketLogging", "s3:ListBucket", "s3:GetBucketVersioning", "s3:PutLifecycleConfiguration", "s3:GetBucketLocation", "s3:GetObject*"`	30. Januar 2023
Accelerate hat begonnen, Änderungen nachzuverfolgen	Accelerate hat mit der Nachverfolgung von Änderungen für seine dienstbezogenen Rollen begonnen.	30. November 2022
Neue dienstleistungsbezogene Rolle — Detective Controls	Accelerate hat eine neue dienstbezogene Rolle für die Implementierung von Accelerate Detective Controls hinzugefügt. AWS Managed Services verwendet diese servicebezogene Rolle, um Config-Recorder, Konfigurationsregeln und S3-Bucket Detective-Kontrollen bereitzustellen.	13. Oktober 2022
Neue serviceverknüpfte Rolle — Deployment Toolkit	Accelerate hat eine neue dienstbezogene Rolle für die Bereitstellung der Accelerate-Infrastruktur hinzugefügt. Diese Rolle stellt die AMS Accelerate-Infrastruktur für Kundenkonten bereit.	09. Juni 2022

AWS verwaltete Richtlinien für AMS Accelerate

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Eine Tabelle der Änderungen finden Sie unterBeschleunigen Sie die Aktualisierung AWS verwalteter Richtlinien.

AWS verwaltete Richtlinie: AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) verwendet die `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS verwaltete Richtlinie. Diese AWS-verwaltete Richtlinie wird im AWSManagedServices_AlarmManager _ verwendet, ServiceRolePolicy um die Berechtigungen von IAM-Rollen einzuschränken, die von erstellt wurden. AWSServiceRoleForManagedServices_AlarmManager

Diese Richtlinie gewährt IAM-Rollen, die im Rahmen von erstellt wurdenWie funktioniert Alarm Manager, Berechtigungen zur Ausführung von Vorgängen wie der AWS Konfigurationsprüfung, dem Lesen der AWS Config zum Abrufen der Alarm Manager-Konfiguration und der Erstellung der erforderlichen CloudWatch Amazon-Alarme.

Die `AWSManagedServices_AlarmManagerPermissionsBoundary` Richtlinie ist der `AWSServiceRoleForManagedServices_DetectiveControlsConfig` serviceverknüpften Rolle

zugeordnet. Aktualisierungen zu dieser Rolle finden Sie unterBeschleunigen Sie die Aktualisierung von serviceverknüpften Rollen.

Sie können diese Richtlinie an Ihre IAM-Identitäten anhängen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `AWS Config`— Ermöglicht Berechtigungen zur Auswertung von Konfigurationsregeln und zur Auswahl der Ressourcenkonfiguration.
- `AWS AppConfig`— Erlaubt Berechtigungen zum Abrufen der AlarmManager Konfiguration.
- `Amazon S3`— Erlaubt Berechtigungen zum Betrieb von AlarmManager Buckets und Objekten.
- `Amazon CloudWatch`— Erlaubt Berechtigungen zum Lesen und Speichern AlarmManager verwalteter Alarme und Messwerte.
- `AWS Resource Groups and Tags`— Erlaubt Berechtigungen zum Lesen von Ressourcen-Tags.
- `Amazon EC2`— Erlaubt Berechtigungen zum Lesen von EC2 Amazon-Ressourcen.
- `Amazon Redshift`— Erlaubt Berechtigungen zum Lesen von Redshift-Instanzen und -Clustern.
- `Amazon FSx`— Ermöglicht Berechtigungen zur Beschreibung von Dateisystemen, Volumes und Ressourcen-Tags.
- `Amazon CloudWatch Synthetics`— Erlaubt Berechtigungen zum Lesen von Synthetics-Ressourcen.
- `Amazon Elastic Kubernetes Service`— Erlaubt Berechtigungen zur Beschreibung des Amazon EKS-Clusters.
- `Amazon ElastiCache`— Erlaubt Berechtigungen zur Beschreibung von Ressourcen.

Sie können die Richtliniendatei in dieser ZIP-Datei herunterladen: RecommendedPermissionBoundary.zip.

AWS verwaltete Richtlinie: _ AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy

AWS Managed Services (AMS) verwendet die `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der

AWSServiceRoleForManagedServices_DetectiveControlsConfigdienstbezogenen Rolle zugeordnet (siehe Detective kontrolliert die dienstbezogene Rolle für AMS Accelerate). Aktualisierungen der AWSServiceRoleForManagedServices_DetectiveControlsConfig dienstbezogenen Rolle finden Sie unter. Beschleunigen Sie die Aktualisierung von serviceverknüpften Rollen

Die Richtlinie ermöglicht es der dienstbezogenen Rolle, Aktionen für Sie abzuschließen.

Sie können die ServiceRolePolicy Richtlinie AWSManagedServices_DetectiveControlsConfig _ an Ihre IAM-Entitäten anhängen.

Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AMS Accelerate.

Details zu Berechtigungen

Diese Richtlinie verfügt über die folgenden Berechtigungen, damit AWS Managed Services Detective Controls alle erforderlichen Ressourcen bereitstellen und konfigurieren kann.

- CloudFormation— Ermöglicht AMS Detective Controls die Bereitstellung von CloudFormation Stacks mit Ressourcen wie S3-Buckets, Konfigurationsregeln und Config-Recorder.
- AWS Config— Ermöglicht AMS Detective Controls, AMS-Konfigurationsregeln zu erstellen, einen Aggregator zu konfigurieren und Ressourcen zu taggen.
- Amazon S3— ermöglicht AMS Detective Controls die Verwaltung seiner S3-Buckets.

Sie können die JSON-Richtliniendatei in dieser ZIP-Datei herunterladen: DetectiveControlsConfig_ ServiceRolePolicy .zip.

AWS verwaltete Richtlinie: AWSManaged ServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) verwendet die AWSManagedServicesDeploymentToolkitPolicy AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der AWSServiceRoleForAWSManagedServicesDeploymentToolkitdienstbezogenen Rolle zugeordnet (siehe Servicebezogene Rolle im Deployment Toolkit für AMS Accelerate). Die Richtlinie ermöglicht es der dienstbezogenen Rolle, Aktionen für Sie abzuschließen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AMS Accelerate.

Aktualisierungen der `AWSServiceRoleForManagedServicesDeploymentToolkitPolicy` dienstbezogenen Rolle finden Sie unter. Beschleunigen Sie die Aktualisierung von serviceverknüpften Rollen

Details zu Berechtigungen

Diese Richtlinie verfügt über die folgenden Berechtigungen, damit AWS Managed Services Detective Controls alle erforderlichen Ressourcen bereitstellen und konfigurieren kann.

- `CloudFormation`— Ermöglicht dem AMS Deployment Toolkit die Bereitstellung von CFN-Stacks mit S3-Ressourcen, die von CDK benötigt werden.
- `Amazon S3`— ermöglicht dem AMS Deployment Toolkit die Verwaltung seiner S3-Buckets.
- `Elastic Container Registry`— ermöglicht dem AMS Deployment Toolkit die Verwaltung seines ECR-Repositorys, das für die Bereitstellung von Ressourcen verwendet wird, die von AMS CDK-Apps benötigt werden.

Sie können die JSON-Richtliniendatei in dieser ZIP-Datei herunterladen: .zip. AWSManaged ServicesDeploymentToolkitPolicy

AWS verwaltete Richtlinie: AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) verwendet die von `AWSManagedServices_EventsServiceRolePolicy` AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der Rolle zugeordnet, die mit dem `AWSServiceRoleForManagedServices_EventsService` verknüpft ist. Die Richtlinie ermöglicht es der dienstbezogenen Rolle, Aktionen für Sie abzuschließen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AMS Accelerate.

Aktualisierungen der `AWSServiceRoleForManagedServices_Events` dienstbezogenen Rolle finden Sie unter. Beschleunigen Sie die Aktualisierung von serviceverknüpften Rollen

Details zu Berechtigungen

Diese Richtlinie verfügt über die folgenden Berechtigungen, damit Amazon Informationen EventBridge zur Änderung des Alarmstatus von Ihrem Konto an AWS Managed Services übermitteln kann.

- `events`— Ermöglicht Accelerate, von Amazon EventBridge verwaltete Regeln zu erstellen. Bei dieser Regel handelt es sich um die Infrastruktur, die Sie benötigen AWS-Konto , um Informationen zur Änderung des Alarmstatus von Ihrem Konto aus zu übermitteln AWS Managed Services.

Sie können die JSON-Richtliniendatei in dieser ZIP-Datei herunterladen: EventsServiceRolePolicy.zip.

AWS verwaltete Richtlinie: AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) verwendet die von `AWSManagedServices_ContactsServiceRolePolicy` AWS verwaltete Richtlinie. Diese AWS verwaltete Richtlinie ist der Rolle zugeordnet, die mit dem `AWSServiceRoleForManagedServices_Contacts` Service verknüpft ist (sieheEine Spiegelreflexkamera für Kontakte für AMS Accelerate erstellen). Die Richtlinie ermöglicht es AMS Contacts SLR, Ihre Ressourcen-Tags und deren Werte auf AWS-Ressourcen einzusehen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AMS Accelerate.

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. AMS verwendet Tags, um Ihnen Verwaltungsdienste zur Verfügung zu stellen. Tags sind nicht für private oder vertrauliche Daten gedacht.

Aktualisierungen der `AWSServiceRoleForManagedServices_Contacts` serviceverknüpften Rolle finden Sie unterBeschleunigen Sie die Aktualisierung von serviceverknüpften Rollen.

Details zu Berechtigungen

Diese Richtlinie verfügt über die folgenden Berechtigungen, damit Contacts SLR Ihre Ressourcen-Tags lesen kann, um die Kontaktinformationen der Ressourcen abzurufen, die Sie im Voraus eingerichtet haben.

- `IAM`— Ermöglicht dem Dienst „Kontakte“, sich Tags von IAM-Rollen und IAM-Benutzern anzusehen.
- `Amazon EC2`— Ermöglicht dem Kontaktservice, sich Tags auf EC2 Amazon-Ressourcen anzusehen.

- `Amazon S3`— Ermöglicht Contacts Service, sich Tags in Amazon S3 S3-Buckets anzusehen. Diese Aktion verwendet eine Bedingung, um sicherzustellen, dass AMS über den HTTP-Autorisierungsheader, das SigV4-Signaturprotokoll und HTTPS mit TLS 1.2 oder höher auf Ihre Bucket-Tags zugreift. Weitere Informationen finden Sie unter Authentifizierungsmethoden und Amazon S3 Signature Version 4 Authentication Specific Policy Keys.
- `Tag`— Ermöglicht dem Kontaktservice, sich Tags auf anderen AWS Ressourcen anzusehen.

- „iam: ListRoleTags „, „iam: ListUserTags „, „tag: GetResources „, „tag: „, GetTagKeys „tag: „, GetTagValues „ec2: „, DescribeTags „s3:“ GetBucketTagging

Sie können die JSON-Richtliniendatei in dieser ZIP-Datei herunterladen: .zip. ContactsServicePolicy

Beschleunigen Sie die Aktualisierung AWS verwalteter Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Accelerate an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

Änderungen	Beschreibung	Datum

Aktualisierte Richtlinie — Deployment Toolkit	• Diese neuen Berechtigungen wurden für die Ressource `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` hinzugefügt:
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4. April 2024

Aktualisierte Richtlinie — Deployment Toolkit	• Diese neuen Berechtigungen wurden für die Ressource `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` hinzugefügt:
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
		09. Mai 2023

Änderungen	Beschreibung	Datum

	• Diese neuen Berechtigungen wurden für die Ressource hinzugefügt`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	
	`ecr:CreateRepository`
	
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
	`ecr:SetRepositoryPolicy`
	`ecr:TagResource`
	`ecr:UntagResource`
	• Außerdem wurden einige bestehende Aktionen mit Platzhaltern auf einzelne Aktionen beschränkt:
	
	`- s3:DeleteObject*`
	
	`+ s3:DeleteObject`
	`+ s3:DeleteObjectTagging`
	`+ s3:DeleteObjectVersion`
	`+ s3:DeleteObjectVersionTagging`
	
	`- s3:GetObject*`
	`+ s3:GetObject`
	`+ s3:GetObjectAcl`
	`+ s3:GetObjectAttributes`
	`+ s3:GetObjectLegalHold`
	`+ s3:GetObjectRetention`
	`+ s3:GetObjectTagging`
	`+ s3:GetObjectVersion`
	`+ s3:GetObjectVersionAcl`
	`+ s3:GetObjectVersionAttributes`
	`+ s3:GetObjectVersionForReplication`
	`+ s3:GetObjectVersionTagging`
	`+ s3:GetObjectVersionTorrent`	

Änderungen	Beschreibung	Datum

	<pre>- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProtection</pre>	

Aktualisierte Richtlinie — Detective Controls	• Die CloudFormation Maßnahmen wurden nach Bestätigung durch das Sicherheits- und Zugangsteam weiter eingegrenzt • Die Lambda-Aktionen wurden aus der Richtlinie entfernt, da sie sich nicht auf das Boarding auswirken onboarding/off	10. April 2023
Aktualisierte Richtlinie — Detective Controls	Die `ListAttachedRolePolicies` Aktion wurde aus der Richtlinie entfernt. Die Aktion hatte Ressource als Platzhalter (*). Da es sich bei „list“ um eine nicht mutative Aktion handelt, erhält sie Zugriff auf alle Ressourcen und der Platzhalter ist nicht zulässig.	28. März 2023
Aktualisierte Richtlinie — Detective Controls	Die Richtlinie wurde aktualisiert und die Richtlinie zur Begrenzung der Zugriffsrechte hinzugefügt.	21. März 2023
Neue Richtlinie — Contacts Service	Accelerate hat eine neue Richtlinie hinzugefügt, mit der Sie die Kontaktinformationen Ihres Kontos anhand Ihrer Ressourcen-Tags einsehen können. Accelerate hat eine neue Richtlinie hinzugefügt, mit der Ihre Ressourcen-Tags gelesen werden können, sodass die Ressourcenkontaktinformationen abgerufen werden können, die Sie im Voraus eingerichtet haben.	16. Februar 2023

Änderungen	Beschreibung	Datum
Neue Richtlinie — Veranstaltungsservice	Accelerate hat eine neue Richtlinie hinzugefügt, um Informationen zur Änderung des Alarmstatus von Ihrem Konto an AWS Managed Services zu übermitteln. Gewährt IAM-Rollen, die im Rahmen von Wie funktioniert Alarm Manager Berechtigungen zum Erstellen einer erforderlichen von Amazon EventBridge verwalteten Regel erstellt wurden.	07. Februar 2023
Aktualisierte Richtlinie — Deployment Toolkit	Es wurden S3-Berechtigungen hinzugefügt, um das Offboarding von Kunden über Accelerate zu unterstützen.	30. Januar 2023
Neue Richtlinie — Detective Controls	Ermöglicht der dienstbezogenen Rolle,Detective kontrolliert die dienstbezogene Rolle für AMS Accelerate, die Durchführung von Aktionen zur Implementierung von Accelerate Detective Controls.	19. Dezember 2022
Neue Richtlinie — Alarm Manager	Accelerate hat eine neue Richtlinie hinzugefügt, um Berechtigungen zur Ausführung von Alarm Manager-Aufgaben zu gewähren. Gewährt IAM-Rollen, die im Rahmen von Wie funktioniert Alarm Manager Berechtigungen zur Ausführung von Vorgängen wie der AWS Konfigurationsauswertung, AWS dem Lesen von Konfigurationen zum Abrufen der Alarm-Manager-Konfiguration und der Erstellung der erforderlichen CloudWatch Amazon-Alarme erstellt wurden.	30. November 2022
Beschleunigt hat die Nachverfolgung von Änderungen gestartet	Accelerate hat mit der Nachverfolgung von Änderungen für die von AWS ihm verwalteten Richtlinien begonnen.	30. November 2022

Änderungen	Beschreibung	Datum
Neue Richtlinie — Deployment Toolkit	Accelerate hat diese Richtlinie für Bereitstellungsauf gaben hinzugefügt. Gewährt der serviceverknüpften Rolle AWSServic eRoleForAWSManagedServicesDeployment ToolkitBerechtigungen für den Zugriff auf bereitste llungsbezogene Amazon S3 S3-Buckets und -Stacks und deren Aktualisierung. CloudFormation	09. Juni 2022

Datenschutz in Accelerate

AMS Accelerate nutzt native Tools und Prozesse AWS-Services wie Amazon GuardDuty, Amazon Macie (optional) und andere interne proprietäre Tools und Prozesse, um Ihre verwalteten Konten kontinuierlich zu überwachen. Nach dem Auslösen eines Alarms übernimmt AMS Accelerate die Verantwortung für die erste Auswahl und Reaktion auf den Alarm. Die Reaktionsprozesse von AMS basieren auf NIST-Standards. AMS Accelerate testet gemeinsam mit Ihnen regelmäßig Reaktionsprozesse mithilfe von Security Incident Response Simulation, um Ihren Arbeitsablauf an die bestehenden Sicherheitsreaktionsprogramme für Kunden anzupassen.

Wenn AMS Accelerate einen Verstoß oder die unmittelbare Gefahr eines Verstoßes gegen Ihre Sicherheitsrichtlinien feststellt, sammelt Accelerate Informationen, einschließlich der betroffenen Ressourcen und aller konfigurationsbezogenen Änderungen. AWS AMS Accelerate bietet rund um die Uhr follow-the-sun Support mit engagierten Mitarbeitern, die Überwachungs-Dashboards, Warteschlangen und Serviceanfragen für all Ihre verwalteten Konten aktiv überprüfen und untersuchen. Accelerate untersucht die Ergebnisse zusammen mit internen Sicherheitsexperten, um die Aktivitäten zu analysieren und Sie über die in Ihrem Konto aufgeführten Ansprechpartner für die Sicherheitseskalation zu benachrichtigen.

Auf der Grundlage der Ergebnisse setzt sich Accelerate proaktiv mit Ihnen in Verbindung. Wenn Sie feststellen, dass die Aktivität nicht autorisiert oder verdächtig ist, arbeitet AMS mit Ihnen zusammen, um das Problem zu untersuchen und zu beheben oder einzudämmen. Es gibt bestimmte Arten von Ergebnissen, bei GuardDuty denen Sie die Auswirkungen bestätigen müssen, bevor Accelerate Maßnahmen ergreift. Beispielsweise weist der GuardDuty Befundtyp UnauthorizedAccess:IAMUser/darauf hinConsoleLogin, dass sich einer Ihrer Benutzer von einem

ungewöhnlichen Ort aus angemeldet hat. AMS benachrichtigt Sie und bittet Sie, das Ergebnis zu überprüfen, um zu bestätigen, ob dieses Verhalten legitim ist.

Überwachen Sie mit Amazon Macie

AMS Accelerate unterstützt Amazon Macie, und es ist eine bewährte Methode, Amazon Macie zu verwenden, um eine große und umfassende Liste vertraulicher Daten wie persönliche Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII) und Finanzdaten zu erkennen.

Sie können Macie so konfigurieren, dass es regelmäßig auf jedem Amazon S3 S3-Bucket ausgeführt wird. Dadurch wird die Bewertung neuer oder geänderter Objekte innerhalb eines Buckets im Laufe der Zeit automatisiert. Sobald Sicherheitsfeststellungen generiert werden, benachrichtigt AMS Sie und arbeitet mit Ihnen zusammen, um die Sicherheitslücken bei Bedarf zu beheben.

Weitere Informationen finden Sie unter Analysieren der Amazon Macie Macie-Ergebnisse.

Überwachen Sie mit GuardDuty

GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Feeds mit Bedrohungsinformationen wie Listen bösartiger IP-Adressen und Domänen sowie maschinelles Lernen verwendet, um unerwartete und potenziell unautorisierte und bösartige Aktivitäten in Ihrer AWS Umgebung zu identifizieren. Dazu können Probleme wie die Eskalation von Rechten, die Verwendung offengelegter Anmeldeinformationen oder die Kommunikation mit bösartigen IP-Adressen oder Domänen gehören. GuardDuty überwacht das AWS-Konto Zugriffsverhalten auf Anzeichen einer Beeinträchtigung, wie z. B. unautorisierte Infrastrukturbereitstellungen oder Instanzen, die in einer AWS Region bereitgestellt werden, die Sie noch nie genutzt haben. GuardDuty erkennt auch ungewöhnliche API-Aufrufe, wie z. B. eine Änderung der Passwortrichtlinie zur Verringerung der Passwortstärke. Weitere Informationen finden Sie im GuardDuty - Benutzerhandbuch.

Gehen Sie wie folgt vor, um Ihre GuardDuty Ergebnisse einzusehen und zu analysieren:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie Ergebnisse und dann ein bestimmtes Ergebnis aus, um Details anzuzeigen. Die Details für jedes Ergebnis unterscheiden sich je nach Art des Ergebnisses, den beteiligten Ressourcen und der Art der Aktivität.

Weitere Informationen zu verfügbaren Suchfeldern finden Sie unter GuardDuty Findungsdetails.

Verwenden Sie GuardDuty Unterdrückungsregeln, um Ergebnisse zu filtern

Eine Unterdrückungsregel besteht aus einer Reihe von Kriterien, die aus einem Filterattribut und einem Wert bestehen. Sie können Unterdrückungsregeln verwenden, um Ergebnisse mit geringem Wert zu filtern, auf die Sie nicht reagieren möchten, z. B. falsch positive Ergebnisse oder bekannte Aktivitäten. Durch das Filtern Ihrer Ergebnisse können Sie leichter die Sicherheitsbedrohungen erkennen, die sich möglicherweise am stärksten auf Ihre Umgebung auswirken.

Um Ergebnisse zu filtern, archivieren Unterdrückungsregeln automatisch neue Ergebnisse, die Ihren angegebenen Kriterien entsprechen. Archivierte Ergebnisse werden nicht an AWS Security Hub, Amazon S3 oder CloudTrail Events gesendet. Unterdrückungsfilter reduzieren also Daten, die nicht bearbeitet werden können, wenn Sie GuardDuty Ergebnisse über Security Hub oder eine SIEM-Warn- und Ticketing-Anwendung eines Drittanbieters nutzen.

AMS verfügt über eine Reihe definierter Kriterien zur Identifizierung von Unterdrückungsregeln für Ihre verwalteten Konten. Wenn ein verwaltetes Konto diese Kriterien erfüllt, wendet AMS die Filter an und erstellt eine Serviceanfrage (SR) an Sie, in der der verwendete Unterdrückungsfilter detailliert beschrieben wird.

Sie können mit AMS über einen SR kommunizieren, um die Unterdrückungsfilter zu ändern oder rückgängig zu machen.

Archivierte Ergebnisse anzeigen

GuardDuty generiert weiterhin Ergebnisse, auch wenn diese Ergebnisse Ihren Unterdrückungsregeln entsprechen. Unterdrückte Ergebnisse werden als archiviert markiert. GuardDuty speichert archivierte Ergebnisse 90 Tage lang. Sie können die archivierten Ergebnisse für diese 90 Tage in der GuardDuty Konsole anzeigen, indem Sie in der Tabelle mit den Ergebnissen die Option Archiviert auswählen. Oder zeigen Sie archivierte Ergebnisse über die GuardDuty API an, indem Sie die ListFindingsAPI verwenden, wobei findingCriteria service.archived gleich true ist.

Häufige Anwendungsfälle für Unterdrückungsregeln

Die folgenden Befundtypen haben häufig Anwendungsfälle für die Anwendung von Unterdrückungsregeln.

- Recon: EC2 /Portscan: Verwenden Sie eine Unterdrückungsregel, um Ergebnisse automatisch zu archivieren, wenn Sie einen autorisierten Schwachstellenscanner verwenden.
- UnauthorizedAccess:EC2/SSHBruteForce: Verwenden Sie eine Unterdrückungsregel, um Ergebnisse automatisch zu archivieren, wenn sie auf Bastion-Instances abzielen.

- Recon:EC2/PortProbeUnprotectedPort: Verwenden Sie eine Unterdrückungsregel, um Ergebnisse automatisch zu archivieren, wenn sie auf absichtlich offengelegte Instanzen abzielen.

Überwachen Sie mit der Amazon Route 53 Resolver DNS-Firewall

Amazon Route 53 Resolver reagiert rekursiv auf DNS-Abfragen von AWS Ressourcen für öffentliche Aufzeichnungen, Amazon VPC-spezifische DNS-Namen und private gehostete Zonen von Amazon Route 53 und ist standardmäßig in allen verfügbar. VPCs Mit der Route-53-Resolver-DNS-Firewall können Sie ausgehenden DNS-Datenverkehr für Ihre virtuelle private Cloud (VPCs, Virtual Private Clouds) filtern und regulieren. Dazu erstellen Sie wiederverwendbare Sammlungen von Filterregeln in Regelgruppen der DNS-Firewall, ordnen die Regelgruppen Ihrer VPC zu und überwachen dann Aktivitäten in DNS-Firewall-Protokollen und -Metriken. Je nach Aktivität können Sie das Verhalten der DNS-Firewall entsprechend anpassen. Weitere Informationen finden Sie unter Verwenden der DNS-Firewall zum Filtern von ausgehendem DNS-Verkehr.

Gehen Sie wie folgt vor, um Ihre Route 53 Resolver DNS-Firewall-Konfiguration anzuzeigen und zu verwalten:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie unter DNS-Firewall die Option Regelgruppen aus.
3. Überprüfen, bearbeiten oder löschen Sie Ihre bestehende Konfiguration oder erstellen Sie eine neue Regelgruppe. Weitere Informationen finden Sie unter So funktioniert die Route 53 Resolver DNS Firewall.

Amazon Route 53 Resolver DNS-Firewall-Überwachung und Sicherheit

Die Amazon Route 53 DNS-Firewall verwendet die Konzepte Regelzuordnungen, Regelaktion und Regelauswertungspriorität. Eine Domainliste ist ein wiederverwendbarer Satz von Domainspezifikationen, die Sie in einer DNS-Firewall-Regel innerhalb einer Regelgruppe verwenden. Wenn Sie eine Regelgruppe mit einer VPC verknüpfen, vergleicht die DNS-Firewall Ihre DNS-Abfragen mit den Domainlisten, die in den Regeln verwendet werden. Wenn die DNS-Firewall eine Übereinstimmung findet, verarbeitet sie die DNS-Abfrage entsprechend der Aktion der Abgleichsregel. Weitere Informationen zu Regelgruppen und Regeln finden Sie unter Regelgruppen und Regeln für die DNS-Firewall.

Domainlisten lassen sich in zwei Hauptkategorien einteilen:

- Verwaltete Domainlisten, die für Sie AWS erstellt und verwaltet werden.
- Ihre eigenen Domainlisten, die Sie erstellen und verwalten.

Regelgruppen werden anhand ihres Zuordnungsprioritätsindex bewertet.

Standardmäßig stellt AMS eine Basiskonfiguration bereit, die aus der folgenden Regel und Regelgruppe besteht:

- Eine Regelgruppe mit dem Namen`DefaultSecurityMonitoringRule`. Die Regelgruppe hat die höchste Zuordnungspriorität, die zum Zeitpunkt der Erstellung für jede vorhandene VPC in jeder aktivierten AWS-Region Version verfügbar ist.
- Eine Regel `DefaultSecurityMonitoringRule` mit Priorität 1 innerhalb der `DefaultSecurityMonitoringRule` Regelgruppe, die die Liste der `AWSManagedDomainsAggregateThreatList` verwalteten Domänen mit der Aktion ALERT verwendet.

Wenn Sie über eine bestehende Konfiguration verfügen, wird die Basiskonfiguration mit einer niedrigeren Priorität als Ihre bestehende Konfiguration bereitgestellt. Ihre bestehende Konfiguration ist die Standardkonfiguration. Sie verwenden die AMS-Basiskonfiguration als Sammellösung, wenn Ihre bestehende Konfiguration keine Anweisung mit höherer Priorität zum Umgang mit der Abfrageauflösung enthält. Gehen Sie wie folgt vor, um die Basiskonfiguration zu ändern oder zu entfernen:

- Wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM) oder Cloud Architect (CA).
- Erstellen Sie eine Serviceanfrage.

Datenverschlüsselung in AMS Accelerate

AMS Accelerate verwendet mehrere AWS-Services zur Datenverschlüsselung.

Amazon Simple Storage Service bietet mehrere Objektverschlüsselungsoptionen, die Daten während der Übertragung und im Speicher schützen. Bei der serverseitigen Verschlüsselung wird das Objekt verschlüsselt, bevor es auf Datenträgern im Rechenzentrum gespeichert wird. Wenn die Objekte heruntergeladen werden, werden sie wieder entschlüsselt. Wenn Sie Ihre Anforderung authentifizieren und Zugriffsberechtigungen besitzen, gibt es in Bezug auf die Art und Weise, wie Sie auf verschlüsselte oder nicht verschlüsselte Objekte zugreifen, keinen Unterschied. Weitere Informationen finden Sie unter Datenschutz in Amazon S3.

AWS Identity and Access Management in AMS Accelerate

AWS Identity and Access Management ist ein Webservice, mit dem Sie den Zugriff auf AWS Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen. Während des Onboardings von AMS Accelerate sind Sie dafür verantwortlich, kontoübergreifende IAM-Administratorrollen in jedem Ihrer verwalteten Konten einzurichten.

In AMS Accelerate sind Sie für die Verwaltung des Zugriffs auf Ihre AWS-Konten und die ihnen zugrunde liegenden Ressourcen verantwortlich, z. B. für Zugriffsverwaltungslösungen, Zugriffsrichtlinien und verwandte Prozesse. Das bedeutet, dass Sie Ihren Benutzerlebenszyklus, die Berechtigungen in Verzeichnisdiensten und das föderierte Authentifizierungssystem für den Zugriff auf die AWS Konsole oder AWS APIs verwalten. Um Sie bei der Verwaltung Ihrer Zugriffslösung zu unterstützen, stellt AMS Accelerate AWS Config Regeln bereit, die häufig auftretende IAM-Fehlkonfigurationen erkennen, und sendet Korrekturbenachrichtigungen. Weitere Informationen finden Sie unter AWS Config Managed Rules.

Authentifizierung mit Identitäten in AMS Accelerate

AMS verwendet IAM-Rollen, bei denen es sich um eine Art von IAM-Identität handelt. Eine IAM-Rolle ähnelt einem Benutzer insofern, als es sich um eine Identität mit Berechtigungsrichtlinien handelt, die festlegen, was die Identität tun kann und was nicht. AWS Einer Rolle sind jedoch keine Anmeldeinformationen zugeordnet. Anstatt eindeutig einer Person zugeordnet zu sein, kann jeder, der sie benötigt, davon ausgehen. Ein IAM-Benutzer kann eine Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu erlangen.

Die Zugriffsrollen werden durch die interne Gruppenmitgliedschaft gesteuert, die vom Operations Management verwaltet und regelmäßig überprüft wird. AMS verwendet die folgenden IAM-Rollen.

> **Note**
>
> AMS-Zugriffsrollen ermöglichen AMS-Operatoren den Zugriff auf Ihre Ressourcen, um AMS-Funktionen bereitzustellen (siehe Service description (Service-Beschreibung)). Eine Änderung dieser Rollen kann uns daran hindern, diese Funktionen bereitzustellen. Wenn Sie die AMS-Zugriffsrollen ändern müssen, wenden Sie sich an Ihren Cloud-Architekten.

Name der Rolle	Beschreibung
Wird verwendet von (Entität): Nur AMS Access Service	
ams-access-management	Wird von Ihnen während des Onboardings manuell bereitgestellt. Wird nur von AMS Access für die Bereitstellung oder Aktualisierung von Zugriffsrollen vorausgesetzt. Bleibt nach dem Onboarding in Ihrem Konto für future Aktualisierungen der Zugriffsrollen.
Wird verwendet von (Entität): AMS Operations	
ams-access-admin-operations	Diese Rolle verfügt über Administratorberechtigungen für den Betrieb in Konten, jedoch nicht über Berechtigungen zum Lesen, Schreiben oder Löschen von Kundeninhalten in AWS Diensten, die üblicherweise als Datenspeicher verwendet werden, wie Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift und Amazon. ElastiCache Nur sehr wenige ausgewählte AMS-Mitarbeiter können diese Rolle übernehmen.
ams-access-operations	Diese AMS Operations-Rolle ist berechtigt, administrative Aufgaben in Ihren Konten auszuführen. Diese Rolle hat keine Lese-, Schreib- oder Löschberechtigungen für Kundeninhalte in AWS Diensten, die üblicherweise als Datenspeicher verwendet werden, wie Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift und Amazon. ElastiCache Berechtigungen zur Ausführung von AWS Identity and Access Managemen

Name der Rolle	Beschreibung
	t Schreibvorgängen sind ebenfalls von dieser Rolle ausgeschlossen.
ams-access-read-only	Diese schreibgeschützte AMS-Rolle ist auf schreibgeschützte Berechtigungen in Ihrem AMS-Konto beschränkt. Leseberechtigungen für Kundeninhalte in AWS Diensten, die üblicherweise als Datenspeicher verwendet werden, wie Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift und ElastiCache, werden von dieser Rolle nicht gewährt.
Wird verwendet von (Entität): AMS Operations und AMS Services	
ams_ssm_automation_role	Wird davon ausgegangen, SSM AWS Systems Manager Automation-Dokumente in Ihrem Konto auszuführen.
ams_ssm_automation_role	
Wird verwendet von (Entität): AMS Security	
ams-access-security-analyst	Diese AMS-Sicherheitsrolle ist in Ihrem AMS-Konto berechtigt, spezielle Sicherheitswarnungen zu überwachen und Sicherheitsvorfälle zu behandeln. Nur sehr wenige ausgewählte AMS Security-Mitarbeiter können diese Rolle übernehmen. Leseberechtigungen für Kundeninhalte in AWS Diensten, die häufig als Datenspeicher verwendet werden, wie Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift und ElastiCache, werden von dieser Rolle nicht gewährt.

Name der Rolle	Beschreibung
ams-access-security-analyst-nur lesbar	Diese AMS-Sicherheitsrolle ist auf Leseberechtigungen in Ihrem AMS-Konto beschränkt, um spezielle Sicherheitswarnungen zu überwachen und Sicherheitsvorfälle zu behandeln. Leseberechtigungen für Kundeninhalte in AWS Diensten, die häufig als Datenspeicher verwendet werden, wie Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift und ElastiCache, werden von dieser Rolle nicht gewährt.
Benutzt von (Entität): AWS Services	
ams-access-admin	Diese AMS-Administratorrolle verfügt über volle Berechtigungen für den Betrieb von Konten ohne Einschränkungen. Nur interne AMS-Dienste (mit einer abgegrenzten Sitzungsrichtlinie) können die Administratorrolle übernehmen.
ams-opscenter-eventbridge-role	Wird von Amazon EventBridge AWS Systems Manager OpsItems als Teil eines AMS-spezifischen AWS-Config-Regeln Behebungsworkflows erstellt.
AMSOSConfigurationCustomerInstanceRole	Diese IAM-Rolle wird auf Ihre EC2 Amazon-Instances angewendet, wenn der AMS OS-Konfigurationsservice feststellt, dass die erforderlichen IAM-Richtlinien fehlen. Es ermöglicht Ihren EC2 Amazon-Instances die Interaktion mit AWS Systems Manager Amazon CloudWatch - und EventBridge Amazon-Diensten. Außerdem wurde die individuell verwaltete AMS-Richtlinie beigefügt, um den RDP-Zugriff auf Ihre Windows-Instances zu ermöglichen.

Name der Rolle	Beschreibung
mc-patch-glue-service-Rolle	Wird vom AWS Glue ETL-Workflow für die Durchführung der Datentransformation und deren Vorbereitung für den AMS-Patch-Berichtsgenerator übernommen.
Wird verwendet von (Entität): AMS Service	
ams-alarm-manager- AWSManaged ServicesAlarmManagerDe - <8-digit hash>	Wird von der AMS Alarm Manager-Infrastruktur in Ihrem AMS-Konto verwendet, um die AWS-Config-Regeln Evaluierung für eine neue AWS AppConfig Bereitstellung durchzuführen.
ams-alarm-manager- AWSManaged ServicesAlarmManagerRe - <8-digit hash>	Wird von AMS Alarm Manager als Behebungs infrastruktur in Ihrem AMS-Konto verwendet, um die Erstellung oder Löschung von Alarmen zur Behebung zu ermöglichen.
ams-alarm-manager- AWSManaged ServicesAlarmManager SS- <8-digit hash>	Wird davon ausgegangen AWS Systems Manager , dass der AMS Alarm Manager Remediation Service in Ihrem AMS-Konto aufgerufen wird.
ams-alarm-manager- - AWSManaged ServicesAlarmManagerTr <8-digit hash>	Wird von der AMS Alarm Manager-Infrastruktur in Ihrem AWS Konto übernommen, um regelmäßige AWS-Config-Regeln AMS-Evaluierungen durchzuführen.
ams-alarm-manager- AWSManaged ServicesAlarmManagerVa - <8-digit hash>	Wird von der AMS Alarm Manager-Infrastruktur in Ihrem AMS-Konto übernommen, um sicherzustellen, dass die erforderlichen Alarme im AWS Konto vorhanden sind.
ams-backup-iam-role	Diese Rolle wird für die Ausführung AWS Backup innerhalb Ihrer Konten verwendet.

Name der Rolle	Beschreibung
AMS-Überwachung- - AWSManaged ServicesLogGroupLimitLamb <8-digit hash>	Wird von der AMS Logging & Monitoring-Infrastruktur in Ihrem AMS-Konto verwendet, um das Amazon CloudWatch Logs-Gruppenlimit auszuwerten und mit den Servicekontingenten zu vergleichen.
ams-monitoring- AWSManaged Dienste RDSMonitoring RDSE- <8-digit hash>	Wird von der AMS Logging & Monitoring-Infrastruktur in Ihrem AMS-Konto verwendet, um Amazon RDS-Ereignisse an Amazon CloudWatch Events weiterzuleiten.
AMS-Überwachung- - AWSManaged ServicesRedshiftMonitorin <8-digit hash>	Wird von der AMS Logging & Monitoring-Infrastruktur in Ihrem AMS-Konto übernommen, um Amazon Redshift Redshift-Ereignisse (CreateCluster und DeleteCuster) an Amazon CloudWatch Events weiterzuleiten.
ams-monitoring-infrastruc- - AWSManaged ServicesMonito <8-digit hash>	Wird von der AMS Logging & Monitoring-Infrastruktur in Ihrem AMS-Konto vorausgesetzt, um Nachrichten an Amazon Simple Notification Service zu veröffentlichen, um zu überprüfen, ob das Konto alle erforderlichen Daten meldet.
ams-opscenter-role	Wird vom AMS Notification Management System in Ihrem AMS-Konto für die AWS Systems Manager OpsItems Verwaltung der Benachrichtigungen in Ihrem Konto übernommen.
ams-opsitem-autoexecution-role	Wird vom AMS Notification Management System übernommen, um automatische Problembehebungen mithilfe von SSM-Dokumenten zur Überwachung von Warnmeldungen im Zusammenhang mit Ressourcen in Ihrem Konto durchzuführen.

Name der Rolle	Beschreibung
ams-patch-infrastructure-amspatchconfigruleroleC1- <8-digit hash>	Wird angenommen AWS Config , um die AMS-Patch-Ressourcen auszuwerten und Abweichungen in den CloudFormation Stacks zu erkennen.
ams-patch-infrastructure-amspatchcwruleopsitemams- <8-digit hash>	Von Amazon angenommen, dass EventBridge es AWS Systems Manager OpsItems für Patch-Fehler erstellt.
ams-patch-infrastructure-amspatchservicebusamspat- <8-digit hash>	Geht von Amazon davon aus EventBridge , dass es ein Ereignis an den AMS Patch Orchestrator-Ereignisbus sendet, um Benachrichtigungen über Statusänderungen in der AWS Systems Manager Wartung von Windows zu erhalten.
ams-patch-reporting-infra-amspatchreportingconfigr- <8-digit hash>	Wird verwendet AWS Config , um die AMS-Patch-Berichtsressourcen auszuwerten und Abweichungen in den Stacks zu erkennen. CloudFormation
ams-resource-tagger- - AWSManagedServicesResourceTagg <8-digit hash>	Wird von der AMS Resource Tagger-Infrastruktur in Ihrem AMS-Konto übernommen, um bei einer neuen AWS AppConfig Bereitstellung eine AWS-Config-Regeln Evaluierung durchzuführen.
ams-resource-tagger- - AWSManagedServicesResourceTagg <8-digit hash>	Wird von der AMS Resource Tagger-Infrastruktur in Ihrem AMS-Konto vorausgesetzt, um zu überprüfen, ob die erforderlichen AWS Tags für die verwalteten Ressourcen vorhanden sind.
ams-resource-tagger- - AWSManagedServicesResourceTagg <8-digit hash>	Wird davon ausgegangen, dass der Workflow AWS Systems Manager zur Behebung von AMS Resource Tagger in Ihrem AMS-Konto aufgerufen wird.

Name der Rolle	Beschreibung
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Wird von der AMS Resource Tagger Remediation-Infrastruktur in Ihrem AMS-Konto übernommen, um AWS Tags für die verwaltet en Ressourcen zu erstellen oder zu löschen.
ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash>	Wird von der AMS Resource Tagger-Infrastrukt ur in Ihrem AWS Konto zur regelmäßigen Evaluierung der AMS Config Rule vorausges etzt.
ams_os_configuration_event_rule_role- <AWS Region>	Geht davon aus EventBridge , dass Amazon Ereignisse von Ihrem Konto an den AMS OS-Konfigurationsservice EventBus in der richtigen Region weiterleitet.
mc-patch-reporting-service	Wird vom AMS-Patchdatenaggregator und Berichtsgenerator vorausgesetzt.

> **Note**
>
> Dies ist die Vorlage für die ams-access-management Rolle. Es ist der Stack, den Cloud-Architekten (CAs) beim Onboarding manuell in Ihrem Konto bereitstellen: management-role.yaml.
> Dies ist die Vorlage für die verschiedenen Zugriffsrollen und Zugriffsebenen:,,,: accelerate-roles.yaml. ams-access-read-only ams-access-operations ams-access-admin-operations ams-access-admin

Weitere Informationen zu AWS Cloud Development Kit (AWS CDK) (AWS CDK) -Bezeichnern, einschließlich Hashes, finden Sie unter Unique. IDs

AMS Accelerate Feature Services übernehmen die ams-access-adminRolle des programmatischen Zugriffs auf das Konto, allerdings mit einer Sitzungsrichtlinie, die auf den jeweiligen Feature-Service beschränkt ist (z. B. Patch, Backup, Überwachung usw.).

AMS Accelerate hält sich an branchenweit bewährte Verfahren, um die Voraussetzungen für die Einhaltung von Vorschriften zu erfüllen und aufrechtzuerhalten. Der Zugriff von AMS Accelerate auf Ihr Konto wird aufgezeichnet CloudTrail und steht Ihnen auch zur Überprüfung über die Änderungsverfolgung zur Verfügung. Informationen zu Abfragen, mit denen Sie diese Informationen abrufen können, finden Sie unterÄnderungen in Ihren AMS Accelerate-Konten verfolgen.

Verwalten des Zugriffs mit Richtlinien

Verschiedene AMS Accelerate-Support-Teams wie Operations Engineers, Cloud Architects und Cloud Service Delivery Manager (CSDMs) benötigen manchmal Zugriff auf Ihre Konten, um auf Serviceanfragen und Vorfälle zu reagieren. Ihr Zugriff wird durch einen internen AMS-Zugangsdienst geregelt, der Kontrollen wie z. B. geschäftliche Begründungen, Serviceanfragen, operative Aufgaben und Supportfälle durchsetzt. Der Standardzugriff ist schreibgeschützt, und der gesamte Zugriff wird nachverfolgt und aufgezeichnet (siehe auch). Änderungen in Ihren AMS Accelerate-Konten verfolgen

Validierung von IAM-Ressourcen

Das AMS Accelerate-Zugriffssystem übernimmt regelmäßig Rollen in Ihren Konten (mindestens alle 24 Stunden) und überprüft, ob alle unsere IAM-Ressourcen den Erwartungen entsprechen.

Um Ihre Konten zu schützen, verfügt AMS Accelerate über ein „Kanariensystem“, das das Vorhandensein und den Status der IAM-Rollen sowie der damit verbundenen Richtlinien, die oben erwähnt wurden, überwacht und Alarme sendet. In regelmäßigen Abständen übernimmt der Canary die ams-access-read-onlyRolle CloudFormation und leitet IAM-API-Aufrufe gegen Ihre Konten ein. Der Canary bewertet den Status der AMS Accelerate-Zugriffsrollen, um sicherzustellen, dass sie immer unverändert sind und. up-to-date Durch diese Aktivität werden CloudTrail Protokolle im Konto erstellt.

Der Sitzungsname AWS -Security-Token-Service (AWS STS) des Canary lautet AMS-Access-Roles-Auditor- {uuid4 ()}, wie in beschrieben, und die folgenden API-Aufrufe finden statt: CloudTrail

- API-Aufrufe von Cloud Formation: `describe_stacks()`
- IAM-API-Aufrufe:
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`

- `get_policy_version()`
- `get_role_policy()`

Reaktion auf Sicherheitsvorfälle in AMS

Sicherheit hat bei AWS Managed Services (AMS) oberste Priorität. AMS stellt Ressourcen und Kontrollen in Ihren Konten bereit, um diese zu verwalten. AWS hat ein Modell der geteilten Verantwortung: AWS verwaltet die Sicherheit der Cloud, und Sie sind für die Sicherheit in der Cloud verantwortlich. AMS schützt Ihre Daten und Vermögenswerte und trägt dazu bei, Ihre AWS Infrastruktur zu schützen, indem es Sicherheitskontrollen einsetzt und Sicherheitsprobleme aktiv überwacht. Diese Funktionen helfen Ihnen dabei, eine Sicherheitsgrundlage für Anwendungen zu schaffen, die in der AWS Cloud ausgeführt werden. AMS arbeitet im Rahmen von Security Incident Response mit Ihnen zusammen, um die Auswirkungen zu bewerten und dann auf der Grundlage von Best-Practice-Empfehlungen Eindämmungs- und Abhilfemaßnahmen durchzuführen.

Wenn eine Abweichung vom Ausgangswert auftritt, z. B. durch eine Fehlkonfiguration oder eine Änderung externer Faktoren, müssen Sie reagieren und Nachforschungen anstellen. Um dies erfolgreich zu tun, müssen Sie die grundlegenden Konzepte der Reaktion auf Sicherheitsvorfälle in Ihrer AMS-Umgebung verstehen. Sie müssen auch die Anforderungen für die Vorbereitung, Schulung und Schulung von Cloud-Teams verstehen, bevor Sicherheitsprobleme auftreten. Es ist wichtig, die Kontrollen und Funktionen zu kennen, die Sie verwenden können, Reaktionspläne für häufig auftretende Sicherheitsprobleme wie die Kompromittierung von Benutzerkonten oder den Missbrauch privilegierter Konten zu erstellen und Abhilfemaßnahmen zu identifizieren, die mithilfe von Automatisierung die Reaktionsgeschwindigkeit und Konsistenz verbessern. Darüber hinaus müssen Sie Ihre Compliance- und regulatorischen Anforderungen im Zusammenhang mit dem Aufbau eines Programms zur Reaktion auf Sicherheitsvorfälle zur Erfüllung dieser Anforderungen verstehen.

Die Reaktion auf Sicherheitsvorfälle kann komplex sein, aber durch die Implementierung eines iterativen Ansatzes können Sie den Prozess vereinfachen und es dem Incident-Response-Team ermöglichen, durch frühzeitige und kontinuierliche Erkennung und Reaktion alle Beteiligten zufrieden zu stellen. In diesem Leitfaden stellen wir Ihnen die Methodik vor, die AMS für die Reaktion auf Vorfälle verwendet, die AMS Responsibility Matrix (RACI), wie Sie sich auf ein Sicherheitsereignis vorbereiten können, wie Sie AMS bei Sicherheitsvorfällen einbeziehen können, und einige der von AMS verwendeten Runbooks zur Reaktion auf Vorfälle.

So funktioniert AMS Security Incident Response

AWS Managed Services entspricht dem NIST 800-61 Leitfaden zur Behandlung von Sicherheitsvorfällen für die Reaktion auf Sicherheitsvorfälle. Durch die Ausrichtung an diesem Industriestandard bieten wir einen konsistenten Ansatz für das Management von Sicherheitsereignissen und halten uns an bewährte Verfahren bei der Sicherung und Reaktion auf Sicherheitsvorfälle in Ihrer Cloud.

Lebenszyklus der Reaktion auf Vorfälle

Wenn die Erkennung eine Sicherheitswarnung identifiziert und generiert oder Sie Sicherheitsunterstützung anfordern, stellt das AWS Managed Services Operations Team sicher, dass eine zeitnahe Untersuchung stattfindet, führt Automatisierungen zur Datenerfassung, Triage und Analyse durch, informiert Sie über die Analyse, führt Untersuchungen und alle Eindämmungsaktivitäten durch und veröffentlicht dann die Ereignisanalyse.

Die während der Reaktion auf den Vorfall durchgeführten Aktivitäten zur Erfassung, Auswertung, Analyse und Eindämmung von Daten variieren je nach Art des untersuchten Sicherheitsereignisses. Beispiele für Workflows zur Reaktion auf Sicherheitsvorfälle für ausgewählte Szenarien finden Sie am Ende dieses Dokuments.

Bei Vorfällen bestimmt AMS dynamisch die richtige Vorgehensweise, was dazu führen kann, dass dokumentierte Schritte gegebenenfalls neu angeordnet oder umgangen werden, um sicherzustellen, dass das richtige Ergebnis eintritt.

Vorbereitung

Im Zuge der Weiterentwicklung der Bedrohungslandschaft erweitert AMS kontinuierlich die Erkennungs- und Reaktionsmöglichkeiten. Wenn neue Erkennungen hinzukommen, integriert AMS die Warnmeldungen dieser neuen Erkennungen in die Erkennungs- und Reaktionsplattform. Die Sicherheitsmitarbeiter von AMS sind darauf geschult, Ihnen während des gesamten Sicherheitsvorfall-Reaktionszyklus Nachforschungen anzustellen und mit Ihnen zusammenzuarbeiten.

Aufgrund dieses partnerschaftlichen Ansatzes ist es wichtig, dass Ihre Sicherheits- und Anwendungsteams bereit sind, mit AMS zusammenzuarbeiten, um Sicherheitsvorfälle zu behandeln, sobald diese Ereignisse eintreten. Diese Dokumentation erklärt, was Sie bei einem Sicherheitsereignis erwartet, und hilft Ihnen, sich auf eine schnelle Reaktion vorzubereiten, wenn ein Sicherheitsvorfall eintritt.

Diese Dokumentation verwendet die NIST 800-61-Definition eines Ereignisses als jedes beobachtbare Ereignis in einem System oder Netzwerk und als Vorfall als Verstoß oder unmittelbar drohende Verletzung von Richtlinien, Richtlinien zur akzeptablen Nutzung oder Standardsicherheitspraktiken.

Checkliste für die Vorbereitung

Arbeiten Sie die folgende Checkliste mit Ihrem AMS Cloud Solution Delivery Manager (CSDM) und AMS Cloud Architect (CA) durch:

- Verstehen Sie, welche Workloads in welchen Konten ausgeführt werden.
- Verstehen Sie, welche internen Teams für die verschiedenen Workloads verantwortlich sind, und kennzeichnen Sie sie entsprechend in den Workloads.
- Pflegen Sie intern die Kontaktdaten anderer Teams, die möglicherweise bei der Untersuchung eines Sicherheitsvorfalls und bei Entscheidungen zur Eindämmung benötigt werden.
- Vergewissern Sie sich, dass die Sicherheitskontakte auf dem neuesten Stand sind und allen verwalteten AWS Konten hinzugefügt wurden. Die Kontakte werden pro Konto verwaltet.
- Informieren Sie sich darüber, wie Sie AMS über einen Sicherheitsvorfall informieren können, und machen Sie sich mit dem Schweregrad und den zu erwartenden Reaktionszeiten vertraut.
- Stellen Sie sicher, dass eingehende Sicherheitsbenachrichtigungen an die entsprechenden Personen und Systeme wie Pager oder Ihr Security Operations Center weitergeleitet werden.
- Erfahren Sie, welche Protokollquellen Ihnen zur Verfügung stehen, wo diese in Ihren Konten gespeichert sind und wer Zugriff darauf hat.
- Erfahren Sie, wie Sie CloudWatch Insights verwenden können, um Logs bei Untersuchungen abzufragen.
- Machen Sie sich mit den Containment-Optionen vertraut, die Ihnen je nach Ressource (EC2, IAM, S3 usw.) zur Verfügung stehen, und welche Auswirkungen dies auf Ihre Workload-Verfügbarkeit hat, wenn Sie sich im Containment befinden.

Detect

Während der Verwaltung Ihrer AWS Konten überwacht AMS anhand von Daten, die aus Erkennungsquellen und Kontrollen gesammelt wurden, einschließlich, aber nicht beschränkt auf Amazon, Amazon, VPC Flow Logs, Amazon Macie und interne Threat Intelligence-Feeds von Amazon CloudWatch, Amazon, Amazon, Amazon, Amazon, Amazon, Amazon, Amazon GuardDuty,

Amazon, auf Anomalien im Hinblick auf Benutzerverhalten, Kontoaktivitäten AWS Config und potenzielle Sicherheitsereignisse.

AMS verwendet sowohl native AWS Dienste als auch andere Erkennungstechnologien, um auf Sicherheitsereignisse zu reagieren, die verursacht werden durch:

- Typen zur Suche nach Konformität bei der Config
- GuardDuty Typen finden
- Macie Findet Typen
- DNS-Firewall-Ereignisse für Amazon Route 53 Resolver
- AMS-Sicherheitsereignisse (Cloud-Watch-Alarme)

Im Zuge der Weiterentwicklung von Diensten, Produkten und Bedrohungsökosystemen kommen weitere Erkenntnisse hinzu.

Melden Sie Sicherheitsereignisse an AMS

Melden Sie einen Vorfall über das AMS Support Portal oder Support Center, um AMS über einen Sicherheitsvorfall zu informieren oder um Untersuchungen anzufordern.

Analysieren

Nachdem ein Sicherheitsereignis identifiziert und gemeldet wurde, besteht der nächste Schritt darin, zu analysieren, ob es sich bei dem gemeldeten Ereignis um einen falsch positiven oder einen echten Vorfall handelt. AMS verwendet Automatisierungs- und manuelle Ermittlungstechniken, um mit Sicherheitsereignissen umzugehen. Die Analyse umfasst die Untersuchung von Protokollen aus verschiedenen Erkennungsquellen wie Netzwerkdatenverkehrsprotokollen, Hostprotokollen, CloudTrail Ereignissen, AWS Serviceprotokollen usw. Bei der Analyse wird auch nach Mustern gesucht, die durch Korrelation ein anomales Verhalten zeigen.

Ihre Partnerschaft ist erforderlich, um den spezifischen Kontext der Kontoumgebung zu verstehen und herauszufinden, was für Ihr Konto und Ihre Workloads normal ist. Auf diese Weise kann AMS eine Anomalie schneller erkennen und schneller auf Vorfälle reagieren.

Bearbeitung von Mitteilungen von AMS über Sicherheitsereignisse

AMS hält Sie während der Untersuchung auf dem Laufenden, indem es Ihre Sicherheitskontakte über ein Incident-Ticket kontaktiert. Ihr AMS Cloud Service Delivery Manager (CSDM) und Ihr

AMS Cloud Architect (CA) sind die Ansprechpartner, an die Sie sich während einer aktiven Sicherheitsuntersuchung für jegliche Kommunikation wenden können.

Die Kommunikation umfasst die automatische Benachrichtigung, wenn eine Sicherheitswarnung generiert wird, die Kommunikation nach der Ereignisanalyse, die Einrichtung von Call Bridges und die fortlaufende Übermittlung von Artefakten wie Protokolldateien, Snapshots infizierter Ressourcen sowie die Übermittlung der Untersuchungsergebnisse an Sie während des Sicherheitsereignisses.

Die Standardfelder, die in AMS-Sicherheitswarnmeldungen enthalten sind, sind unten aufgeführt. Diese Felder bieten Ihnen Informationen, sodass Sie Ereignisse zur Behebung an die entsprechenden Teams in Ihrer Organisation weiterleiten können.

- Typ wird gesucht
- Identifier finden (sofern relevant)
- Schweregrad ermitteln
- Beschreibung finden
- Datum und Uhrzeit der Suche wurden erstellt
- AWS Konto-ID
- Region (wo relevant)
- AWS Ressourcen (IAMuser/role/policy, S3 EC2, EKS)

Je nach Finding-Typ werden zusätzliche Felder bereitgestellt. EKS-Ergebnisse enthalten beispielsweise Pod-, Container- und Cluster-Details.

Enthalten

Der Eindämmungsansatz von AMS basiert auf einer Partnerschaft mit Ihnen. Sie kennen Ihr Unternehmen und wissen, welche Auswirkungen Containment-Aktivitäten wie Netzwerkisolierung, Deprovisionierung von IAM-Benutzern oder -Rollen, Neuaufbau von Instanzen usw. haben können.

Ein wesentlicher Bestandteil der Eindämmung ist die Entscheidungsfindung. Fahren Sie beispielsweise ein System herunter, isolieren Sie eine Ressource vom Netzwerk, schalten Sie den Zugriff aus oder beenden Sie Sitzungen. Diese Entscheidungen sind leichter zu treffen, wenn es vorher festgelegte Strategien und Verfahren gibt, um den Vorfall einzudämmen. AMS stellt die Eindämmungsstrategie bereit und implementiert dann die Lösung, nachdem Sie das mit der Implementierung der Eindämmungsmaßnahmen verbundene Risiko berücksichtigt haben.

Je nach den zu analysierenden Ressourcen gibt es unterschiedliche Eindämmungsoptionen. AMS geht davon aus, dass bei der Untersuchung eines Vorfalls mehrere Eindämmungsarten gleichzeitig eingesetzt werden. Zu diesen Beispielen gehören unter anderem:

- Wenden Sie Schutzregeln an, um unbefugten Datenverkehr zu blockieren (Sicherheitsgruppe, NACL, WAF-Regeln, SCP-Regeln, Liste verweigern, Signaturaktion auf Quarantäne oder Sperren festlegen)
- Isolierung von Ressourcen
- Netzwerkisolierung
- Deaktivierung von IAM-Benutzern, -Rollen und -Richtlinien
- Ändern/Reduzieren der IAM-Benutzer- und Rollenrechte
- Rechenressourcen beenden, aussetzen oder löschen
- Einschränkung des öffentlichen Zugriffs auf die betroffene Ressource
- Rotierende Zugriffsschlüssel, API-Schlüssel und Passwörter
- Löschen offengelegter Anmeldeinformationen und vertraulicher Informationen

AMS empfiehlt Ihnen, die Art der Eindämmungsstrategien für jede Art von schwerwiegenden Vorfällen, die ihrem Risikoappetit entsprechen, zu prüfen. Die Kriterien sind klar dokumentiert, um im Falle eines Vorfalls die Entscheidungsfindung zu erleichtern. Zu den Kriterien für die Festlegung der geeigneten Strategie gehören:

- Mögliche Schäden an Ressourcen
- Bewahrung von Beweismitteln
- Nichtverfügbarkeit von Diensten (z. B. Netzwerkkonnektivität, Dienste, die für externe Parteien bereitgestellt werden)
- Zeit und Ressourcen, die für die Umsetzung der Strategie benötigt wurden
- Wirksamkeit der Strategie (z. B. teilweise Eindämmung, vollständige Eindämmung)
- Dauerhaftigkeit der Lösung (z. B. Entscheidungen zwischen Einwegtüren und Einwegtüren)
- Dauer der Lösung (z. B. Notfalllösung, die innerhalb von vier Stunden entfernt wird, vorübergehende Behelfslösung, die innerhalb von zwei Wochen entfernt wird, dauerhafte Lösung).
- Wenden Sie Sicherheitskontrollen an, die Sie aktivieren können, um das Risiko zu verringern und Zeit für die Definition und Implementierung einer effektiveren Eindämmung zu gewinnen.

Die Geschwindigkeit der Eindämmung ist entscheidend. AMS empfiehlt einen schrittweisen Ansatz, um eine effiziente und effektive Eindämmung durch strategische Strategien für kurz- und langfristige Konzepte zu erreichen.

Verwenden Sie diesen Leitfaden, um Ihre Eindämmungsstrategie zu überdenken, die je nach Ressourcentyp unterschiedliche Techniken beinhaltet.

- Eindämmungsstrategie
  - Kann AMS den Umfang des Sicherheitsvorfalls ermitteln?
    - Falls ja, identifizieren Sie alle Ressourcen (Benutzer, Systeme, Ressourcen).
    - Falls nein, untersuchen Sie dies parallel zur Ausführung des nächsten Schritts für identifizierte Ressourcen.
  - Kann die Ressource isoliert werden?
    - Falls ja, fahren Sie mit der Isolierung der betroffenen Ressourcen fort.
    - Falls nein, arbeiten Sie mit den Systembesitzern und Managern zusammen, um weitere Maßnahmen zur Eindämmung des Problems zu ergreifen.
  - Sind alle betroffenen Ressourcen von den nicht betroffenen Ressourcen isoliert?
    - Falls ja, fahren Sie mit dem nächsten Schritt fort.
    - Falls nein, isolieren Sie die betroffenen Ressourcen weiter, bis eine kurzfristige Eindämmung erreicht ist, um zu verhindern, dass der Vorfall weiter eskaliert.
- Systemsicherung
  - Wurden für weitere Analysen Sicherungskopien der betroffenen Systeme erstellt?
  - Werden die forensischen Kopien verschlüsselt und an einem sicheren Ort gespeichert?
    - Falls ja, fahren Sie mit dem nächsten Schritt fort.
    - Falls nein, verschlüsseln Sie die forensischen Bilder und speichern Sie sie an einem sicheren Ort, um eine versehentliche Verwendung, Beschädigung und Manipulation zu verhindern.

Ausrotten

Nach der Eindämmung eines Vorfalls kann eine Beseitigung erforderlich sein, um die Bedrohungsquellen vollständig zu eliminieren und das System zu schützen, bevor Sie mit der nächsten Wiederherstellungsphase fortfahren. Zu den Maßnahmen zur Beseitigung können das Löschen von Malware und das Entfernen gefährdeter Benutzerkonten sowie die Identifizierung und Behebung aller ausgenutzten Sicherheitslücken gehören. Bei der Beseitigung ist es wichtig, alle

betroffenen Konten, Ressourcen und Instanzen in der Umgebung zu identifizieren, damit sie behoben werden können.

Es hat sich bewährt, dass die Beseitigung und Wiederherstellung schrittweise erfolgt, sodass die Maßnahmen zur Behebung priorisiert werden. Bei größeren Vorfällen kann die Wiederherstellung Monate dauern. In den ersten Phasen muss die Absicht bestehen, die allgemeine Sicherheit durch relativ schnelle (Tage bis Wochen) wichtige Änderungen zu erhöhen, um future Vorfälle zu verhindern. Die späteren Phasen müssen sich auf längerfristige Änderungen (z. B. Änderungen der Infrastruktur) und laufende Arbeiten konzentrieren, um das Unternehmen so sicher wie möglich zu halten.

Bei einigen Vorfällen ist die Beseitigung entweder nicht erforderlich oder sie erfolgt während der Wiederherstellung.

Berücksichtigen Sie dabei Folgendes:

- Kann das System erneut erstellt und anschließend mit Patches oder anderen Gegenmaßnahmen abgesichert werden, um das Risiko von Angriffen zu verhindern oder zu verringern?
- Werden alle von den Angreifern hinterlassenen Schadsoftware und anderen Artefakte entfernt und die betroffenen Systeme gegen weitere Angriffe abgesichert?

Wiederherstellung

AMS arbeitet mit Ihnen zusammen, um den normalen Betrieb der Systeme wiederherzustellen, sicherzustellen, dass die Systeme normal funktionieren, und (falls zutreffend) Sicherheitslücken zu beheben, um ähnliche Vorfälle zu verhindern.

Berücksichtigen Sie dabei Folgendes:

- Wurden die betroffenen Systeme gepatcht und sind sie gegen den jüngsten Angriff und mögliche zukünftige Angriffe abgesichert?
- An welchem Tag und zu welcher Uhrzeit können die betroffenen Systeme wieder in Betrieb genommen werden?
- Welche Tools werden Sie verwenden, um zu testen, zu überwachen und sicherzustellen, dass die Systeme, die Sie in Betrieb nehmen, nicht anfällig für die ersten Angriffstechniken sind?

Bericht nach dem Vorfall

Nach dem Ereignis führt AMS einen Ermittlungsprozess zur Überprüfung aller Sicherheitsvorfälle durch. Und AMS leitet einen Prozess zur Fehlerkorrektur (COE) ein, um Sicherheitsvorfälle zu beheben, die durch ein System oder einen verfahrenstechnischen Fehler verursacht wurden, der plausibel verbesserungswürdig ist. AMS arbeitet mit Ihnen zusammen, um die Erfahrung mit Sicherheitsuntersuchungen kontinuierlich zu verbessern. Der COE-Prozess hilft AMS dabei, die Faktoren zu identifizieren, die sich auf die Kunden auswirken, und verknüpft diese Ursachen mit den nächsten Maßnahmen, die verhindern können, dass sich ähnliche Ereignisse wiederholen, oder trägt dazu bei, die Dauer oder das Ausmaß der Auswirkungen zu verringern.

Das Verfahren zur Überprüfung von Sicherheitsvorfällen befasst sich mit den folgenden Punkten, um Verbesserungsmöglichkeiten zu ermitteln:

- Wie lange verging zwischen dem Beginn des Vorfalls, der Entdeckung des Vorfalls, der ersten Folgenabschätzung und den einzelnen Phasen der Bearbeitung des Vorfalls (z. B. Eindämmung, Behebung)?
- Wie lange hat es gedauert, bis das Incident-Response-Team auf den ersten Bericht über den Vorfall reagiert hat?
- Wie lange hat es gedauert, eine erste Folgenabschätzung durchzuführen?
- War das vermeidbar und wie? Gibt es ein Tool oder einen Prozess, der dies hätte verhindern können?
- Hätten wir das früher erkennen können und wie?
- Was hätte die Untersuchung beschleunigen können?
- Wurden die dokumentierten Verfahren zur Reaktion auf Vorfälle eingehalten? Waren sie ausreichend?
- Wurde der Informationsaustausch mit anderen Interessenträgern rechtzeitig durchgeführt? Wie könnte er verbessert werden?
- War die Zusammenarbeit mit anderen Teams (AWS Sicherheit, Kundenteams, AWS Entwicklungsteam und Kundensicherheitsteam) effektiv? Wenn nicht, was könnte verbessert werden?
- Welche Vorbereitungsschritte fehlten, die hätten helfen können: Eskalationsmatrizen, RACIs, Modelle der geteilten Verantwortung und so weiter? Müssen Runbooks aktualisiert werden?

- Was war der Unterschied zwischen der ursprünglichen Folgenabschätzung und der endgültigen Folgenabschätzung? Was können wir tun, um die Genauigkeit der Bewertungen zu einem früheren Zeitpunkt der Reaktion auf Vorfälle zu verbessern?
- Welche Maßnahmen ergeben sich aus den gewonnenen Erkenntnissen?

Runbooks zur Reaktion auf Sicherheitsvorfälle in AMS

Dieser Abschnitt enthält zwei Runbooks:

- Reaktion auf Root-Benutzeraktivitäten
- Reaktion auf Malware-Ereignisse

Reaktion auf Root-Benutzeraktivitäten

Der Root-Benutzer ist der Superuser in Ihrem AWS Konto. Beachten Sie, dass AMS die Root-Nutzung überwacht. Es hat sich bewährt, den Root-Benutzer nur für die wenigen Aufgaben zu verwenden, für die er erforderlich ist, z. B. um Ihre Kontoeinstellungen zu ändern, den AWS Identity and Access Management (IAM-) Zugriff auf die Abrechnung und das Kostenmanagement zu aktivieren, Ihr Root-Passwort zu ändern und die Multi-Faktor-Authentifizierung (MFA) zu aktivieren. Weitere Informationen finden Sie unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind.

Weitere Informationen darüber, wie AMS über die geplante Root-Nutzung informiert werden kann, finden Sie unter Wann und wie wird das Root-Konto in AMS verwendet?

Wenn Root-Benutzeraktivitäten erkannt werden, entweder fehlgeschlagene Anmeldeversuche, die auf einen Brute-Force-Angriff hinweisen könnten, oder Aktivitäten im Konto nach einer erfolgreichen Anmeldung, wird ein Ereignis generiert und ein Vorfall an Ihre definierten Sicherheitskontakte gesendet.

AWS Managed Services Operations untersucht ungeplante Root-Benutzeraktivitäten, führt Datenerfassung, Triage und Analyse durch und führt Eindämmungsaktivitäten auf Ihre Anweisung hin durch, gefolgt von einer Analyse nach dem Ereignis.

Wenn Sie das AMS Advanced-Betriebsmodell nutzen, erhalten Sie zusätzliche Mitteilungen von den Technikern von AMS CSDM und AMS Ops, die ungeplante Root-Benutzeraktivitäten bestätigen, da AMS für die Sicherung der Root-Benutzeranmeldedaten verantwortlich ist. AMS untersucht die Root-Benutzeraktivitäten, bis Sie einen weiteren Weg bestätigt haben.

Vorbereitung

Informieren Sie AMS über jede geplante Nutzung des Root-Benutzers, indem Sie eine AMS-Serviceanfrage mit den Daten und Zeiten des geplanten Ereignisses einreichen, um unnötige Maßnahmen zur Reaktion auf Vorfälle zu vermeiden.

Nehmen Sie regelmäßig Kontakt GameDays mit AMS auf, um die Prozesse von AMS zur Reaktion auf Kundenvorfälle zu überprüfen, Mitarbeiter und Systeme auf dem neuesten Stand zu halten, und bauen Sie gemeinsam mit verantwortlichen Personen ein gutes Gedächtnis auf, um eine schnellere Reaktion auf Vorfälle zu erreichen.

Phase A: Erkennen

AMS überwacht die Konten anhand von Erkennungsquellen, einschließlich GuardDuty AMS-Überwachung, auf Root-Aktivitäten.

Wenn Sie AMS Accelerate verwenden, reagiert das Betriebsmodell auf den Vorfall und fordert eine Untersuchung auf unerwartete Root-Benutzeraktivitäten an. In diesem Fall initiiert AMS Operations das Runbook für kompromittierte Konten.

Wenn Sie AMS Advanced verwenden, reagiert das Betriebsmodell auf den Vorfall oder informiert das CSDM über geplante Root-Benutzeraktivitäten, um eine aktive Untersuchung zur Kontengefährdung zu beenden.

Phase B: Analysieren

AMS führt eine gründliche Untersuchung der Root-Benutzerereignisse durch, wenn festgestellt wird, dass die Aktivität nicht autorisiert ist. Sowohl mithilfe von Automatisierungen als auch mithilfe des AMS Security Response Teams werden Protokolle und Ereignisse auf Anomalien und unerwartetes Verhalten von Root-Benutzern analysiert. Mithilfe von Protokollen können Sie feststellen, ob die Aktivität unbekannt ist, ob es sich um ein autorisiertes Root-Benutzer-Ereignis handelt oder ob weitere Untersuchungen erforderlich sind.

Zu den Informationen, die während der Untersuchung zur Unterstützung interner Kontrollen zur Verfügung gestellt wurden, gehören unter anderem:

- Kontoinformationen: Für welches Konto wurde das Root-Konto verwendet?
- E-Mail-Adresse für den Root-Benutzer: Jeder Root-Benutzer ist mit einer E-Mail-Adresse aus Ihrer Organisation verknüpft

- Authentifizierungsdetails: Wo und wann hat der Root-Benutzer auf Ihre Umgebung zugegriffen?
- Aktivitätsaufzeichnungen: Was hat der Benutzer getan, als er als Root angemeldet war? Diese Aufzeichnungen liegen in Form von CloudWatch Ereignissen vor. Zu verstehen, wie man diese Protokolle liest, hilft bei der Untersuchung.

Es hat sich bewährt, dass Sie bereit sind, die Analyseinformationen zu erhalten, und einen Plan haben, wie Sie autorisierte Ansprechpartner für Konten in Ihrem Unternehmen erreichen können. Da Stammbenutzer nicht als Einzelpersonen benannt werden, können Fragen schnell intern weitergeleitet werden, wenn Sie feststellen, wer Zugriff auf die für das Konto verwendete Stamm-E-Mail-Adresse innerhalb Ihrer Organisation hat.

Phase C: Eindämmen und Ausrotten

AMS arbeitet mit Ihren Sicherheitsteams zusammen, um die Eindämmung auf Anweisung Ihrer autorisierten Ansprechpartner für Kundensicherheit durchzuführen. Zu den Eindämmungsoptionen gehören:

- Rotation der entsprechenden Anmeldeinformationen und Schlüssel.
- Beenden aktiver Sitzungen mit Konten und Ressourcen.
- Beseitigung der erstellten Ressourcen.

Während der Eindämmungsmaßnahmen arbeitet AMS eng mit Ihrem Sicherheitsteam zusammen, um sicherzustellen, dass Störungen Ihrer Workloads so gering wie möglich gehalten werden und die Root-Zugangsdaten angemessen gesichert sind.

Nach Abschluss des Eindämmungsplans arbeiten Sie mit dem AMS Operations Team zusammen, um alle erforderlichen Wiederherstellungsmaßnahmen durchzuführen.

Bericht nach dem Vorfall

Bei Bedarf leitet AMS den Überprüfungsprozess der Untersuchung ein, um alle gewonnenen Erkenntnisse zu ermitteln. Im Rahmen der Durchführung eines COE teilt AMS den betroffenen Kunden alle relevanten Ergebnisse mit, um ihnen zu helfen, ihren Prozess zur Reaktion auf Vorfälle zu verbessern.

AMS dokumentiert alle endgültigen Einzelheiten der Untersuchung, erfasst die entsprechenden Kennzahlen und meldet den Vorfall dann allen internen Teams von AMS, die Informationen benötigen, einschließlich der von Ihnen zugewiesenen CSDM und CA.

Reaktion auf Malware-Ereignisse

EC2 Amazon-Instances werden verwendet, um eine Vielzahl von Workloads zu hosten, darunter Software von Drittanbietern und individuell entwickelte Software, die von Anwendungsteams innerhalb von Organisationen bereitgestellt wird. AMS stellt Images bereit und ermutigt Sie dazu, Ihre Workloads auf Images bereitzustellen, die von AMS fortlaufend gepatcht und gewartet werden.

Während des Betriebs von Instances überwacht AMS mithilfe einer Vielzahl von Sicherheitserkennungskontrollen, darunter Amazon, Network Traffic und interne Threat Intelligence-Feeds von Amazon GuardDuty, auf Verhaltens- oder Aktivitätsanomalien.

AMS überwacht auch GuardDuty Malware-Ergebnisse. Diese sind sowohl für AMS Advanced als auch für AMS Accelerate verfügbar, sofern sie aktiviert sind. Weitere Informationen finden Sie unter Malware-Schutz bei Amazon GuardDuty.

> **Note**
>
> Wenn Sie sich für Bring Your Own EPS entschieden haben, unterscheidet sich das Verfahren zur Reaktion auf Vorfälle von dem, was auf dieser Seite beschrieben wird. Weitere Informationen finden Sie in der Dokumentation, auf die verwiesen wird.

Wenn Malware erkannt wird, wird ein Vorfall erstellt und Sie werden darüber informiert. Auf diese Benachrichtigung folgen alle aufgetretenen Behebungsmaßnahmen. AMS Operations untersucht, führt Datenerfassung, Sortierung und Analyse durch und führt dann auf Ihre Anweisung hin Eindämmungsmaßnahmen durch, gefolgt von Analysen nach dem Ereignis.

Phase A: Erkennen

AMS überwacht Ereignisse auf Instanzen mit. GuardDuty AMS bestimmt die geeigneten Anreicherungs- und Triage-Aktivitäten, um Ihnen dabei zu helfen, Entscheidungen zur Eindämmung oder Risikoakzeptanz auf der Grundlage des Befundes oder der Art der Warnung zu treffen.

Die Datenerfassung erfolgt auf der Grundlage des Ergebnistyps. Bei der Datenerhebung werden mehrere Datenquellen innerhalb und außerhalb des betroffenen Kontos abgefragt, um sich ein Bild von der beobachteten Aktivität oder den besorgniserregenden Konfigurationen zu machen.

AMS korreliert die Ergebnisse mit allen anderen Alarmen und Warnmeldungen oder Telemetriedaten von allen betroffenen Konten oder AMS-Bedrohungsinformationsplattformen.

Phase B: Analysieren

Nachdem die Daten gesammelt wurden, werden sie analysiert, um mögliche Aktivitäten oder besorgniserregende Indikatoren zu identifizieren. In dieser Phase der Untersuchung arbeitet AMS mit Ihnen zusammen, um Geschäfts- und Domänenwissen über die Instanzen und Workloads zu integrieren, damit Sie besser verstehen, was erwartet wird und was ungewöhnlich ist.

Zu den Informationen, die während der Untersuchung zur Unterstützung interner Kontrollen zur Verfügung gestellt wurden, gehören unter anderem:

- Kontoinformationen: Auf welchem Konto wurde die Malware-Aktivität beobachtet?
- Instanzdetails: Welche Instanz (en) sind von den Malware-Ereignissen betroffen?
- Zeitstempel des Ereignisses: Wann wurde die Warnung ausgelöst?
- Informationen zur Arbeitslast: Was läuft auf der Instance?
- Malware-Details, falls relevant: Malware-Familien und Open-Source-Informationen zu der Malware.
- Benutzer- oder Rollendetails: Welche Benutzer oder Rollen sind von der Aktivität betroffen und an der Aktivität beteiligt?
- Aktivitätsaufzeichnungen: Welche Aktivitäten werden auf der Instance aufgezeichnet? Diese liegen in Form von CloudWatch Ereignissen und Systemereignissen aus der Instanz vor. Wenn Sie wissen, wie diese Protokolle gelesen werden, können Sie sie leichter untersuchen
- Netzwerkaktivität: Welche Endpunkte stellen eine Verbindung zu der Instance her, mit wem stellt die Instance eine Verbindung her und was ist die Traffic-Analyse?

Es hat sich bewährt, darauf vorbereitet zu sein, Ermittlungsinformationen zu erhalten, und einen Plan zu haben, wie Sie die entsprechenden Kontaktstellen für Accounts, Instances und Workloads innerhalb Ihres Unternehmens kontaktieren können. Wenn Sie Ihre Netzwerktopologie und die erwartete Verbindung kennen, können Sie die Folgenabschätzung beschleunigen. Kenntnisse über geplante Penetrationstests in der Umgebung und aktuelle Implementierungen, die von Anwendungsbesitzern durchgeführt wurden, können die Untersuchung ebenfalls beschleunigen.

Wenn Sie feststellen, dass die Aktivität geplant und autorisiert ist, wird der Vorfall aktualisiert und die Untersuchung abgeschlossen. Wenn der Kompromiss bestätigt wird, legen Sie und AMS den geeigneten Eindämmungsplan fest.

Phase C: Eindämmen und Ausrotten

AMS arbeitet mit Ihnen zusammen, um auf der Grundlage der gesammelten Daten und der bekannten Informationen geeignete Maßnahmen zur Eindämmung zu ermitteln. Zu den Eindämmungsoptionen gehören unter anderem:

- Aufbewahrung von Daten durch Schnappschüsse
- Änderung der Netzwerkregeln zur Begrenzung des Datenverkehrs innerhalb oder außerhalb von Instanzen
- Änderung der SCP-, IAM-Benutzer- und Rollenrichtlinien zur Beschränkung des Zugriffs
- Instanzen beenden, aussetzen oder ausschalten
- Beenden aller dauerhaften Verbindungen
- Rotieren der entsprechenden Anmeldeinformationen/Schlüssel

Wenn Sie sich dafür entscheiden, eine Eradikationsaktivität gegen die Instance durchzuführen, unterstützt Sie AMS dabei, dies zu erreichen. Zu den Optionen gehören, sind aber nicht beschränkt auf:

- Unerwünschte Software entfernen
- Neuaufbau der Instanz aus einem sauberen, vollständig gepatchten Image und erneutes Bereitstellen von Anwendungen und Konfiguration
- Wiederherstellung der Instanz aus einem früheren Backup
- Bereitstellen von Anwendungen und Diensten auf einer anderen Instanz innerhalb Ihres Kontos, die möglicherweise zum Hosten der Workloads geeignet ist.

Es ist wichtig, vor der Wiederherstellung des Dienstes festzustellen, wie die Malware übertragen und auf der Instanz ausgeführt wurde, um sicherzustellen, dass alle zusätzlichen Kontrollen angewendet werden, um ein erneutes Auftreten der Malware auf der Instanz zu verhindern. AMS stellt Ihren forensischen Partnern oder Teams bei Bedarf zusätzliche Erkenntnisse oder Informationen zur Verfügung, um die Forensik zu unterstützen.

Derzeit arbeiten Sie für die Wiederherstellungsaktivitäten mit AMS Operations zusammen. AMS arbeitet eng mit Ihnen zusammen, um Unterbrechungen der Workloads zu minimieren und die Instanzen zu sichern.

Bericht nach dem Vorfall

Bei Bedarf leitet AMS die Überprüfung der Untersuchung ein, um die gewonnenen Erkenntnisse zu ermitteln. Im Rahmen der Durchführung eines COE teilt AMS Ihnen die relevanten Ergebnisse mit, damit Sie Ihren Prozess zur Reaktion auf Vorfälle verbessern können.

AMS dokumentiert die letzten Einzelheiten der Untersuchung, sammelt geeignete Kennzahlen und meldet den Vorfall den internen Teams von AMS, die Informationen benötigen, einschließlich der von Ihnen zugewiesenen CSDM und CA.

Protokollierung und Überwachung von Sicherheitsereignissen in Accelerate

Konten, die bei AMS Accelerate registriert sind, sind mit einer grundlegenden Bereitstellung von CloudWatch Ereignissen und Alarmen konfiguriert, die optimiert wurden, um Störgeräusche zu reduzieren und Hinweise auf einen echten Vorfall zu erkennen. AMS Accelerate setzt auch GuardDuty für die Kontoüberwachung ein. Weitere Informationen finden Sie unter Überwachen Sie mit GuardDuty.

Konformität mit der Konfiguration in Accelerate

AMS Accelerate hilft Ihnen dabei, Ihre Ressourcen nach hohen Standards für Sicherheit und Betriebsintegrität zu konfigurieren und die folgenden Industriestandards einzuhalten:

- Zentrum für Internetsicherheit (CIS)
- Cloud Security Framework (CSF) des Nationalen Instituts für Standards und Technologie (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Datensicherheitsstandard (DSS) der Zahlungskartenindustrie (PCI)

Wir tun dies, indem wir unseren gesamten AWS Config Compliance-Regelsatz für Ihr Konto bereitstellen, sieheBibliothek mit AMS-Konfigurationsregeln. Eine AWS Config Regel stellt die gewünschten Konfigurationen für eine Ressource dar und wird anhand von Konfigurationsänderungen an den Einstellungen Ihrer AWS Ressourcen bewertet. Jede Konfigurationsänderung löst eine große Anzahl von Regeln aus, um die Einhaltung der Vorschriften zu testen. Nehmen wir zum Beispiel an, Sie erstellen einen Amazon S3 S3-Bucket und konfigurieren ihn so, dass er öffentlich lesbar ist, was gegen die NIST-Standards verstößt. Die ams-nist-cis-

sbucket-public-read-prohibited 3-Regel erkennt den Verstoß und kennzeichnet Ihren S3-Bucket in Ihrem Konfigurationsbericht als nicht konform. Da diese Regel zur Kategorie Automatische Behebung von Vorfällen gehört, erstellt sie sofort einen Incident-Bericht, der Sie auf das Problem aufmerksam macht. Andere schwerwiegendere Regelverstöße können dazu führen, dass AMS das Problem automatisch behebt. Siehe Reaktionen auf Verstöße in Accelerate.

> **Important**
>
> Wenn Sie möchten, dass wir mehr tun, z. B. wenn Sie möchten, dass AMS einen Verstoß für Sie behebt, unabhängig von der Kategorie der Behebung, reichen Sie eine Serviceanfrage ein, in der AMS gebeten wird, die nicht konformen Ressourcen für Sie zu beheben.
> Geben Sie in der Serviceanfrage einen Kommentar wie „Im Rahmen der Behebung der AMS-Konfigurationsregel korrigieren Sie bitte Ressourcen, die keine Beschwerden haben, konfigurieren Sie die Regel *CONFIG_RULE_NAME* im Konto“ ein und fügen Sie die erforderlichen Eingaben hinzu*RESOURCE_ARNS_OR_IDs*, um den Verstoß zu beheben.
> Wenn Sie möchten, dass wir weniger tun, wenn Sie beispielsweise nicht möchten, dass wir Maßnahmen für einen bestimmten S3-Bucket ergreifen, der standardmäßig öffentlichen Zugriff erfordert, können Sie Ausnahmen erstellen, siehe. Regelausnahmen in Accelerate erstellen

Bibliothek mit AMS-Konfigurationsregeln

Accelerate stellt eine Bibliothek mit AMS-Konfigurationsregeln bereit, um Ihr Konto zu schützen. Diese Konfigurationsregeln beginnen mit`ams-`. Sie können Regeln in Ihrem Konto und deren Konformitätsstatus entweder von der AWS Config Konsole, der AWS CLI oder der AWS Config API aus einsehen. Allgemeine Informationen zur Verwendung AWS Config finden Sie unter ViewingConfiguration Compliance.

> **Note**
>
> Für Opt-In AWS-Regionen- und Gov-Cloud-Regionen stellen wir aufgrund von Regionsbeschränkungen nur einen Teil der Konfigurationsregeln bereit. Überprüfen Sie die Verfügbarkeit der Regeln in Regionen, indem Sie den Link überprüfen, der dem Identifier in der Tabelle mit den AMS Accelerate-Konfigurationsregeln zugeordnet ist.
> Sie können keine der bereitgestellten AMS-Konfigurationsregeln entfernen.

Tabelle der Regeln

Laden Sie es als ams_config_rules.zip herunter.

AMS-Konfigurationsregeln

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-guardduty-aktiviert-zentralisiert	GuardDuty	Regelmäßig	Korrigieren	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 2.2, 3.4, 8.2.1;
ams-nist-cis-vpc-flow-logs-enabled	VPC	Regelmäßig	Korrigieren	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1,10.3.2,10.3.2,10.3.10.3.4,10.3.5,10.3.6;
ams-eks-secrets-encrypted	EKS	Regelmäßig	Vorfall	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-eks-endpoint-no-öffentlich zugänglich	EKS	Regelmäßig	Vorfall	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-nist-cis-vpc-default-security-group-closed	VPC	Änderungen an der Config	Vorfall	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1.2,1.3,2.1,2.2,1.2.1,1.3.1,1.3.2.2.2.2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-iam-Passwort-Richtlinie	IAM	Regelmäßig	Vorfall	CIS: NA; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii), 164,308 (a) (4) (a), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii), 164,308 (a) (4) (a), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) 308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.1.2, 7.1.3, 7.2.1, 7.2.2;
ams-nist-cis-iam-root-access-key-check	IAM	Regelmäßig	Vorfall	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a), 164,308 (a), 164,308 (a)) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2,2,7.1.2,7.1.3,7.2.1.7.2.2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-iam-user-mfa-enabled	IAM	Regelmäßig	Vorfall	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C) ,164.312 (a) (1); PCI: 2,2,7.1.2,7.1.3,7.2.1,7.2.2;
ams-nist-cis-restricted-ssh	Sicherheitsgruppen	Änderungen an der Config	Vorfall	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2,2, 7,2,1, 8,1,4;
ams-nist-cis-restricted-gemeinsame Anschlüsse	Sicherheitsgruppen	Änderungen an der Config	Vorfall	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164,308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii)) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 2,2, 2,1,1,1,1,1.3,2, 2,2,2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-s3 account-level-public-access - Blöcke	S3	Änderungen an der Config	Vorfall	CIS: CIS.9, CIS.12, CIS.14; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164.312 (a) (1), 164.312 (e) (1); PCI: 1.2,1.2.1 ,1.3.1,1.3.1,1.3.2,1.3.4,1. 3.6,2.2,2.2.2;
ams-nist-cis-s3- bucket-public-read-prohibited	S3	Änderungen an der Config	Vorfall	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2,1,3,2 ,2,1,1.3,1.3,1.3,2,1.3,4,1, 3,6,2,2,2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-s3- bucket-public-write-prohibited	S3	Änderungen an der Config	Vorfall	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2,1,3,2 ,2,1,1.3,1.3,1.3,2,1.3,4,1, 3,6,2,2,2;
ams-nist-cis-s3 bucket-server-side-encryption - aktiviert	S3	Änderungen an der Config	Vorfall	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (c) (2) ,164.312 (e) (2) (ii); PCI: 2.2,3.4,10.5,8.2.1;
ams-nist-cis-securityhub-aktiviert	Security Hub	Regelmäßig	Vorfall	CIS: CIS.3 , CIS.4, CIS.6, CIS.12, CIS.16, CIS.19; NIST-CSF: PR.DS-5, PR.PT-1; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-ec2-Geschäftsführer instance-managed-by-systems	EC2	Änderungen an der Config	Bericht	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 2.4;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-cloudtrail-aktiviert	CloudTrail	Regelmäßig	Bericht	CIS: CIS.16, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A), 164,308 (a) (5) (ii) (C) ,164.312 (b); PCI: 10.1,10.2.1,10.2.1 ,10.2.2,10.2,10.2,10 2,3, 10,2,4, 10,2,5, 10,2,6, 10,2,7, 10,3.1, 10,3,2, 10,3,3, 10,3,4, 10,3,5, 10,3,5, 10,3,6;
ams-nist-cis-access-Tasten gedreht	IAM	Regelmäßig	Bericht	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: 2.2;
ams-nist-cis-acm-certificate-expiration-check	Certificate Manager	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.AC-5, PR.PT-4; HIPAA: NA; PCI: 4.1;
ams-nist-cis-alb- überprüfen http-to-https-redirection	ALB	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164,312 (a) (2) (iv) ,164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2.3,4.1,8.2.1;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-api- -verschlüsselt gw-cache-enabled-and	API Gateway	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	Änderungen an der Config	Bericht	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.10.3.4,10.3. 5,10.3.6,10.5.4;
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: PR.PT-1, PR.PT-5; HIPAA: 164.312 (b); PCI: 2.2;
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (e) (2) (ii); PCI: 2.2,3.4,10.5;
ams-nist-cis-cloud- -aktiviert trail-log-file-validation	CloudTrail	Regelmäßig	Bericht	CIS: CIS.6; NIST-CSF: PR.DS-6; HIPAA: 164,312 (c) (1), 164,312 (c) (2); PCI: 2.2,10.5,11.5,10.5 .2,10.5.5;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-cloudtrail-s3-dataevents-aktiviert	CloudTrail	Regelmäßig	Bericht	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A), 164.312 (b); PCI: 2.2,10.1,10.2.2,10.2.2,10.2.2,10.2.3,10.2.5,10.3.6;
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-cloudwatch-log-group-encrypted	CloudWatch	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-codebuild-project-envvar-awscred-check	CodeBuild	Änderungen an der Config	Bericht	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1;
ams-nist-cis-codebuild-überprüfen project-source-repo-url	CodeBuild	Änderungen an der Config	Bericht	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-db-instance-backup-enabled	RDS	Änderungen an der Config	Bericht	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (B); PCI: NA;
ams-nist-cis-dms-replication-not-public	DMS	Regelmäßig	Bericht	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1,1, 3,2, 3,4, 1,6, 2,2,2;
ams-nist-dynamodb-autoscaling-aktiviert	DynamoDB	Regelmäßig	Bericht	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (C); PCI: NA;
ams-nist-cis-dynamodb-Pitr-fähig	DynamoDB	Regelmäßig	Bericht	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (B); PCI: NA;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-dynamodb-throughput-Limit-Check	DynamoDB	Regelmäßig	Bericht	CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA;
ams-nist-ebs-optimized-Instanz	EBS	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: NA; HIPAA: 164.308 (a) (7) (i); PCI: NA;
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	Regelmäßig	Bericht	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1,1, 3,2, 3,4, 1,6, 2,2,2;
ams-nist-ec2- instance-detailed-monitoring-enabled	EC2	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: DE.AE-1, PR.PT-1; HIPAA: 164.312 (b); PCI: NA;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-ec2- instance-no-public-ip	EC2	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (C), 164.308 (a) (4) (ii), 164.308 (a) (4) (ii) (C), 164.308 (a) (4) (c), 164.308 (a) (4) (ii), 164.308 (a) (4) (c), 164.308 (a) (4) (ii), 164.308 (a) (4) (c), 164.308 (312 (a) (1) ,164.312 (e) (1); PCI: 1,2,1.3,1.2,1.3,1.3,1.3,2,1 .3,4,1.3,6,2,2.2;
ams-nist-cis-ec2 managedin stance-as sociation-compliance-status - prüfen	EC2	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ,164.312 (e) (1); PCI: 1,2,1,3,1.2,1.3,1,1.3,2,1.3 ,4,1.3,6,2,2.2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-ec2 managedinstance-patch-compliance-status - prüfen	EC2	Änderungen an der Config	Bericht	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164.308 (a) (5) (ii) (B); PCI: 6.2;
ams-nist-cis-eclnstanz mit 2 Stopps	EC2	Regelmäßig	Bericht	CIS: CIS.2; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: NA; PCI: NA;
ams-nist-cis-ec2- volume-in use-check	EC2	Änderungen an der Config	Bericht	CIS: CIS.2; NIST-CSF: PR.IP-1; HIPAA: NA; PCI: NA;
ams-nist-cis-efs-verschlüsselter Scheck	EFS	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1;
ams-nist-cis-eip-beigefügt	EC2	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1;
ams-nist-cis-elasticache-überprüfen redis-cluster-automatic-backup	ElastiCache	Regelmäßig	Bericht	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (B); PCI: NA;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	Regelmäßig	Bericht	CIS: CIS.14, CIS.13; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1;
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1;
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (i), 164,308 (a) (ii) (C) 164,312 (a) (1) ,164.312 (e) (1); PCI: 1,2,1,3,1.2,1,1.3,1.3,1.3,2 ,1.3,4,1.3,6,2,2.2;
ams-nist-elb-deletion-Schutz aktiviert	ELB	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii), PCI: 4.1,8.2.1;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-elb-Protokollierung aktiviert	ELB	Änderungen an der Config	Bericht	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.10.3.4,10.3. 5,10.3.6,10.5.4;
ams-nist-cis-emr-Kerberos-aktiviert	EMR	Regelmäßig	Bericht	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.10.3.4,10.3. 5,10.3.6,10.3.6.10.5.4;
ams-nist-cis-emr-master-no-public-ip	EMR	Regelmäßig	Bericht	CIS: CIS.14, CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.AC-6; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a), 164,308 (a), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.2.1;
ams-nist-cis-encrypted-Bände	EBS	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ,164.312 (e) (1); PCI: 1,2,1,3,1.2,1.3,1,1.3,2,1.3 ,4,1.3,6,2,2.2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	Regelmäßig	Bericht	CIS: CIS.12, CIS.13, CIS.16, CIS.19, CIS.3, CIS.4, CIS.6, CIS.8; NIST-CSF: DE.AE-2, DE.AE-3, DE.CM-4, DE.DP-5, ID.RA-1, ID.RA-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (5) (5) ii) (C), 164,308 (a) (6) (ii), 164,312 (b); PCI: 6.1,11.4, 5.1.2;
ams-nist-iam-group-has-users-check	IAM	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: PR.AC-4, PR.AC-1; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (4) (ii), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii), 164,308 (a) (4) (a), 164,308 (a) (4) (ii), 164,308 (a) (4) (a), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) 308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.1.2, 7.1.3, 7.2.1, 7.2.2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-iam- policy-no -statements- with -Admin- Zugang	IAM	Änderungen an der Config	Bericht	CIS: CIS.16; NIST-CSF: PR.AC-6, PR.AC-7; HIPAA: 164,308 (a) (4) (ii) (B) ,164.308 (a) (5) (ii) (D) ,164.312 (d); PCI: 8.2.3, 8.2.4, 8.2.5;
ams-nist-cis-iam-user-group-membership-check	IAM	Änderungen an der Config	Bericht	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a), 164,308 (a) (ii) (C), 164,308 (a) (4) (ii), 164,308 (a) (4) (ii) (C), 164,308 (a) (4) (c), 164,308 (a) (4) (ii), 164,308 (a) (4) (ii) (C), 164,308 312 (a) (1) ,164.312 (a) (2) (i); PCI: 2.2, 7.1.2, 7.2.1, 8.1.1;
ams-nist-cis-iam-user-no-policies-check	IAM	Änderungen an der Config	Bericht	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-7; HIPAA: 164.308 (a) (4) (ii) (B), 164.312 (d); PCI: 8.3;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-iam-user-unused-credentials-check	IAM	Regelmäßig	Bericht	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (B) ,164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 2.2,7.1.2.7.1.3,7.2.1.7.2.2;
ams-nist-cis-ec2- instances-in-vpc	EC2	Änderungen an der Config	Bericht	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164,308 (a) (3) (i) ,164.308 (a) (3) (ii) (B) ,164.308 (a) (4) (ii), 164.308 (a) (4) (ii)) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 2,2, 2,1,1,1,1,1.3,2, 2,2,2;
ams-nist-cis-internet-gateway-authorized-vpc-only	Internet Gateway	Regelmäßig	Bericht	CIS: CIS.9 , CIS.12; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-nist-cis-kms- -Löschung cmk-not-scheduled-for	KMS	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: NA; PCI: 3.5, 3.6;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-lambda-concurrency-überprüfen	Lambda	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA;
ams-nist-lambda-dlq-überprüfen	Lambda	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: NA; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (i), 164,308 (a) (ii) (C) 164,312 (a) (1) ,164.312 (e) (1); PCI: 1,2,1,3,1.2,1,1.3,1.3,1.3,2 ,1.3,4,2,2.2;
ams-nist-cis-lambda-inner-vpc	Lambda	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 2,1, 1,1, 3,1, 3,2, 3,4, 2,2,2;
ams-nist-cis-mfa- enabled-for-iam-console-Zugang	IAM	Regelmäßig	Bericht	CIS: CIS.16; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2,8.3;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	Regelmäßig	Bericht	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A), 164.312 (b); PCI: 2.2,10.1,10.2.1,10 .2.2,10.2.2,10.2.2,10.2.3,1 0.2.4,10.2.5,10.2.6,10.2.7, 10.3.3 1,10,3,2, 10,3,3, 10,3,4, 10,3,5, 10,3,6;
ams-nist-rds-enhanced-überwachungsfähig	RDS	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: PR.PT-1; HIPAA: 164.312 (b); PCI: NA;
ams-nist-cis-rds-instance-public-access-check	RDS	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1,1, 3,2, 3,4, 1,6, 2,2,2;
ams-nist-rds-multi-az-Unterstützung	RDS	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i) ,164.308 (a) (7) (ii) (C); PCI: NA;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-rds-snapshots-public-prohibited	RDS	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1,1, 3,2, 3,4, 1,6, 2,2,2;
ams-nist-cis-rds-speicherverschlüsselt	RDS	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.5, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (b) ,164.312 (b) ,164.312 (e) (2) (ii); PCI: 3.4,10.1, 10.2.1.10.2.4,10.2.4,10 0.2.5, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.5, 10,3.6, 8.2.1;
ams-nist-cis-redshift-cluster-configuration-check	RedShift	Änderungen an der Config	Bericht	CIS: CIS.6, CIS.13, CIS.5; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv) ,164.312 (b) ,164.312 (e) (2) (ii); PCI: 3.4,8.2.1,10.1,10. 2,12.1.12.3,12.1.12.3,12 0.2.4, 10.2.5, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-redshift-cluster-public-access-check	RedShift	Änderungen an der Config	Bericht	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii)) (C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1,1, 3,2, 3,4, 1,6, 2,2,2;
ams-nist-cis-redshift-require-tls-ssl	RedShift	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164,312 (a) (2) (iv), 164,312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii); PCI: 2.3,4.1;
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	Regelmäßig	Bericht	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2,8.3;
ams-nist-cis-root-account-mfa-enabled	IAM	Regelmäßig	Bericht	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2,8.3;
ams-nist-cis-s3- bucket-default-lock-enabled	S3	Änderungen an der Config	Bericht	CIS: CIS.14, CIS.13; NIST-CSF: ID.BE-5, PR.PT-5, RC.RP-1; HIPAA: NA; PCI: NA;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-s3- bucket-logging-enabled	S3	Änderungen an der Config	Bericht	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A), 164.312 (b); PCI: 2.2,10.1,10.2.2,10 .2.2,10.2.2,10.2.10.2.4,10. 2.5,10.2.7,10.3.1.10.3.12.1 3.13.4.103,5,10,3,6;
ams-nist-cis-s3- bucket-replication-enabled	S3	Änderungen an der Config	Bericht	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (B); PCI: 2.2,10.5.3;
ams-nist-cis-s3- bucket-ssl-requests-only	S3	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv) ,164.312 (c) (2) ,164.312 (e) (1) ,164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii); PCI: 2.2,4.1,8.2.1;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-s3- bucket-versioning-enabled	S3	Regelmäßig	Bericht	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.DS-6, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164,308 (a) (7) (i), 164,312 (c) (1), 164,312 (c) (2); PCI: 10,5,3;
ams-nist-cis-sagemaker-endpoint-configuration-kms-key - konfiguriert	SageMaker	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1;
ams-nist-cis-sagemaker--konfiguriert notebook-instance-kms-key	SageMaker	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1;
ams-nist-cis-sagemaker- -Zugang notebook-no-direct-internet	SageMaker	Regelmäßig	Bericht	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164,308 (a) (3) (i), 164,308 (a) (i), 164,308 (a) (ii) (C) 164,312 (a) (1) ,164.312 (e) (1); PCI: 1,2,1,3,1.2,1,1.3,1.3,1.3,2 ,1.3,4,1.3,6,2,2.2;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	Änderungen an der Config	Bericht	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA;
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	Änderungen an der Config	Bericht	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164.308 (a) (4) (ii) (B); PCI: NA;
ams-nist-cis-sns-verschlüsselt-KMS	SNS	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 8.2.1;
ams-nist-cis-vpc- -autorisierte Ports sg-open-only-to	VPC	Änderungen an der Config	Bericht	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2.2.2.2;
ams-nist-vpc-vpn-2-Tunnel nach oben	VPC	Änderungen an der Config	Bericht	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i); PCI: NA;

Regelname	Service	Auslöser	Aktion	Frameworks
ams-cis-ec2-ebs-encryption-by-default	EC2	Regelmäßig	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 2.2, 3.4, 8.2.1;
ams-cis-rds-snapshot-verschlüsselt	RDS	Änderungen an der Config	Bericht	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4, 8.2.1;
ams-cis-redshift-cluster-Wartungseinstellungen - überprüfen	RedShift	Änderungen an der Config	Bericht	CIS: CIS.5; NIST-CSF: PR.DS-4, PR.IP-1, PR.IP-4; HIPAA: 164,308 (a) (5) (ii) (A), 164,308 (a) (7) (ii) (A); PCI: 6.2;

Reaktionen auf Verstöße in Accelerate

Alle Verstöße gegen die Konfigurationsregeln werden in Ihrem Konfigurationsbericht angezeigt. Dies ist eine universelle Antwort. Abhängig von der Behebungskategorie (Schweregrad) der Regel kann AMS zusätzliche Maßnahmen ergreifen, die in der folgenden Tabelle zusammengefasst sind. Einzelheiten zum Anpassen des Aktionscodes für bestimmte Regeln finden Sie unterMaßgeschneiderte Antworten auf Ergebnisse.

Abhilfemaßnahmen

Aktionscode	AMS-Aktionen
Bericht	1. Zum Konfigurationsbericht hinzufügen
Vorfall	1. Zum Konfigurationsbericht hinzufügen 2. Automatischer Vorfallbericht in Accelerate
Abhilfe schaffen	1. Zum Konfigurationsbericht hinzufügen

Aktionscode	AMS-Aktionen
	2. Automatischer Vorfallbericht in Accelerate 3. Automatische Problembehebung in Accelerate

Zusätzliche Hilfe anfordern

> **Note**
>
> AMS kann jeden Verstoß für Sie beheben, unabhängig von der Kategorie der Behebung. Um Hilfe anzufordern, reichen Sie eine Serviceanfrage ein und geben Sie an, welche Ressourcen AMS mit einem Kommentar wie „Im Rahmen der Behebung der AMS-Konfigurationsregel korrigieren Sie bitte die Ressourcen *RESOURCE_ARNS_OR_IDs* Ressource ARNs/IDs>, die Konfigurationsregel *CONFIG_RULE_NAME* im Konto“ beheben soll, und fügen Sie die erforderlichen Eingaben hinzu, um den Verstoß zu beheben.

AMS Accelerate verfügt über eine Bibliothek mit AWS Systems Manager Automatisierungsdokumenten und Runbooks, die Sie bei der Behebung nicht richtlinienkonformer Ressourcen unterstützen.

Zum Konfigurationsbericht hinzufügen

AMS generiert einen Konfigurationsbericht, der den Compliance-Status aller Regeln und Ressourcen in Ihrem Konto verfolgt. Sie können den Bericht bei Ihrem CSDM anfordern. Sie können den Konformitätsstatus auch über die AWS Config-Konsole, die AWS CLI oder die AWS Config-API überprüfen. Ihr Konfigurationsbericht beinhaltet:

- Die wichtigsten, nicht richtlinientreuen Ressourcen in Ihrer Umgebung, um potenzielle Bedrohungen und Fehlkonfigurationen aufzudecken
- Einhaltung der Ressourcen- und Konfigurationsregeln im Laufe der Zeit
- Config von Regelbeschreibungen, Schweregrad der Regeln und empfohlene Behebungsschritte zur Behebung nicht konformer Ressourcen

Wenn eine Ressource in den Status „Nicht konform“ wechselt, wird der Ressourcenstatus (und der Regelstatus) in Ihrem Konfigurationsbericht auf „Nicht konform“ gesetzt. Wenn die Regel

zur Behebungskategorie „Nur Config Report Only“ gehört, ergreift AMS standardmäßig keine weiteren Maßnahmen. Sie können jederzeit eine Serviceanfrage erstellen, um zusätzliche Hilfe oder Problembehebung von AMS anzufordern.

Weitere Informationen finden Sie unter AWS Config Reporting.

Automatischer Vorfallbericht in Accelerate

Bei mittelschweren Regelverstößen erstellt AMS automatisch einen Vorfallbericht, um Sie darüber zu informieren, dass eine Ressource in einen nicht konformen Zustand übergegangen ist, und fragt, welche Aktionen Sie durchführen möchten. Sie haben die folgenden Optionen, wenn Sie auf einen Vorfall reagieren möchten:

- Bitten Sie AMS, die im Vorfall aufgeführten Ressourcen, die nicht den Vorschriften entsprechen, zu beheben. Anschließend versuchen wir, die nicht konforme Ressource zu beheben, und benachrichtigen Sie, sobald der zugrundeliegende Vorfall behoben wurde.
- Sie können das nicht konforme Problem manuell in der Konsole oder über Ihr automatisiertes Bereitstellungssystem (z. B. durch Aktualisierungen von CI/CD Pipeline-Vorlagen) beheben. Anschließend können Sie den Vorfall lösen. Die nicht konforme Ressource wird gemäß dem Zeitplan der Regel erneut bewertet, und wenn die Ressource als nicht konform eingestuft wird, wird ein neuer Vorfallbericht erstellt.
- Sie können sich dafür entscheiden, die nicht konforme Ressource nicht zu lösen und den Vorfall einfach zu lösen. Wenn Sie die Konfiguration der Ressource später aktualisieren, löst AWS Config eine Neubewertung aus und Sie werden erneut aufgefordert, die Nichtkonformität dieser Ressource zu bewerten.

Automatische Problembehebung in Accelerate

Die wichtigsten Regeln gehören zur Kategorie Auto Remediate. Die Nichteinhaltung dieser Regeln kann sich stark auf die Sicherheit und Verfügbarkeit Ihrer Konten auswirken. Wenn eine Ressource gegen eine dieser Regeln verstößt:

1. AMS benachrichtigt Sie automatisch mit einem Vorfallbericht.
2. AMS leitet mithilfe unserer automatisierten SSM-Dokumente eine automatische Problembehebung ein.
3. AMS aktualisiert den Vorfallbericht über Erfolg oder Misserfolg der automatisierten Problembehebung.

4. Wenn die automatische Behebung fehlgeschlagen ist, untersucht ein AMS-Techniker das Problem.

Regelausnahmen in Accelerate erstellen

Mit der Funktion für AWS-Config-Regeln Ressourcenausnahmen können Sie die Meldung bestimmter, nicht konformer Ressourcen für bestimmte Regeln unterdrücken.

> **Note**
>
> Die ausgenommenen Ressourcen werden in Ihrer AWS Config Service-Konsole immer noch als Nicht konform angezeigt. Die ausgenommenen Ressourcen werden in Konfigurationsberichten mit einem speziellen Flag angezeigt (resource_exception:true). Sie CSDMs können diese Ressourcen beim Generieren von Berichten entsprechend dieser Spalte herausfiltern.

Wenn Sie über Ressourcen verfügen, von denen Sie wissen, dass sie nicht konform sind, können Sie eine bestimmte Ressource für eine bestimmte Konfigurationsregel in ihren Konfigurationsberichten entfernen. So gehen Sie vor:

Senden Sie an Accelerate eine Serviceanfrage für Ihr Konto mit einer Liste der Konfigurationsregeln und Ressourcen, die von der Meldung ausgenommen werden sollen. Sie müssen eine ausdrückliche geschäftliche Begründung angeben (z. B. müssen Sie das nicht melden *resource_name_1* und wir haben kein Backup, weil wir nicht möchten, dass sie gesichert *resource_name_2* werden). Hilfe beim Einreichen einer Accelerate-Serviceanfrage finden Sie unterEine Serviceanfrage in Accelerate erstellen.

Fügen Sie die folgenden Eingaben in die Anfrage ein (fügen Sie für jede Ressource einen separaten Block mit allen erforderlichen Feldern hinzu, wie abgebildet), und senden Sie sie dann ab:

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
```

```
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

Reduzieren Sie die AWS Config Kosten in Accelerate

Sie können die Kosten für AWS Config reduzieren, indem Sie die Option verwenden, den `AWS::EC2::Instance` Ressourcentyp regelmäßig aufzuzeichnen. Durch die regelmäßige Aufzeichnung werden die neuesten Konfigurationsänderungen Ihrer Ressourcen alle 24 Stunden erfasst, wodurch die Anzahl der vorgenommenen Änderungen reduziert wird. Wenn diese Option aktiviert ist, wird AWS Config nur die letzte Konfiguration einer Ressource am Ende eines Zeitraums von 24 Stunden aufgezeichnet. Auf diese Weise können Sie die Konfigurationsdaten an spezifische Anwendungsfälle in den Bereichen Betriebsplanung, Einhaltung von Vorschriften und Audits anpassen, die keine kontinuierliche Überwachung erfordern. Diese Änderung wird nur empfohlen, wenn Sie über Anwendungen verfügen, die von kurzlebigen Architekturen abhängen, was bedeutet, dass Sie die Anzahl der Instanzen ständig nach oben oder unten skalieren.

Wenn Sie sich für die regelmäßige Aufzeichnung des `AWS::EC2::Instance` Ressourcentyps entscheiden möchten, wenden Sie sich an Ihr AMS Delivery Team.

Maßgeschneiderte Antworten auf Ergebnisse

Sie können wählen, wie AMS Accelerate auf einige Ergebnisse reagieren soll (nicht konforme Konfigurationsregeln). Sie können AMS so konfigurieren, dass es auf Ergebnisse reagiert, indem es das Ergebnis behebt, Sie um Ihre Zustimmung zur Behebung bittet oder Ihnen einfach in Ihrem nächsten Monthly Business Review (MBR) Bericht erstattet. Sie können die Standardantworten für AMS Accelerate Config-Regeln ändern. Um die Regeln einzusehen, gehen Sie zu Configuration Compliance > Table of Rules oder laden Sie die Regeltabelle als ZIP-Datei ams_config_rules.zip herunter.

Wenn Sie die Standardantworten ändern, können Sie die Sicherheit und den Compliance-Status Ihres Kontos verbessern, da mehr Fehler behoben werden können. Wenn Sie mehr Ergebnisse korrigieren, haben Sie weniger Fälle, die auf eine manuelle Überprüfung und Genehmigung warten müssen. Die umfangreiche Bibliothek mit AMS-Runbooks zur Problembehebung behebt ständig fehlerhafte Ressourcen, und Sie werden nur dann kontaktiert, wenn dies erforderlich ist.

Maßgeschneiderte Antworten werden nur bei neuen Ressourcen oder bei bestehenden Ressourcen bei neuen Ereignissen verwendet. Zum Beispiel eine Ressource, die nach einer Änderung nicht

mehr richtlinientreu ist. Das liegt daran, dass ältere Ressourcen vor der Behebung in der Regel einer eingehenderen Prüfung bedürfen und es einfacher ist, die Ressourcenkorrektur durchzusetzen, sobald sie erstellt oder geändert werden. Wenn Sie jederzeit die Behebung des Fehlers für eine Ressource beantragen möchten, reichen Sie eine Serviceanfrage ein.

Eine Änderung der Standardantworten beantragen

Cloud-Architekten (CAs) arbeiten beim Onboarding mit Ihnen zusammen, um Ihre Einstellungen zu erfassen. CAsrichten Sie dann die Erstkonfiguration auf internen AMS-Systemen ein. Erstellen Sie nach dem Onboarding eine Serviceanfrage, um Aktualisierungen Ihrer Konfigurationen anzufordern. Sie können Konfigurationsupdates so oft wie nötig anfordern. Bitte beachten Sie, dass Operations nur Konfigurationen für das Konto aktualisiert, in dem die Serviceanfrage erstellt wurde. Wenn Sie mehrere Konten gleichzeitig aktualisieren müssen, wenden Sie sich an Ihren Cloud Architect. Ihre CA wird Sie bitten, eine Serviceanfrage mit Ihren Präferenzen zu Prüfungszwecken auszuschneiden.

Änderung der Standardantworten für Ihre Ergebnisse und Konten

Sie benötigen immer eine bevorzugte Antwort für jedes Konto und jeden Befund. AMS bietet eine Standardantwort (siehe Konformität mit der Konfiguration), sodass diese Konfiguration optional ist. Sie können die Standardantworten für jedes Ergebnis auf die folgenden Optionen ändern:

- Korrigieren: AMS behebt das Ergebnis manuell oder automatisch. AMS überprüft die Behebung und teilt Ihnen mit, ob sie fehlschlägt.
- Genehmigung beantragen: AMS erstellt einen ausgehenden Fall, um Sie über das Ergebnis zu informieren. Verwenden Sie diese Option, wenn Sie das Ergebnis überprüfen möchten, bevor Sie dessen Behebung oder Freistellung genehmigen. AMS führt dann die von Ihnen bevorzugte Aktion aus.
- Keine Maßnahme (nur Bericht): AMS ergreift keine Maßnahmen zur Behebung oder Eskalation des Fehlers. Die Ergebnisse werden möglicherweise weiterhin auf der Konsole angezeigt und die Berichte werden währenddessen angezeigt. MBRs

> **Note**
>
> Sie können die Konfiguration von Regeln, die von AMS behoben werden müssen, nicht ändern. Zum Beispiel die Aktivierung von Amazon GuardDuty und VPC Flow Logs.

Standardantworten nach Ressourcen ändern

Sie können die Antwort auf bestimmte Ressourcen mithilfe von Tags weiter konfigurieren. Mit Resource Tagger können Sie Ihre bereits vorhandenen Tags oder Tag-Ressourcen verwenden. Einzelheiten finden Sie unterBeschleunigen Sie Resource Tagger). Die Konfiguration für Ressourcen mit Tags hat Vorrang vor der Standardaktion für die Suche. Wenn eine Ressource über mehrere Tags mit unterschiedlichen zugehörigen Konfigurationen verfügt, kann AMS keine benutzerdefinierten Problembehebungen durchführen. Stattdessen sendet AMS Ihnen eine ausgehende Serviceanfrage, um Sie über die Situation zu informieren. Für die bucket-server-side-encryptions3-fähige Suche können Sie beispielsweise:

- Ändern Sie die Antwort, um unverschlüsselte S3-Buckets mit dem Tag-Schlüsselwertpaar „Reguliert: True“ zu „korrigieren“
- Ändern Sie die Antwort auf „Keine Aktion“, wenn unverschlüsselte S3-Buckets die Tags „Reguliert: Falsch“ haben, und
- Ändern Sie die Standardantwort unverschlüsselter S3-Buckets in „Nach Genehmigung fragen“. Dies gilt für alle S3-Buckets, die nicht die Tags „Reguliert: Wahr“ oder „Reguliert: Falsch“ tragen

Sie können auch die Eingabe hinzufügen, die für die Ausführung einer benutzerdefinierten Suchantwort erforderlich ist. Bei Problembehebungen, für die ein Verschlüsselungsschlüssel erforderlich ist, können Sie Ihren Schlüssel beispielsweise AMS IDs zur Verfügung stellen. Sie können die Eingabeparameter der Behebungs-Runbooks ändern, AMS unterstützt jedoch keine Integration mit benutzerdefinierten Runbooks. Eine Beschreibung der AMS-Remediation-Runbooks im Config Report finden Sie unter. AWS Config Bericht zur Einhaltung der Kontrollvorschriften

Reaktion auf Vorfälle in Accelerate

Nach Erhalt einer Warnung setzt das AMS-Team automatische und manuelle Abhilfemaßnahmen ein, um die Ressourcen wieder in einen gesunden Zustand zu versetzen. Schlägt die Behebung fehl, startet AMS den Incident-Management-Prozess, um mit Ihrem Team zusammenzuarbeiten. Sie können die Baselines ändern, indem Sie die Standardkonfiguration in einer Konfigurationsdatei aktualisieren.

Reaktion auf Vorfälle und Onboarding in AMS Accelerate

Beim Onboarding unterdrückt AMS Accelerate die automatische Erstellung von Vorfällen für Ihre vorhandenen Ressourcen, die die Vorschriften nicht einhalten. Stattdessen stellt Ihnen Ihr Cloud

Service Deliver Manager (CSDM) einen Bericht zur Verfügung, der alle Regeln und Ressourcen für Verstöße enthält, die Sie überprüfen müssen. Nachdem Sie die Regeln identifiziert haben, die AMS korrigieren soll, erstellen Sie in der Support Center-Konsole eine Serviceanfrage, in der Sie diese Regel und Ressourcen angeben. Die folgende Vorlage für eine Serviceanfrage ist ein Beispiel für eine Kundenanfrage an AMS, Ressourcen, die nicht den Anforderungen entsprechen, manuell zu korrigieren. Falls AMS weitere Fragen hat, erarbeiten wir gemeinsam mit Ihnen die Serviceanfrage, um die erforderlichen Informationen zu sammeln.

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

Nach Abschluss des Onboarding-Prozesses erstellt AMS Accelerate automatisch einen Incident für jede Ressource, die nicht den Regeln entspricht, die als Automatischer Vorfall gekennzeichnet sind.

Resilienz bei Accelerate

Die AWS globale Infrastruktur basiert auf AWS-Regionen Verfügbarkeitszonen. AWS-Regionen stellen mehrere physisch getrennte und isolierte Verfügbarkeitszonen bereit, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mit Availability Zones können Sie Anwendungen und Datenbanken entwerfen und betreiben, die automatisch und ohne Unterbrechung ein Failover zwischen Zonen durchführen. Availability Zones sind hochverfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS-Regionen und Verfügbarkeitszonen finden Sie unter AWS Globale Infrastruktur.

Informationen zu AMS Accelerate Continuity Management finden Sie unterKontinuitätsmanagement in AMS Accelerate.

Sicherheitskontrolle für end-of-support Betriebssysteme

Betriebssysteme, die außerhalb des allgemeinen Supportzeitraums von "end-of-support" oder EOS des Betriebssystemherstellers liegen und keine Sicherheitsupdates erhalten, bergen ein erhöhtes Sicherheitsrisiko.

AWS bietet einige Dienste an, die bei der Handhabung des Betriebssystems helfen end-of-support. Informationen zu Windows end-of-support finden Sie unter End-of-SupportMigrationsprogramm für Windows Server.

> **Note**
>
> Zusätzliche Informationen zu diesem Thema finden Sie in den AWS Artifact-Berichten. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu Erste Schritte mit AWS Artifact. Diese Informationen sind nicht in diesem Benutzerhandbuch enthalten, da sie sensible Sicherheitsinhalte enthalten.

Bewährte Sicherheitsmethoden in Accelerate

AMS Accelerate verwendet Konformitätspakete, die ein allgemeines Compliance-Framework bieten, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS-Config-Regeln Maßnahmen Governance-Prüfungen zur Sicherheit, zum Betrieb oder zur Kostenoptimierung durchzuführen. AWS Config Informationen zur optimalen Konfiguration dieser Conformance Packs finden Sie unter Operational Best Practices for NIST CSF und Operational Best Practices for AWS Config CIS Top 20.

Sicherheitsüberprüfungen für Änderungsanfragen

Das Verfahren zur Überprüfung von Änderungsanträgen in AWS Managed Services stellt sicher, dass AMS eine Sicherheitsüberprüfung der angeforderten Änderungen durchführt, da diese in Ihrem Namen in Ihrem Konto implementiert werden.

AMS Accelerate — technische Standardsdefinieren Sie die Mindestsicherheitskriterien, Konfigurationen und Prozesse, um die grundlegende Sicherheit Ihrer Konten zu gewährleisten. Wenn AMS die angeforderten Änderungen umsetzt, halten wir uns an diese Standards.

AMS bewertet alle Änderungsanfragen anhand der technischen Standards von AMS. Jede Änderung, die die Sicherheitslage Ihres Kontos durch Abweichung von den technischen Standards beeinträchtigen könnte, wird einer Sicherheitsüberprüfung unterzogen. Während dieses Prozesses werden relevante Risiken von AMS hervorgehoben und von Ihrem autorisierten Risikobeauftragten geprüft und genehmigt, um ein ausgewogenes Verhältnis zwischen Sicherheits- und Geschäftsanforderungen zu gewährleisten.

Prozess des Kundensicherheitsrisikomanagements

Der AMS Accelerate Customer Security Risk Management (CSRM) -Prozess hilft dabei, Risiken klar zu identifizieren und den richtigen Eigentümern mitzuteilen. Dieser Prozess minimiert die Sicherheitsrisiken in Ihrer Umgebung und reduziert den laufenden Betriebsaufwand für identifizierte Risiken.

Wenn jemand aus Ihrem Unternehmen AMS auffordert, eine Änderung an Ihrer verwalteten Umgebung vorzunehmen, überprüft AMS die Änderung standardmäßig, um festzustellen, ob die Anfrage nicht den technischen Standards entspricht, was sich auf die Sicherheitslage Ihres Kontos auswirken kann. Wenn ein hohes oder sehr hohes Sicherheitsrisiko besteht, wird die Änderungsprüfung von Ihrem autorisierten Sicherheitspersonal akzeptiert oder abgelehnt. Angeforderte Änderungen werden auch im Hinblick auf nachteilige Auswirkungen auf die Fähigkeit von AMS, das Konto zu führen, geprüft. Wenn bei der Überprüfung mögliche nachteilige Auswirkungen festgestellt werden, sind zusätzliche Prüfungen und Genehmigungen innerhalb von AMS erforderlich.

Sie können sich bei hohen oder sehr hohen Risiken vom genehmigungsbasierten Workflow im CSRM-Prozess abmelden. Um die CSRM-Option für bestimmte Konten von Standard-CSRM auf Nur Benachrichtigung zu ändern, arbeiten Sie mit Ihren Cloud Service Delivery Managern zusammen, um eine einmalige Risikoakzeptanz zu erreichen. Wenn Sie sich für die Option Nur Benachrichtigung entscheiden, implementiert AMS die angeforderten Änderungen unabhängig von der Risikokategorie. Außerdem sendet AMS eine Risikobenachrichtigung an Ihre autorisierten Risikogenehmiger, anstatt vor der Implementierung der Änderung eine Genehmigung einzuholen. Sprechen Sie mit Ihren Cloud-Architekten oder Cloud Service Delivery Managern, um weitere Informationen zum AMS CSRM-Prozess zu erhalten, wie Sie die standardmäßige CSRM-Option beim Onboarding neuer AMS-Konten ändern oder bestehende Konten aktualisieren können.

> **Note**
>
> AMS empfiehlt dringend, dass Sie in all Ihren Konten die Standardoption Standard CSRM verwenden.

AMS Accelerate — technische Standards

Die technischen Standards von Accelerate sind in folgende Kategorien unterteilt:

ID	Kategorie
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	Netzwerksicherheit
AMS-STD-X004	Penetrationstests
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	Protokollierung

Standardsteuerungen in AMS Accelerate

Im Folgenden sind die Standardsteuerungen in AMS aufgeführt:

AMS-STD-X002 - (IAM) AWS Identity and Access Management

ID	Technischer Standard
1,0	Dauer des Timeouts
1.1	Das standardmäßige Timeout einer Sitzung für Verbundbenutzer beträgt eine Stunde und kann auf bis zu vier Stunden erhöht werden.
1.2	Das RDP-Sitzungstimeout für Microsoft Windows Server ist auf 15 Minuten festgeleg t und kann je nach Anwendungsfall verlängert werden.
2.0	AWS Nutzung des Root-Kontos
2.1	Wenn aus irgendeinem Grund ein Root-Kont o genutzt wird, GuardDuty muss Amazon so konfiguriert werden, dass relevante Ergebnisse generiert werden.

ID	Technischer Standard
2.2	Zugriffsschlüssel für das Root-Konto dürfen nicht erstellt werden.
3.0	Erstellung und Änderung von Benutzern
3.1	IAM users/roles mit programmatischem Zugriff und nur Leseberechtigungen können ohne zeitlich begrenzte Richtlinien erstellt werden. Die Erlaubnis, das Lesen von Objekten (z. B. S3:GetObject) in allen Amazon Simple Storage Service-Buckets des Kontos zuzulassen, ist jedoch nicht zulässig.
3.1.1	Menschliche IAM-Benutzer für Konsolenzugriff und mit Leseberechtigungen können mit der zeitgebundenen Richtlinie (bis zu 180 Tage) erstellt werden, während die Richtlinie mit zeitgebundenem Zugriff zu removal/renewal/ extension einer Risikobenachrichtigung führt. Die Erlaubnis, das Lesen von Objekten (z. B. S3:GetObject) in allen S3-Buckets des Kontos zuzulassen, ist jedoch nicht zulässig.
3.2	IAM-Benutzer und -Rollen für den Konsolen- und programmatischen Zugriff mit allen infrastrukturverändernden Berechtig ungen (Schreib- und Rechteverwaltung) im Kundenkonto dürfen nicht ohne Risikober eitschaft erstellt werden. Ausnahmen bestehen für S3-Schreibberechtigungen auf Objektebe ne, die ohne Risikoübernahme zulässig sind, sofern sich die spezifischen Buckets im Gültigkeitsbereich und bei Tagging-Vorgängen für Tags befinden, die nichts mit AMS zu tun haben.

ID	Technischer Standard
3.3	Auf Microsoft Windows-Servern muss nur das Microsoft Group Managed Service Account (gMSA) erstellt werden.
4.0	Richtlinien, Maßnahmen und APIs
4.4	Eine Richtlinie darf den Administratorzugriff nicht mit einer Aussage wie „Wirkung“: „Zulassen“ mit „Aktion“: „*“ statt „Ressource“: „*“ ohne Risikobereitschaft gewähren.
4.6	API-Aufrufe gegen KMS-Schlüsselrichtlinien für AMS-Infrastrukturschlüssel in den IAM-Richtlinien des Kunden dürfen nicht zulässig sein.
4.8	Aktionen, die die DNS-Einträge der AMS-Infrastruktur in Amazon Route 53 ändern, dürfen nicht zugelassen werden.
4,9 bis 4,9	Menschliche IAM-Benutzer mit Konsolenzugriff, die nach Ablauf des ordnungsgemäßen Verfahrens erstellt wurden, dürfen keine Richtlinien direkt angehängt haben, mit Ausnahme der Richtlinien „Vertrauen“, „Rolle übernehmen“ und „Zeitbegrenzung“.
4.10	EC2 Amazon-Instanzprofile mit Lesezugriff auf ein bestimmtes Geheimnis oder einen bestimmten Namespace AWS Secrets Manager innerhalb desselben Kontos können erstellt werden.

ID	Technischer Standard
4.12	Die IAM-Richtlinie darf keine Aktion beinhalte n, zu der auch die Aktionen Logs zulassen: DeleteLogGroup und Logs: DeleteLogStream für eine CloudWatch AMS-Amazon-Protoko llgruppe gehören.
4.13	Berechtigungen zur Erstellung von Schlüssel n für mehrere Regionen dürfen nicht zulässig sein.
4.14	Der Zugriff auf S3-Bucket-ARN, die noch nicht in den Kundenkonten erstellt wurden, kann bereitgestellt werden, indem der Zugriff auf die Buckets auf die Kundenkonten beschränk t wird, indem die Kontonummer mithilfe des dienstspezifischen S3-Bedingungsschlüssels s3: angegeben wird. ResourceAccount
4.15.1	Sie können Zugriff auf Ihr benutzerdefinierte s S3 Storage Lens Dashboard haben, es anzeigen, erstellen, auflisten und löschen.
4.16	Für die Arbeit mit Amazon Redshift Redshift-Datenbanken können vollständige Berechtig ungen im Zusammenhang mit SQL Workbench erteilt werden. roles/users
4.17	Als Alternative zur CLI können Kundenrollen beliebige AWS CloudShell Berechtigungen erteilt werden.
4.18	Eine IAM-Rolle mit AWS Service als vertrauen swürdigem Principal muss ebenfalls den technischen IAM-Standards entsprechen.

ID	Technischer Standard
4.19	Service Linked Roles (SLRs) unterliegen nicht den technischen Standards von AMS IAM, da sie vom IAM Service Team erstellt und verwaltet werden.
4.20	Die IAM-Richtlinie sollte das Lesen von Objekten (z. B. S3:GetObject) in allen S3-Buckets des Kontos nicht zulassen.
4.21	Alle IAM-Berechtigungen für den Ressourcentyp „Savingsplan“ können Kunden gewährt werden.
4.22	Der AMS-Techniker ist nicht berechtigt, Kundendaten (Dateien, S3-Objekte, Datenbanken usw.) manuell in einem der Datenspeicherdienste wie Amazon S3, Amazon Relational Database Service, Amazon DynamoDB usw. oder im Dateisystem des Betriebssystems zu kopieren oder zu verschieben.
6.0	Kontenübergreifende Richtlinien
6.1	IAM-Rollen und Vertrauensrichtlinien zwischen AMS-Konten, die laut Kundendatensätzen demselben Kunden gehören, können konfiguriert werden.
6.2	Vertrauensrichtlinien für IAM-Rollen zwischen AMS- und Nicht-AMS-Konten müssen nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird).

ID	Technischer Standard
6.3	Vertrauensrichtlinien für IAM-Rollen zwischen AMS-Konten und Konten von Drittanbietern dürfen nicht ohne Risikobereitschaft konfiguriert werden.
6.4	Kontoübergreifende Richtlinien für den Zugriff auf alle Kunden, die CMKs zwischen AMS-Konten desselben Kunden verwaltet werden, können konfiguriert werden.
6,5	Kontoübergreifende Richtlinien für den Zugriff auf jeden KMS-Schlüssel innerhalb eines Nicht-AMS-Kontos über ein AMS-Konto können konfiguriert werden.
6.6	Kontoübergreifende Richtlinien für den Zugriff auf alle KMS-Schlüssel innerhalb eines AMS-Kontos durch ein Drittanbieterkonto dürfen nur zulässig sein, wenn das Risiko eingegangen wird.
6.6.1	Kontoübergreifende Richtlinien für den Zugriff auf jeden KMS-Schlüssel innerhalb eines AMS-Kontos über ein Nicht-AMS-Konto können nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört.
6.7	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), zwischen AMS-Konten desselben Kunden können konfiguriert werden.

ID	Technischer Standard
6.8	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), können von einem AMS-Konto mit schreibgeschütztem Zugriff in einem Nicht-AMS-Konto aus konfiguriert werden.
6.9	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift) mit Schreibberechtigun gen von AMS auf ein Nicht-AMS-Konto (oder ein Nicht-AMS-zu-AMS-Konto), müssen nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird).
6.10	Kontoübergreifende Richtlinien für den Zugriff auf alle S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), können von einem AMS-Konto mit schreibgeschütztem Zugriff aus einem Drittanbieter-Konto konfiguriert werden.

ID	Technischer Standard
6.11	Kontoübergreifende Richtlinien für den Zugriff auf S3-Bucket-Daten oder Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), von einem AMS-Konto mit Schreibzugriff in einem Drittanbieter-Konto aus dürfen nicht konfiguriert werden.
6.12	Kontoübergreifende Richtlinien von Drittanbieterkonten für den Zugriff auf einen S3-Bucket eines AMS-Kunden oder auf Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift), dürfen nicht ohne Risikoberechtigung konfiguriert werden.
7.0	User Groups (Benutzergruppen)
7.1	IAM-Gruppen mit schreibgeschützten und nicht mutativen Berechtigungen sind zulässig.
8.0	Ressourcenbasierte Richtlinien
8,4	Die AMS-Infrastrukturressourcen sollten durch das Hinzufügen von ressourcenbasierten Richtlinien vor der Verwaltung durch unbefugte Identitäten geschützt werden.
8.2	Kundenressourcen sollten mit ressourcenbasierten Richtlinien mit den geringsten Rechten konfiguriert werden, es sei denn, der Kunde spezifiziert ausdrücklich eine andere Richtlinie.

AMS-STD-X003 — Netzwerksicherheit

Im Folgenden finden Sie die Standardsteuerung für X003 — Netzwerksicherheit:

ID	Technischer Standard
	Netzwerkfunktionen
1,0	Reserviert für future Kontrolle
2.0	Elastic IP auf EC2 Instances ist zulässig
3.0	Die AMS-Steuerebene und damit auch TLS 1.2+ in der Datenebene müssen verwendet werden.
5.0	Eine Sicherheitsgruppe darf in der Regel für eingehenden Datenverkehr nicht die Quelle 0.0.0.0/0 haben, wenn sie nicht gemäß 9.0 an einen Load Balancer angehängt ist
6.0	S3-Buckets oder Objekte dürfen nicht ohne Risikobereitschaft veröffentlicht werden.
7.0	Der Serververwaltungszugriff auf die Ports SSH/22 oder SSH/2222 (nicht SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 oder 1604, LDAP/389 oder 636 und RPC/135, NETBIOS/137-139 darf nicht von außerhalb der VPC über Sicherheitsgruppen zugelassen werden.
8.0	Der Zugriff auf die Datenbankverwaltung auf Ports (MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) oder auf einem benutzerdefinierten Port darf nicht von öffentlich zugelassen werden, nicht über DX, VPC-Peer oder VPN über eine Sicherheitsgruppe an VPC geroutet werden. IPs

ID	Technischer Standard
8.1	Jede Ressource, in der Kundendaten gespeichert werden können, sollte nicht direkt dem öffentlichen Internet zugänglich gemacht werden.
9.0	Direkter Anwendungszugriff über die Ports HTTP/80, HTTPS/8443 und HTTPS/443 aus dem Internet ist nur für Load Balancer zulässig, nicht jedoch für direkte Rechenressourcen, z. B. Instanzen, Container usw. EC2 ECS/EKS/Fargate
10.0	Der Zugriff auf Anwendungen über die Ports HTTP/80 und HTTPS/443 aus dem privaten IP-Bereich des Kunden kann zugelassen werden.
11.0	Jegliche Änderungen an den Sicherheitsgruppen, die den Zugriff auf die AMS-Infrastruktur kontrollieren, dürfen nicht ohne Risikobereitschaft zugelassen werden.
12.0	AMS Security bezieht sich jedes Mal auf die Standards, wenn eine Sicherheitsgruppe aufgefordert wird, einer Instance zugeordnet zu werden.

ID	Technischer Standard
14.0	Die kontenübergreifende Zuordnung von privaten gehosteten Zonen mit einem VPCs AMS-Konto zu einem Nicht-AMS-Konto (oder einem Nicht-AMS-Konto zu AMS-Konto) muss nur konfiguriert werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS-Organisationskonto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird). Verwenden Sie dazu interne Tools.
15.0	VPC-Peering-Verbindungen zwischen Konten, die demselben Kunden gehören, können zugelassen werden.
16.0	Die AMIs AMS-Basis kann mithilfe interner Tools mit einem anderen Konto gemeinsam genutzt werden, sofern beide Konten demselben Kunden gehören (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain dem Firmennamen des Kunden zugeordnet wird).
17.0	FTP-Port 21 darf in keiner der Sicherhei tsgruppen konfiguriert werden, ohne dass ein Risiko eingegangen ist.
18.0	Kontoübergreifende Netzwerkkonnektivität über das Transit-Gateway ist zulässig, solange sich alle Konten im Besitz des Kunden befinden.
19.0	Es ist nicht zulässig, ein privates Subnetz öffentlich zugänglich zu machen

ID	Technischer Standard
20.0	VPC-Peering-Verbindungen mit Konten von Drittanbietern (die nicht dem Kunden gehören) dürfen nicht zugelassen werden.
21.0	Eine Verbindung mit einem Drittanbieterkonto (das nicht dem Kunden gehört) durch Transit Gateway darf nicht zugelassen werden.
22.0	Jeglicher Netzwerkverkehr, der für AMS zur Bereitstellung der Dienste für Kunden erforderl ich ist, darf am Netzwerkausgangspunkt des Kunden nicht blockiert werden.
23,0	Für eingehende ICMP-Anfragen EC2 von der Kundeninfrastruktur an Amazon ist eine Risikobenachrichtigung erforderlich.
24,0	Eingehende Anfragen von der Öffentlichkeit, die über DX, VPC-Peer oder VPN über eine Sicherheitsgruppe an Amazon VPC IPs weitergeleitet werden, sind zulässig.
25.0	Eingehende Anfragen von der Öffentlichkeit, die IPs nicht über DX, VPC-Peer oder VPN über eine Sicherheitsgruppe an Amazon VPC weitergeleitet werden, erfordern eine Risikoakz eptanz.
26,0	Ausgehende ICMP-Anfragen von Amazon EC2 an ein beliebiges Ziel sind zulässig.
27,0	Gemeinsame Nutzung von Sicherheitsgruppen

ID	Technischer Standard
27.1	Wenn eine Sicherheitsgruppe diesen Sicherheitsstandard erfüllt, kann sie von mehreren Mitgliedern VPCs desselben Kontos und von Konten derselben Organisation gemeinsam genutzt werden.
27.2	Wenn eine Sicherheitsgruppe diesen Standard nicht erfüllt und zuvor eine Risikoakzeptanz für diese Sicherheitsgruppe erforderlich war, ist die Verwendung der Funktion zur gemeinsamen Nutzung von Sicherheitsgruppen zwischen VPCs Konten innerhalb desselben Kontos oder zwischen Konten in derselben Organisation ohne Risikoakzeptanz für diese neue VPC oder dieses neue Konto nicht zulässig.

AMS-STD-X004 — Penetrationstests

Im Folgenden finden Sie die Standardsteuerung für X004 — Penetrationstests

1. AMS unterstützt keine Pentest-Infrastruktur. Es liegt in der Verantwortung des Kunden. Kali ist beispielsweise keine AMS-unterstützte Linux-Distribution.
2. Kunden müssen sich an Penetrationstests halten.
3. AMS muss 24 Stunden im Voraus benachrichtigt werden, falls der Kunde Infrastruktur-Penetrationstests für Konten durchführen möchte.
4. AMS stellt dem Kunden eine Pentesting-Infrastruktur gemäß den Kundenanforderungen bereit, die ausdrücklich in der Änderungsanfrage oder Serviceanfrage des Kunden angegeben sind.
5. Das Identitätsmanagement für die Pentesting-Infrastruktur des Kunden liegt in der Verantwortung des Kunden.

AMS-STD-X005 - GuardDuty

Das Folgende ist die Standardsteuerung für X005 - GuardDuty

1. GuardDuty muss in allen Kundenkonten jederzeit aktiviert sein.

2. GuardDuty Benachrichtigungen müssen in demselben Konto oder in einem anderen verwalteten Konto derselben Organisation gespeichert werden.
3. Die Funktion „Liste vertrauenswürdiger IP-Adressen“ von GuardDuty darf nicht verwendet werden. Stattdessen kann die automatische Archivierung als Alternative verwendet werden, was für Auditzwecke nützlich ist.

AMS-STD-X007 — Protokollierung

Im Folgenden finden Sie die Standardsteuerung für X007 — Logging

ID	Technischer Standard
1,0	Typen von Protokollen
1.1	Betriebssystemprotokolle: Alle Hosts müssen mindestens Host-Authentifizierungserei gnisse, Zugriffsereignisse für alle Nutzungen erhöhter Rechte und Zugriffsereignisse für alle Änderungen an der Zugriffs- und Rechtekon figuration protokollieren, einschließlich Erfolg und Misserfolg.
1.2	AWS CloudTrail: Die Protokollierung von CloudTrail Verwaltungsereignissen muss aktiviert und konfiguriert sein, um Protokolle an einen S3-Bucket zu übermitteln.
1.3	VPC Flow Logs: Alle Netzwerkverkehrspr otokolle müssen über VPC Flow Logs protokoll iert werden.
1.4	Amazon S3 S3-Serverzugriffsprotokollierung: Für von AMS vorgeschriebene S3-Buckets, in denen Protokolle gespeichert werden, muss die Serverzugriffsprotokollierung aktiviert sein.
1.5	AWS Config Snapshots: AWS Config müssen Konfigurationsänderungen für alle unterstüt

ID	Technischer Standard
	zten Ressourcen in allen Regionen aufzeichn en und die Konfigurations-Snapshot-Dateien mindestens einmal täglich an S3-Buckets liefern.
1,7	Anwendungsprotokolle: Kunden können die Protokollierung in ihren Anwendungen aktiviere n und diese in der Protokollgruppe CloudWatch Logs oder in einem S3-Bucket speichern.
1.8	S3-Protokollierung auf Objektebene: Kunden können die Protokollierung auf Objektebene in ihren S3-Buckets aktivieren.
1.9	Serviceprotokollierung: Kunden sind berechtig t, Protokolle für SSPS-Dienste wie für alle Kerndienste zu aktivieren und weiterzuleiten.
1.10	Elastic Load Classic/Application Load Balancer/ Network Balancing (Load Balancer) -Protokolle: Zugriffs- und Fehlerprotokolleinträge müssen in den von AMS 2.0 verwalteten S3-Buckets gespeichert werden.
2.0	Zugriffskontrolle
2.3	Von AMS vorgeschriebene S3-Buckets, in denen Logs gespeichert werden, dürfen laut den Bucket-Richtlinien grundsätzlich keine Benutzer von Drittanbieterkonten zulassen.
2.4	CloudWatch Protokolle aus Logs-Protokollgrup pen dürfen ohne ausdrückliche Genehmigu ng des vom Kunden autorisierten Sicherhei tskontakts nicht gelöscht werden.
3.0	Aufbewahrung von Protokollen

ID	Technischer Standard
3.1	Für CloudWatch Protokollgruppen, die von AMS vorgeschrieben sind, muss eine Mindestaufbewahrungsdauer von 90 Tagen für die Protokolle gelten.
3.2	Von AMS vorgeschriebene S3-Buckets, in denen die Protokolle gespeichert werden, müssen eine Mindestaufbewahrungsdauer von 18 Monaten für die Protokolle haben.
3.3	AWS Backup Snapshots sollten mit einer Mindestdauer von 31 Tagen auf den unterstützten Ressourcen verfügbar sein.
4.0	Verschlüsselung
4.1	Die Verschlüsselung muss in allen S3-Buckets aktiviert sein, die von AMS Teams, das Protokolle speichert, benötigt werden.
4.2	Jede Protokollweiterleitung von Kundenkonten zu anderen Konten muss verschlüsselt sein.
5.0	Integrität
5.1	Der Integritätsmechanismus für Protokolldateien muss aktiviert sein. Das bedeutet, dass Sie die „Überprüfung der Protokolldateien“ in den von den AMS-Teams benötigten AWS CloudTrail Pfaden konfigurieren müssen.
6.0	Weiterleitung von Protokollen
6.1	Jedes Protokoll kann von einem AMS-Konto an ein anderes AMS-Konto desselben Kunden weitergeleitet werden.

ID	Technischer Standard
6.2	Jedes Protokoll kann mithilfe interner Tools nur dann von AMS an ein Nicht-AMS-Konto weitergeleitet werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass es sich um dasselbe AWS Organizations Konto handelt, oder indem die E-Mail-Domain dem Firmennamen des Kunden und dem mit PAYER verknüpften Konto zugeordnet wird).

Änderungen, die hohe oder sehr hohe Sicherheitsrisiken in Ihrer Umgebung mit sich bringen

Die folgenden Änderungen stellen ein hohes oder sehr hohes Sicherheitsrisiko in Ihrer Umgebung dar:

AWS Identity and Access Management

- High_Risk-IAM-001: Erstellen Sie Zugriffsschlüssel für das Root-Konto
- High_Risk-IAM-002: Änderung der SCP-Richtlinie, um zusätzlichen Zugriff zu ermöglichen
- High_Risk-IAM-003: Änderung der SCP-Richtlinie, die die AMS-Infrastruktur beschädigen könnte
- High_Risk-IAM-004: Erstellung eines role/user mit der Infrastruktur verändernden Berechtigungen (Schreiben, Rechteverwaltung oder Tagging) im Kundenkonto
- High_Risk-IAM-005: IAM-Rollen vertrauen auf Vertrauensrichtlinien zwischen AMS-Konten und Konten von Drittanbietern (die nicht dem Kunden gehören)
- High_Risk-IAM-006: Kontoübergreifende Richtlinien für den Zugriff auf beliebige KMS-Schlüssel von einem AMS-Konto aus (durch ein Drittanbieterkonto)
- High_Risk-IAM-007: Kontoübergreifende Richtlinien von Drittanbieterkonten für den Zugriff auf einen S3-Bucket eines AMS-Kunden oder auf Ressourcen, in denen Daten gespeichert werden können (wie Amazon RDS, Amazon DynamoDB oder Amazon Redshift)
- high_risk-IAM-008: Weisen Sie die IAM-Berechtigungen einer beliebigen Infrastruktur-Mutationsberechtigung im Kundenkonto zu

- High_Risk-IAM-009: Erlaubt das Auflisten und Lesen aller S3-Buckets im Konto

Netzwerksicherheit

- High_Risk-NET-001: Öffnen Sie die Betriebssystemmanagement-Ports SSH/22 oder SSH/2222 (nicht SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 oder 1604, LDAP/389 oder 636 und NETBIOS/137-139 aus dem Internet
- High_Risk-NET-002: Öffnen Sie die Datenbankmanagement-Ports MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 oder einen beliebigen Management-Kundenport aus dem Internet
- High_Risk-NET-003: Öffnen Sie die Anwendungsports HTTP/80, HTTPS/8443 und HTTPS/443 direkt auf beliebigen Rechenressourcen. Zum Beispiel Instanzen, Container usw. aus dem Internet EC2 ECS/EKS/Fargate
- High_Risk-NET-004: Alle Änderungen an den Sicherheitsgruppen, die den Zugriff auf die AMS-Infrastruktur kontrollieren
- High_Risk-NET-006: VPC-Peering mit dem Drittanbieter-Konto (nicht im Besitz des Kunden)
- High_Risk-NET-007: Kunden-Firewall als Ausgangspunkt für den gesamten AMS-Verkehr hinzufügen
- High_Risk-NET-008: Ein Transit Gateway Gateway-Anhang mit dem Drittanbieterkonto ist nicht zulässig
- High_Risk-S3-001: Bereitstellung oder Aktivierung des öffentlichen Zugriffs im S3-Bucket

Protokollierung

- CloudTrailHigh_Risk-Log-001: Deaktivieren.
- High_Risk-Log-002: Deaktivieren Sie VPC-Flow-Logs.
- High_Risk-Log-003: Protokollweiterleitung über eine beliebige Methode (S3-Ereignisbenachrichtigung, SIEM-Agent-Pull, SIEM-Agent-Push usw.) von einem AMS-verwalteten Konto an ein Drittanbieter-Konto (nicht im Besitz des Kunden)
- High_Risk-Log-004: Verwenden Sie den Nicht-AMS-Trail für CloudTrail

Sonstiges

- High_Risk-ENC-001: Deaktiviert die Verschlüsselung in jeder Ressource, falls sie aktiviert ist

Häufig gestellte Fragen zur Sicherheit

AMS bietet rund um die Uhr follow-the-sun Support über globale Betriebszentren. Engagierte Betriebsingenieure von AMS überwachen aktiv die Dashboards und Warteschlangen bei Zwischenfällen. In der Regel verwaltet AMS Ihre Konten automatisiert. In seltenen Fällen, in denen spezielle Problembehebungs- oder Bereitstellungskenntnisse erforderlich sind, kann ein Betriebsingenieur von AMS auf Ihre AWS Konten zugreifen.

Im Folgenden finden Sie häufig gestellte Fragen zu den bewährten Sicherheitsmethoden, Kontrollen, Zugriffsmodellen und Prüfmechanismen, die AMS Accelerate verwendet, wenn ein AMS-Betriebsingenieur oder ein Automatisierungstechniker auf Ihre Konten zugreift.

Wann greifen die Betriebsingenieure von AMS auf meine Umgebungen zu?

Die Betriebsingenieure von AMS haben keinen dauerhaften Zugriff auf Ihre Konten oder Instanzen. Der Zugriff auf Kundenkonten wird AMS-Betreibern nur für berechtigte geschäftliche Anwendungsfälle wie Benachrichtigungen, Vorfälle, Änderungsanfragen usw. gewährt. Der Zugriff wird in AWS CloudTrail Protokollen dokumentiert.

Informationen zur Begründung des Zugriffs, zu Auslösern und Trigger-Initiatoren finden Sie unterAuslöser für den Zugriff auf das AMS-Kundenkonto.

Welche Rollen nehmen die Betriebsingenieure von AMS ein, wenn sie auf meine Konten zugreifen?

In den seltenen Fällen (~ 5%), in denen ein menschliches Eingreifen in Ihre Umgebung erforderlich ist, melden sich die Betriebsingenieure von AMS mit einer standardmäßigen, schreibgeschützten Zugriffsrolle bei Ihrem Konto an. Die Standardrolle hat keinen Zugriff auf Inhalte, die üblicherweise in Datenspeichern wie Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift und Amazon gespeichert sind. ElastiCache

Eine Liste der Rollen, die Betriebstechniker und Systeme von AMS benötigen, um Dienste in Ihrem Konto bereitzustellen, finden Sie unter. Zugriff auf das AMS-Kundenkonto (IAM-Rollen)

Wie greift ein AMS-Betriebsingenieur auf mein Konto zu?

Für den Zugriff auf Kundenkonten verwenden die Betriebsingenieure von AMS einen AWS internen AMS-Zugangsdienst. Dieser interne Service ist nur über einen sicheren, privaten Kanal verfügbar, sodass der Zugriff auf Ihre Konten sicher und geprüft ist.

1. Die Betriebstechniker von AMS verwenden die interne AMS-Zugangsdienst-Authentifizierung zusammen mit einer Zwei-Faktor-Authentifizierung. Außerdem muss der Betriebsingenieur eine geschäftliche Begründung (Incident-Ticket oder Service-Request-ID) vorlegen, aus der hervorgeht, dass Sie auf Ihr AWS Konto zugreifen müssen.
2. Auf der Grundlage der Autorisierung des Betriebstechnikers weist der AMS Access Service dem Techniker die entsprechende Rolle (Lese-only/Operator/Admin) und Anmelde-URL für Ihre AWS Konsole zu. Der Zugriff auf Ihr Konto ist kurzlebig und zeitlich begrenzt.
3. Für den Zugriff auf EC2 Amazon-Instances verwenden die Betriebstechniker von AMS denselben internen AMS-Zugriffsservice wie der Broker. Nachdem der Zugriff gewährt wurde, greifen die Betriebstechniker von AMS mit kurzlebigen Sitzungsdaten auf Ihre Instances AWS Systems Manager Session Manager zu.

   Um RDP-Zugriff für Windows-Instances bereitzustellen, verwendet der Operations Engineer Amazon EC2 Systems Manager, um einen lokalen Benutzer auf der Instance zu erstellen und die Portweiterleitung zur Instance einzurichten. Der Operations Engineer verwendet lokale Benutzeranmeldeinformationen für den RDP-Zugriff auf die Instance. Die lokalen Benutzeranmeldedaten werden am Ende der Sitzung entfernt.

Das folgende Diagramm zeigt den Prozess, mit dem die Betriebstechniker von AMS auf Ihr Konto zugreifen:

Wie verfolge ich die von AMS an meinen von AMS verwalteten AWS Konten vorgenommenen Änderungen?

Zugriff auf das Konto

Um Ihnen zu helfen, Änderungen nachzuverfolgen, die durch Automatisierung oder durch das AMS Accelerate-Betriebsteam vorgenommen wurden, bietet AMS die SQL-Schnittstelle für Änderungsdatensätze in der Amazon Athena Athena-Konsole und AMS Accelerate-Protokolle. Diese Ressourcen bieten die folgenden Informationen:

- Wer hat auf Ihr Konto zugegriffen?
- Wann auf das Konto zugegriffen wurde.
- Welche Rechte wurden für den Zugriff auf Ihr Konto verwendet?
- Welche Änderungen wurden von AMS Accelerate an Ihrem Konto vorgenommen.

- Warum wurden die Änderungen in Ihrem Konto vorgenommen?

Konfiguration der Ressourcen

Zeigen Sie CloudTrail Protokolle an, um die Konfigurationen in Ihren AWS Ressourcen für die letzten 90 Tage nachzuverfolgen. Wenn Ihre Konfiguration älter als 90 Tage ist, greifen Sie auf die Protokolle in Amazon S3 zu.

Instanzprotokolle

Der CloudWatch Amazon-Agent sammelt Betriebssystemprotokolle. Sehen Sie sich die CloudWatch Protokolle an, um die Anmelde- und andere Aktionsprotokolle zu sehen, die Ihr Betriebssystem unterstützt.

Weitere Informationen finden Sie unter Änderungen in Ihren AMS Accelerate-Konten verfolgen.

Was sind die Prozesskontrollen für den Zugriff eines AMS-Betriebsingenieurs auf mein Konto?

Bevor sie zu AMS kommen, werden Betriebsingenieure einer kriminalpolizeilichen Überprüfung unterzogen. Da die Techniker von AMS die Kundeninfrastruktur verwalten, müssen sie auch eine jährliche Zuverlässigkeitsüberprüfung durchführen. Wenn ein Techniker die Zuverlässigkeitsüberprüfung nicht besteht, wird der Zugriff gesperrt.

Alle Betriebsingenieure von AMS müssen eine obligatorische Sicherheitsschulung in den Bereichen Infrastruktursicherheit, Datensicherheit und Reaktion auf Vorfälle absolvieren, bevor ihnen Zugriff auf Ressourcen gewährt wird.

Wie wird der privilegierte Zugriff verwaltet?

Eine Untergruppe von Benutzern muss zusätzliche Schulungen absolvieren und über privilegierte Zugriffsrechte für erweiterte Zugriffsrechte verfügen. Zugriff und Nutzung werden geprüft und geprüft. AMS beschränkt den privilegierten Zugriff auf außergewöhnliche Umstände oder wenn der Zugriff mit den geringsten Rechten Ihre Anfrage nicht erfüllen kann. Privilegierter Zugriff ist auch zeitgebunden.

Verwenden AMS-Betriebsingenieure MFA?

Ja. Alle Benutzer müssen MFA und Proof of Presence verwenden, um Ihnen Dienste anbieten zu können.

Was passiert mit ihren Zugangsdaten, wenn ein AMS-Mitarbeiter das Unternehmen verlässt oder seine berufliche Position wechselt?

Der Zugriff auf Kundenkonten und Ressourcen erfolgt über eine interne Gruppenmitgliedschaft. Die Mitgliedschaft basiert auf strengen Kriterien wie der spezifischen beruflichen Rolle, dem berichterstattenden Manager und dem Beschäftigungsstatus bei AMS. Wenn sich die Berufsgruppe eines Betriebsingenieurs ändert oder seine Benutzer-ID deaktiviert wird, wird der Zugriff gesperrt.

Welche Zugriffskontrollen regeln den Zugriff eines AMS-Betriebsingenieurs auf meine Konten?

Es gibt mehrere Ebenen technischer Kontrollen, um die Prinzipien „Need to know“ und „Least Privilege“ für den Zugriff auf Ihre Umgebung durchzusetzen. Im Folgenden finden Sie eine Liste der Zugriffskontrollen:

- Alle Betriebsingenieure müssen einer bestimmten internen AWS Gruppe angehören, um auf Kundenkonten und Ressourcen zugreifen zu können. Die Gruppenzugehörigkeit basiert ausschließlich auf der Grundlage des Need-to-wisse-Prinzips und wird anhand vordefinierter Kriterien automatisiert.
- AMS praktiziert den „nicht-persistenten“ Zugriff auf Ihre Umgebung. Das bedeutet, dass der Zugriff auf Ihre AWS Konten durch AMS Operations "just-in-time" mit kurzlebigen Zugangsdaten erfolgt. Der Zugriff auf Ihre Konten wird erst gewährt, nachdem ein interner Geschäftsfall (Serviceanfrage, Vorfall, Anfrage zum Änderungsmanagement usw.) eingereicht und geprüft wurde.
- AMS folgt dem Prinzip der geringsten Rechte. Autorisierte Betriebstechniker gehen daher standardmäßig von einem Nur-Lese-Zugriff aus. Schreibzugriff wird nur von Technikern verwendet, wenn aufgrund eines Vorfalls oder einer Änderungsanforderung Änderungen an Ihrer Umgebung erforderlich sind.
- AMS verwendet leicht identifizierbare AWS Identity and Access Management Standardrollen, die das Präfix „ams“ verwenden, um Ihre Konten zu überwachen und zu verwalten. Der gesamte Zugriff ist angemeldet, AWS CloudTrail sodass Sie ihn überprüfen können.
- AMS verwendet automatisierte Backend-Tools, um unbefugte Änderungen an Ihrem Konto während der Überprüfung der Kundeninformationen bei der Ausführung von Änderungen zu erkennen.

Wie überwacht AMS den Root-Benutzerzugriff?

Der Root-Zugriff löst immer den Incident-Response-Prozess aus. AMS verwendet die GuardDuty Amazon-Erkennung, um die Aktivitäten von Root-Benutzern zu überwachen. Wenn eine Warnung GuardDuty generiert wird, erstellt AMS ein Ereignis zur weiteren Untersuchung. AMS benachrichtigt Sie, wenn eine unerwartete Root-Kontoaktivität festgestellt wird, und das AMS-Sicherheitsteam leitet eine Untersuchung ein.

Wie reagiert AMS auf Sicherheitsvorfälle?

AMS untersucht Sicherheitsereignisse, die durch Erkennungsdienste wie Amazon und Amazon GuardDuty Macie sowie durch von Kunden gemeldete Sicherheitsprobleme ausgelöst werden. AMS arbeitet mit Ihrem Sicherheitsteam zusammen, um den SIR-Prozess (Security Incident Response) durchzuführen. Der AMS SIR-Prozess basiert auf dem NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, und bietet rund um die Uhr Sicherheitslösungen. follow-the-sun AMS arbeitet mit Ihnen zusammen, um Sicherheitsvorfälle schnell zu analysieren und einzudämmen.

An welche branchenüblichen Zertifizierungen und Rahmenbedingungen hält sich AMS?

Wie andere AWS Services ist AWS Managed Services für OSPAR, HIPAA, HITRUST, GDPR, SOC*, ISO*, FedRAMP (Medium/High), IRAP und PCI zertifiziert. Weitere Informationen zu den Konformitätszertifizierungen, Vorschriften und Rahmenbedingungen für Kunden, die damit in AWS Einklang stehen, finden Sie unter AWS-Compliance.

Sicherheitsleitplanken

AWS Managed Services verwendet mehrere Kontrollen, um Ihre Informationsressourcen zu schützen und Ihnen zu helfen, Ihre AWS Infrastruktur zu schützen. AMS Accelerate verfügt über eine Bibliothek mit AWS Config Regeln und Abhilfemaßnahmen, mit denen Sie sicherstellen können, dass Ihre Konten den Industriestandards für Sicherheit und Betriebsintegrität entsprechen. AWS Config Regeln verfolgen kontinuierlich Konfigurationsänderungen an Ihren aufgezeichneten Ressourcen. Wenn eine Änderung gegen die Bedingungen einer Regel verstößt, meldet AMS Ihnen die Ergebnisse. Je nach Schwere des Verstoßes können Sie Verstöße automatisch oder auf Anfrage beheben.

AMS verwendet AWS Config Regeln, um die Anforderungen der folgenden Standards zu erfüllen:

- Zentrum für Internetsicherheit (CIS)

- Cloud Security Framework (CSF) des Nationalen Instituts für Standards und Technologie (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Datensicherheitsstandard (DSS) der Zahlungskartenindustrie (PCI)

Weitere Informationen finden Sie unter Sicherheitsmanagement in AMS Accelerate.

Wie erhalte ich Zugriff auf die neuesten Berichte zu Sicherheitszertifizierungen, Frameworks und Compliance? AWS

Aktuelle Sicherheits- und Compliance-Berichte für AWS Services finden Sie mit den folgenden Methoden:

- Hier können AWS ArtifactSie den neuesten Bericht über die Sicherheit, Verfügbarkeit und Vertraulichkeit eines AWS Dienstes herunterladen.
- Eine Liste der meisten AWS Services, einschließlich AWS Managed Services, die den globalen Compliance-Frameworks entsprechen, finden Sie unterhttps://aws.amazon.com/compliance/services-in-scope/. Wählen Sie beispielsweise PCI aus und suchen Sie nach AWS Managed Services.

  Sie können nach „AMS“ suchen, um AMS-spezifische Sicherheitsartefakte aus einem AMS-verwalteten AWS Konto zu finden. AWS Managed Services fällt in den Geltungsbereich von SOC 3.
- Der AWS SOC 2-Bericht (System and Organizations Controls) wird im AWS Artifact Repository veröffentlicht. In diesem Bericht werden die AWS Kontrollen bewertet, die die Kriterien für Sicherheit, Verfügbarkeit und Vertraulichkeit des TSP des American Institute of Certified Public Accountants (AICPA), Abschnitt 100, Trust Services Criteria, erfüllen.

Gibt AMS Referenzarchitekturdiagramme zu verschiedenen Aspekten der AMS-Funktionen weiter?

Um sich die AMS-Referenzarchitektur anzusehen, laden Sie das PDF AWS Managed Services for Proactive Monitoring herunter.

Wie verfolgt AMS, wer auf meine Konten zugreift und was das Unternehmen für den Zugriff benötigt?

Um die Servicekontinuität und die Sicherheit Ihrer Konten zu gewährleisten, greift AMS nur als Reaktion auf proaktive Integritäts- oder Wartungs-, Gesundheits- oder Sicherheitsereignisse, geplante Aktivitäten oder Kundenanfragen auf Ihr Konto oder Ihre Instances zu. Der Zugriff auf Ihre Konten wird über AMS-Prozesse autorisiert, wie im Zugriffsmodell für AMS Accelerate beschrieben. Diese Autorisierungsabläufe enthalten Schutzmaßnahmen, um unbeabsichtigten oder unangemessenen Zugriff zu verhindern. Im Rahmen des Zugriffsflusses stellt AMS das Autorisierungssystem für geschäftliche Zwecke bereit. Bei dieser geschäftlichen Anforderung kann es sich um eine Arbeitsaufgabe handeln, die mit Ihrem Konto verknüpft ist, z. B. ein Fall, den Sie bei AMS eröffnet haben. Oder es könnte sich bei der Geschäftsanforderung um einen autorisierten Workflow handeln, wie z. B. die Patching-Lösung. Jeder Zugriff erfordert eine Begründung, die in Echtzeit von internen AMS-Systemen auf der Grundlage von Geschäftsregeln validiert, verifiziert und autorisiert wird, um Zugriffsanfragen an die Geschäftsanforderungen anzupassen.

Die Betriebsingenieure von AMS erhalten ohne gültige Geschäftsanforderungen keinen Zugang zu Ihren Konten. Jeglicher Kontozugriff und die damit verbundenen geschäftlichen Anforderungen werden auf die AWS CloudTrail Einträge in Ihren AWS Konten übertragen. Dies bietet volle Transparenz und bietet Ihnen die Möglichkeit, Ihre eigenen Audits und Inspektionen durchzuführen. Zusätzlich zu Ihrer Inspektion verfügt AMS über automatisierte Inspektionen und führt bei Bedarf manuelle Inspektionen von Zugriffsanfragen durch. Außerdem führt AMS Audits der Werkzeuge und des Zugriffs von Personen durch, um anomale Zugriffe zu überprüfen.

Haben AMS-Techniker Zugriff auf meine Daten, die in AWS Datenspeicherdiensten wie Amazon S3, Amazon RDS, DynamoDB und Amazon Redshift gespeichert sind?

AMS-Techniker haben keinen Zugriff auf Kundeninhalte, die in AWS Diensten gespeichert sind, die üblicherweise zur Datenspeicherung verwendet werden. Der Zugriff auf Daten, die in diesen Diensten zum Lesen, Schreiben, Ändern oder Löschen AWS APIs verwendet werden, ist durch eine ausdrückliche IAM-Ablehnungsrichtlinie eingeschränkt, die den IAM-Rollen zugeordnet ist, die für den Zugriff von AMS-Technikern verwendet werden. Darüber hinaus verhindern interne AMS-Leitplanken und Automatisierungen, dass die Betriebsingenieure von AMS die Sperrbedingungen entfernen oder ändern können.

Haben AMS-Techniker Zugriff auf Kundendaten, die in Amazon EBS, Amazon EFS und Amazon FSx gespeichert sind?

AMS-Techniker können sich als Administrator Amazon EC2 Amazon-Instances anmelden. In bestimmten Szenarien, zu denen unter anderem Betriebssystemprobleme und Patch-Fehler gehören, sind Administratorrechte für die Problembehebung erforderlich. AMS-Techniker greifen in der Regel auf das Systemvolume zu, um festgestellte Probleme zu beheben. Der Zugriff für AMS-Techniker ist jedoch nicht auf das Systemvolumen beschränkt.

Wie wird der Zugriff für Automatisierungsrollen mit hohen Rechten für meine Umgebungen eingeschränkt oder kontrolliert?

Die `ams-access-admin` Rolle wird ausschließlich von AMS Automation verwendet. Diese Automatisierungen stellen die erforderlichen Ressourcen bereit, verwalten und warten, die AMS zur Bereitstellung in Ihren Umgebungen für die Erfassung von Telemetrie-, Gesundheits- und Sicherheitsdaten zur Ausführung betrieblicher Funktionen benötigt. AMS-Techniker können keine Automatisierungsrollen übernehmen und sind durch die Rollenzuweisung in internen Systemen eingeschränkt. Zur Laufzeit wendet AMS dynamisch auf jede Automatisierung eine nach unten abgegrenzte Sitzungsrichtlinie mit den geringsten Rechten an. Diese Sitzungsrichtlinie schränkt die Funktionen und Berechtigungen der Automatisierung ein.

Wie implementiert AMS das Prinzip der geringsten Rechte, wie es im AWS Well-Architected Framework für Automatisierungsrollen befürwortet wird?

Zur Laufzeit wendet AMS auf jede Automatisierung eine nach unten begrenzte Sitzungsrichtlinie mit den geringsten Rechten an. Diese Sitzungsrichtlinie mit eingeschränktem Geltungsbereich schränkt die Funktionen und Berechtigungen der Automatisierung ein. Für Sitzungsrichtlinien, die über Berechtigungen zum Erstellen von IAM-Ressourcen verfügen, muss auch eine Berechtigungsgrenze festgelegt werden. Diese Berechtigungsgrenze reduziert das Risiko einer Rechteeskalation. Jedes Team führt eine Sitzungsrichtlinie ein, die nur von diesem Team verwendet wird.

Welche Protokollierungs- und Überwachungssysteme werden verwendet, um unbefugte Zugriffsversuche oder verdächtige Aktivitäten im Zusammenhang mit Automatisierungsrollen zu erkennen?

AWS verwaltet zentrale Repositorys, die zentrale Funktionen zur Protokollarchivierung für den internen Gebrauch durch AWS Serviceteams bereitstellen. Diese Protokolle werden in Amazon

S3 gespeichert, um eine hohe Skalierbarkeit, Haltbarkeit und Verfügbarkeit zu gewährleisten. AWS Serviceteams können dann Serviceprotokolle in einem zentralen Protokolldienst sammeln, archivieren und einsehen.

Produktionshosts unter AWS werden mithilfe von Master-Baseline-Images bereitgestellt. Die Baseline-Images sind mit einer Reihe von Standardkonfigurationen und -funktionen ausgestattet, zu denen auch Protokollierung und Überwachung aus Sicherheitsgründen gehören. Diese Protokolle werden gespeichert und können von AWS Sicherheitsteams zur Ursachenanalyse im Falle eines vermuteten Sicherheitsvorfalls abgerufen werden.

Die Protokolle für einen bestimmten Host stehen dem Team zur Verfügung, dem dieser Host gehört. Teams können ihre Protokolle nach Betriebs- und Sicherheitsanalysen durchsuchen.

Wie werden Sicherheitsvorfälle oder Sicherheitslücken im Zusammenhang mit der Automatisierungsinfrastruktur behandelt, und welche Protokolle helfen bei einer schnellen Reaktion und Abwehr?

AWS In Notfallplänen und Playbooks zur Reaktion auf Sicherheitsvorfälle wurden Tools und Prozesse zur Erkennung, Abschwächung, Untersuchung und Bewertung von Sicherheitsvorfällen definiert und getestet. Diese Pläne und Playbooks enthalten Richtlinien für die Reaktion auf potenzielle Datenschutzverletzungen gemäß den vertraglichen und behördlichen Anforderungen.

Werden regelmäßige Sicherheitsbewertungen, Schwachstellenscans und Penetrationstests an der Automatisierungsinfrastruktur durchgeführt?

AWS Security führt mithilfe einer Vielzahl von Tools regelmäßige Schwachstellenscans auf den Host-Betriebssystemen, Webanwendungen und Datenbanken in der AWS Umgebung durch. AWS Sicherheitsteams abonnieren außerdem News-Feeds mit Informationen über mögliche Fehler von Anbietern und überwachen proaktiv die Websites der Anbieter und andere relevante Informationsquellen im Hinblick auf neue Patches.

Inwiefern ist der Zugriff auf die Automatisierungsinfrastruktur auf autorisiertes Personal beschränkt?

Der Zugriff auf AWS Systeme wird auf der Grundlage der geringsten Rechte zugewiesen und von einer autorisierten Person genehmigt. Aufgaben und Verantwortungsbereiche (z. B. Zugriffsanforderung und Genehmigung, Anfrage und Genehmigung von Änderungen, Entwicklung,

Testen und Bereitstellen von Änderungen usw.) sind auf verschiedene Personen aufgeteilt, um unbefugte oder unbeabsichtigte Änderungen oder Missbräuche von Systemen zu verhindern. AWS Gruppen- oder gemeinsame Konten sind innerhalb der Systemgrenzen nicht zulässig.

Welche Maßnahmen werden ergriffen, um Sicherheitsstandards aufrechtzuerhalten und unbefugten Zugriff oder Datenschutzverletzungen in der Automatisierungspipeline zu verhindern?

Der Zugriff auf Ressourcen, einschließlich Dienste, Hosts, Netzwerkgeräte sowie Windows- und UNIX-Gruppen, wird im AWS firmeneigenen Berechtigungsverwaltungssystem vom entsprechenden Eigentümer oder Manager genehmigt. Das Protokoll des Tools zur Rechteverwaltung erfasst Anfragen nach Zugriffsänderungen. Durch Änderungen der Jobfunktion wird dem Mitarbeiter automatisch der Zugriff auf Ressourcen entzogen. Der fortgesetzte Zugriff für diesen Mitarbeiter muss beantragt und genehmigt werden.

AWS erfordert eine Zwei-Faktor-Authentifizierung über einen zugelassenen kryptografischen Kanal für die Authentifizierung am internen AWS Netzwerk von entfernten Standorten aus. Firewall-Geräte schränken den Zugriff auf die Computerumgebung ein, setzen die Grenzen von Computerclustern durch und schränken den Zugriff auf Produktionsnetzwerke ein.

Es werden Verfahren implementiert, um Auditinformationen und Audit-Tools vor unbefugtem Zugriff, Änderung und Löschung zu schützen. Auditaufzeichnungen enthalten eine Reihe von Datenelementen, um die erforderlichen Analyseanforderungen zu erfüllen. Darüber hinaus stehen die Prüfaufzeichnungen autorisierten Benutzern zur Prüfung oder Analyse auf Anfrage und als Reaktion auf sicherheitsrelevante oder geschäftskritische Ereignisse zur Verfügung.

Die Benutzerzugriffsrechte auf AWS Systeme (z. B. Netzwerk, Anwendungen, Tools usw.) werden innerhalb von 24 Stunden nach der Kündigung oder Deaktivierung widerrufen. Inaktive Benutzerkonten werden deaktiviert und mindestens alle 90 Tage and/or entfernt.

Ist die Erkennung oder Überwachung von Anomalien für die Zugriffs- oder Auditprotokollierung aktiviert, um Rechteerweiterungen oder Zugriffsmissbrauch zu erkennen und das AMS-Team proaktiv zu benachrichtigen?

Die Produktions-Hosts unter AWS sind aus Sicherheitsgründen mit einer Protokollierung ausgestattet. Dieser Dienst protokolliert menschliche Aktionen auf Hosts, einschließlich Anmeldungen,

fehlgeschlagene Anmeldeversuche und Abmeldungen. Diese Protokolle werden gespeichert und können von AWS Sicherheitsteams zur Ursachenanalyse im Falle eines vermuteten Sicherheitsvorfalls abgerufen werden. Die Protokolle für einen bestimmten Host stehen auch dem Team zur Verfügung, dem dieser Host gehört. Serviceteams steht ein Front-End-Tool zur Protokollanalyse zur Verfügung, mit dem sie ihre Protokolle nach Betriebs- und Sicherheitsanalysen durchsuchen können. Es werden Prozesse implementiert, um Protokolle und Audit-Tools vor unbefugtem Zugriff, Änderung und Löschung zu schützen. Das AWS Sicherheitsteam führt Protokollanalysen durch, um Ereignisse auf der Grundlage definierter Risikomanagementparameter zu identifizieren.

Welche Arten von Kundendaten werden aus von AMS verwalteten Konten extrahiert und wie werden sie verwendet und gespeichert?

AMS greift zu keinem Zweck auf Ihre Inhalte zu und verwendet sie auch nicht. AMS definiert Kundeninhalte als Software (einschließlich Maschinenbilder), Daten, Text, Audio, Video oder Bilder, an die ein Kunde oder ein Endbenutzer AWS-Services in Verbindung mit einem Kundenkonto AWS zur Verarbeitung, Speicherung oder zum Hosten überträgt, sowie alle Rechenergebnisse, die ein Kunde oder sein Endnutzer aus dem Vorstehenden durch deren Nutzung ableitet. AWS-Services

Überwachung und Eventmanagement in AMS Accelerate

Das AMS Accelerate-Überwachungssystem überwacht Ihre AWS Ressourcen auf Ausfälle, Leistungseinbußen und Sicherheitsprobleme.

Als verwaltetes Konto konfiguriert und implementiert AMS Accelerate Alarme für die entsprechenden AWS Ressourcen, überwacht diese Ressourcen und führt bei Bedarf Abhilfemaßnahmen durch.

Das AMS Accelerate-Überwachungssystem stützt sich auf interne Tools wie Resource Tagger und Alarm Manager und nutzt AWS-Services Amazon CloudWatch (CloudWatch) AWS AppConfig, Amazon EventBridge (früher bekannt als CloudWatch), Amazon GuardDuty, Amazon Macie und. AWS Health

AMS Accelerate bietet eine Reihe von Betriebsdienstleistungen, die Sie dabei unterstützen, betriebliche Exzellenz zu erreichen. AWS Einen schnellen Überblick darüber, wie AMS Ihren Teams dabei hilft, AWS Cloud mit einigen unserer wichtigsten betrieblichen Funktionen, darunter Helpdesk rund um die Uhr, proaktive Überwachung, Sicherheit, Patching, Protokollierung und Backup, zu operativer Exzellenz zu gelangen, finden Sie in den AMS-Referenzarchitekturdiagrammen.

Themen

Informationen zur Überwachung von Amazon EKS finden Sie unter Überwachung und Vorfallmanagement für Amazon EKS in AMS Accelerate

Was ist Überwachung?

AMS Accelerate Monitoring bietet folgende Vorteile:

- Eine Standardkonfiguration, mit der Richtlinien für Ihr verwaltetes Konto für alle oder die von Ihnen ausgewählten unterstützten AWS Ressourcen erstellt, verwaltet und bereitgestellt werden.
- Eine Überwachungsbasis, sodass Sie über ein Standardschutzniveau verfügen, auch wenn Sie keine andere Überwachung für Ihre verwalteten Konten konfigurieren. Weitere Informationen finden Sie unter Warnmeldungen aus der Basisüberwachung in AMS.
- Die Möglichkeit, die grundlegenden Ressourcenalarme an Ihre Anforderungen anzupassen.
- Automatische Behebung von Warnmeldungen durch AMS Operations, wenn möglich, um die Auswirkungen auf Ihre Anwendungen zu verhindern oder zu reduzieren. Wenn Sie beispielsweise eine eigenständige EC2 Amazon-Instance verwenden und diese die Systemintegritätsprüfung nicht besteht, versucht AMS, die Instance wiederherzustellen, indem sie gestoppt und neu gestartet wird. Weitere Informationen finden Sie unter Automatische AMS-Behebung von Warnmeldungen.
- Einblick in aktive und zuvor behobene Warnmeldungen mithilfe von OpsCenter. Wenn Sie beispielsweise eine unerwartet hohe CPU-Auslastung auf einer EC2 Amazon-Instance haben, können Sie Zugriff auf die AWS Systems Manager Konsole anfordern (einschließlich Zugriff auf die OpsCenter Konsole) und diese OpsItem direkt in der OpsCenter Konsole anzeigen.
- Untersuchung von Warnmeldungen, um die geeigneten Maßnahmen zu ermitteln. Weitere Informationen finden Sie unter Vorfallmanagement in AMS Accelerate.
- Benachrichtigungen, die auf der Grundlage der Konfiguration in Ihrem Konto und der unterstützten AWS Dienste generiert werden. Die Überwachungskonfiguration eines Kontos bezieht sich auf alle Ressourcenparameter im Konto, die eine Warnung auslösen. Die Überwachungskonfiguration eines Kontos umfasst CloudWatch Alarmdefinitionen und EventBridge (früher als CloudWatch Ereignisse bezeichnet), die die Warnung auslösen (Alarm oder Ereignis). Weitere Hinweise zu den Ressourcenparametern finden Sie unterWarnmeldungen aus der Basisüberwachung in AMS.
- Benachrichtigung über drohende, andauernde, sich wiederholende oder potenzielle Ausfälle, Leistungseinbußen oder Sicherheitsprobleme, die durch die in einem Konto konfigurierte Basisüberwachung verursacht werden (auch als Warnung bezeichnet). Zu den Warnmeldungen gehören beispielsweise ein CloudWatch Alarm, ein Ereignis oder ein Ergebnis eines AWS Dienstes, z. B. GuardDuty oder. AWS Health

So funktioniert die Überwachung

Sehen Sie sich die folgenden Grafiken zur Überwachungsarchitektur in AWS Managed Services (AMS) an.

Das folgende Diagramm zeigt die AMS Accelerate-Überwachungsarchitektur.

Nachdem Ihre Ressourcen auf der Grundlage der mit Resource Tagger definierten Richtlinie markiert und die Alarmdefinitionen bereitgestellt wurden, werden in der folgenden Liste die AMS-Überwachungsprozesse beschrieben.

- Generierung: Zum Zeitpunkt der Kontoeröffnung konfiguriert AMS die Basisüberwachung (eine Kombination aus CloudWatch (CW-) Alarmen und CW-Ereignisregeln) für all Ihre Ressourcen, die in einem verwalteten Konto erstellt wurden. Die Basisüberwachungskonfiguration generiert eine Warnung, wenn ein CW-Alarm ausgelöst oder ein CW-Ereignis ausgelöst wird.
- Aggregation: Alle von Ihren Ressourcen generierten Benachrichtigungen werden an das AMS-Überwachungssystem gesendet, indem sie an ein SNS-Thema im Konto weitergeleitet werden. Sie können auch konfigurieren, wie AMS EC2 Amazon-Benachrichtigungen gruppiert. AMS gruppiert entweder alle Alerts, die sich auf dieselbe EC2 Instance beziehen, zu einem einzigen Incident oder erstellt je nach Wunsch einen Incident pro Alert. Sie können diese Konfiguration jederzeit ändern, indem Sie mit Ihrem Cloud Service Delivery Manager oder Cloud Architect zusammenarbeiten.
- Verarbeitung: AMS analysiert die Warnmeldungen und verarbeitet sie auf der Grundlage ihres Auswirkungspotenzials. Warnmeldungen werden wie im Folgenden beschrieben verarbeitet.
  - Warnmeldungen mit bekannten Auswirkungen auf den Kunden: Diese führen zur Erstellung eines neuen Vorfallberichts, und AMS folgt dem Incident-Management-Prozess.

    Beispielwarnung: Eine EC2 Amazon-Instance besteht eine Systemintegritätsprüfung nicht. AMS versucht, die Instance wiederherzustellen, indem sie gestoppt und neu gestartet wird.
  - Benachrichtigungen mit ungewisser Auswirkung auf den Kunden: Für diese Art von Benachrichtigungen sendet AMS einen Vorfallbericht, in dem Sie in vielen Fällen aufgefordert werden, die Auswirkungen zu überprüfen, bevor AMS Maßnahmen ergreift. Wenn die infrastrukturbezogenen Prüfungen jedoch bestanden werden, sendet AMS Ihnen keinen Vorfallbericht.

    Beispiel: Eine Warnung für eine CPU-Auslastung von > 85% für mehr als 10 Minuten auf einer EC2 Amazon-Instance kann nicht sofort als Vorfall eingestuft werden, da dieses Verhalten je nach Nutzung zu erwarten sein könnte. In diesem Beispiel führt AMS Automation infrastrukturbezogene Prüfungen der Ressource durch. Wenn diese Prüfungen erfolgreich sind, sendet AMS keine Warnmeldung, auch wenn die CPU-Auslastung 99% überschritten hat. Wenn Automation feststellt, dass infrastrukturbezogene Prüfungen an der Ressource fehlschlagen, sendet AMS eine Warnmeldung und prüft, ob Abhilfemaßnahmen erforderlich sind. Warnmeldungen werden in diesem Abschnitt ausführlich behandelt. AMS bietet in

der Benachrichtigung Optionen zur Risikominderung. Wenn Sie auf die Benachrichtigung antworten, in der bestätigt wird, dass es sich bei der Warnung um einen Vorfall handelt, erstellt AMS einen neuen Vorfallbericht und der AMS-Incident-Management-Prozess beginnt. Servicebenachrichtigungen, bei denen die Antwort „keine Auswirkungen auf den Kunden“ oder drei Tage lang überhaupt keine Antwort erhalten, werden als gelöst markiert, und die entsprechende Warnung wird als gelöst markiert.

- Benachrichtigungen ohne Auswirkungen auf den Kunden: Wenn AMS nach der Auswertung feststellt, dass die Warnung keine Auswirkungen auf den Kunden hat, wird die Warnung geschlossen.

  AWS Health Benachrichtigt beispielsweise über eine EC2 Instanz, die ersetzt werden muss, diese Instanz aber inzwischen beendet wurde.

EC2 Benachrichtigungen, gruppiert nach Instanzen

Sie können die AMS-Überwachung so konfigurieren, dass Warnmeldungen derselben EC2 Instanz zu einem einzigen Vorfall zusammengefasst werden. Ihr Cloud Service Delivery Manager oder Cloud Architect kann dies für Sie konfigurieren. Es gibt vier Parameter, die Sie für jedes von AMS verwaltete Konto konfigurieren können.

1. Umfang: Wählen Sie entweder kontoweit oder tagbasiert.
   - Um eine Konfiguration anzugeben, die für jede EC2 Instanz in diesem Konto gilt, wählen Sie scope = account-wide.
   - Um eine Konfiguration anzugeben, die nur für EC2 Instanzen in diesem Konto mit einem bestimmten Tag gilt, wählen Sie scope = tag-based.
2. Gruppierungsregel: Wählen Sie entweder „klassisch“ oder „Instanz“.
   - Um die Gruppierung auf Instanzebene für jede Ressource in Ihrem Konto zu konfigurieren, wählen Sie Bereich = Kontoweit und Gruppierungsregel = Instanz.
   - Um bestimmte Ressourcen in Ihrem Konto für die Gruppierung auf Instanzebene zu konfigurieren, taggen Sie diese Instanzen und wählen Sie dann Bereich = Tag-basiert und Gruppierungsregel = Instanzebene.
   - Um die Instanzgruppierung nicht für Benachrichtigungen in Ihrem Konto zu verwenden, wählen Sie Gruppierungsregel = klassisch.
3. Interaktionsoption: Wählen Sie entweder „Keine“, „Nur Bericht“ oder „Standard“.

- Damit AMS während der aktiven Konfiguration keine Vorfälle erstellt oder Automatisierungen für Alarme von diesen Ressourcen aus durchführt, wählen Sie „Keine“.
- Damit AMS keine Vorfälle erstellt oder Automatisierungen für Alarme aus diesen Ressourcen ausführt, solange die Konfiguration aktiv ist, und keine automatisierten Systems Manager Manager-Dokumente ausführt, sondern Aufzeichnungen dieser Ereignisse in Ihre Berichterstattung einbezieht, wählen Sie Nur Bericht. Dies kann nützlich sein, wenn Sie die Anzahl der Support-Anfragen reduzieren möchten, mit denen Sie zu tun haben, und wenn einige Vorfälle, die von einigen Ressourcen stammen, nicht sofort bearbeitet werden müssen, z. B. wenn es sich um Vorfälle handelt, bei denen es sich nicht um ein produktives Konto handelt.
- Wählen Sie Standard, damit AMS Ihre Benachrichtigungen verarbeiten, Automatisierungen ausführen und bei Bedarf Incident-Fälle erstellen kann.

4. Lösung nach: Wählen Sie entweder 24 Stunden, 48 Stunden oder 72 Stunden. Stellen Sie abschließend ein, wann Vorfälle automatisch geschlossen werden. Wenn die Zeit seit der letzten Fallkorrespondenz den konfigurierten Wert „Nach lösen“ erreicht, wird der Vorfall geschlossen.

Warnungsbenachrichtigung

Als Teil der Alert-Verarbeitung erstellt AWS Managed Services (AMS) auf der Grundlage der Auswirkungsanalyse einen Vorfall und leitet den Incident-Management-Prozess zur Behebung ein, sobald die Auswirkungen festgestellt werden können. Wenn die Auswirkung nicht festgestellt werden kann, sendet AMS im Rahmen einer Servicemeldung eine Warnmeldung an die mit Ihrem Konto verknüpfte E-Mail-Adresse. In einigen Szenarien wird diese Warnmeldung nicht gesendet. Wenn die infrastrukturbezogenen Prüfungen beispielsweise aufgrund einer Warnung bei hoher CPU-Auslastung erfolgreich sind, wird keine Warnmeldung an Sie gesendet. Weitere Informationen finden Sie im Diagramm zur AMS-Überwachungsarchitektur für den Prozess zur Behandlung von Warnmeldungen unter. So funktioniert die Überwachung

Tag-basierte Warnmeldung

Verwenden Sie Tags, um Warnmeldungen für Ihre Ressourcen an verschiedene E-Mail-Adressen zu senden. Es hat sich bewährt, tagbasierte Warnmeldungen zu verwenden, da Benachrichtigungen, die an eine einzige E-Mail-Adresse gesendet werden, zu Verwirrung führen können, wenn mehrere Entwicklerteams dasselbe Konto verwenden. Tag-basierte Warnmeldungen werden von den von Ihnen ausgewählten EC2 Benachrichtigungen, gruppiert nach Instanzen Einstellungen nicht beeinflusst.

Mit tagbasierten Warnmeldungen können Sie:

- Benachrichtigungen an eine bestimmte E-Mail-Adresse senden: Taggen Sie Ressourcen mit Benachrichtigungen, die an eine bestimmte E-Mail-Adresse gesendet werden müssen, mit dem`key = OwnerTeamEmail`,`value = EMAIL_ADDRESS`.
- Benachrichtigungen an mehrere E-Mail-Adressen senden: Um mehrere E-Mail-Adressen zu verwenden, geben Sie eine durch Kommas getrennte Werteliste an. Zum Beispiel `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. Die Gesamtzahl der Zeichen für das Wertfeld darf 260 nicht überschreiten.
- Verwenden Sie einen benutzerdefinierten Tag-Schlüssel: Um einen benutzerdefinierten Tag-Schlüssel zu verwenden, geben Sie Ihrem CSDM den Namen des benutzerdefinierten Tag-Schlüssels in einer E-Mail an, in der ausdrücklich Ihre Zustimmung zur Aktivierung automatisierter Benachrichtigungen für die tagbasierte Kommunikation erteilt wird. Es hat sich bewährt, für alle Ihre Instances und Ressourcen dieselbe Tagging-Strategie für Kontakt-Tags zu verwenden.

> **Note**
>
> Der Schlüsselwert `OwnerTeamEmail` muss nicht in Camel Case angegeben werden. Bei Tags wird jedoch zwischen Groß- und Kleinschreibung unterschieden, und es empfiehlt sich, das empfohlene Format zu verwenden.
> Die E-Mail-Adresse muss vollständig angegeben werden, mit dem „at“ -Zeichen (@), um den lokalen Teil von der Domain zu trennen. Beispiele für ungültige E-Mail-Adressen: `Team.AppATabc.xyz` oder`john.doe`. Allgemeine Hinweise zu Ihrer Tagging-Strategie finden Sie unter Tagging-Ressourcen AWS. Fügen Sie Ihren Tags keine persönlich identifizierbaren Informationen (PII) hinzu. Verwenden Sie nach Möglichkeit Verteilerlisten oder Aliase.
> Tag-basierte Warnmeldungen werden für Ressourcen der folgenden Amazon Services unterstützt: EC2, Elastic Block Store (EBS), Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS) OpenSearch, Elastic File System (EFS) und VPN. FSx Site-to-Site

Warnmeldungen aus der Basisüberwachung in AMS

Erfahren Sie mehr über die Standardeinstellungen für die Überwachung von AMS Accelerate. Weitere Informationen finden Sie unter Überwachung und Eventmanagement in AMS Accelerate.

Die folgende Tabelle zeigt, was überwacht wird und welche Standardschwellenwerte für Warnmeldungen gelten. Sie können die Warnschwellenwerte mit einem benutzerdefinierten Konfigurationsdokument ändern oder eine Serviceanfrage einreichen. Anweisungen zum Ändern Ihrer benutzerdefinierten Alarmkonfiguration finden Sie unter. Konfiguration des Accelerate-Alarms ändern Um Benachrichtigungen zu erhalten, wenn Alarme ihren Schwellenwert überschreiten, können Sie zusätzlich zum standardmäßigen Warnprozess von AMS die Alarmkonfigurationen überschreiben. Detaillierte Anweisungen finden Sie unter Beschleunigen Sie den Alarm Manager.

Amazon CloudWatch bietet eine erweiterte Aufbewahrung von Metriken. Weitere Informationen finden Sie unter CloudWatch Limits.

> **Note**
>
> AMS Accelerate kalibriert seine Basisüberwachung regelmäßig. Neue Konten werden immer mit der neuesten Basisüberwachung aufgenommen. In der Tabelle wird die Basisüberwachung für ein neu eingeführtes Konto beschrieben. AMS Accelerate aktualisiert die Basisüberwachung für bestehende Konten in regelmäßigen Abständen, und es kann zu Verzögerungen kommen, bis die Updates verfügbar sind.

Warnmeldungen aus der Basisüberwachung

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Bei Warnmeldungen mit Sternchen (*) bewertet AMS proaktiv die Auswirkungen und behebt, wenn möglich. Wenn eine Behebung nicht möglich ist, erstellt AMS einen Vorfall. Wenn die Automatisierung das Problem nicht behebt, informiert AMS Sie über den Vorfall und ein AMS-Techniker wird hinzugezogen. Wenn Sie sich für das Direct-Customer-Alerts SNS-Thema entscheiden, werden diese Benachrichtigungen außerdem direkt an Ihre E-Mail-Adresse gesendet.		
Application Load Balancer Balancer-Instanz	ApplicationLoadBalancerErrorCount (HTTPCode_ELB_5xx_Count/RequestCount) *100 Summe > 15% für 1 Minute, 5 aufeinanderfolgende Male.	Anzahl der LoadBalancer HTTP 5XX-Fehler der Anwendung CloudWatch Alarm bei zu großer Anzahl von HTTP 5XX-Antwortcodes, die vom

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
		Loadbalancer generiert wurden.
Application Load Balancer Balancer-Instanz	RejectedConnectionCount Summe > 0% für 1 Minute, 5 aufeinanderfolgende Male.	Anzahl der LoadBalancer abgelehnten Verbindungen durch die Anwendung CloudWatch Alarm, wenn die Anzahl der Verbindungen, die abgelehnt wurden, weil der Load Balancer sein Maximum erreicht hat
Ziel des Application Load Balancer	TargetConnectionErrorCount (HTTPCode_Target_5 xx_Count/RequestCount) *100 Summe > 15% für 1 Minute, 5 aufeinanderfolgende Male.	$ {ElasticLoadBalancingV2::TargetGroup:FullName} — Anzahl der Verbindungsfehler im LoadBalancer Anwendungsziel — $ {ElasticLoadBalancingV2:TargetGroup: :UUID} CloudWatch Alarm bei zu großer Anzahl von HTTP 5XX-Antwortcodes, die von einem Ziel generiert wurden.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Ziel des Application Load Balancer	ApplicationLoadBalancerTargetGroupErrorCount Summe > 0% für 1 Minute, 5 aufeinanderfolgende Male.	$ {ElasticLoadBalancingV2::TargetGroup:FullName} — Anzahl der HTTP-Fehler für das LoadBalancer Anwendungsziel 5XX — ${ElasticLoadBalancingV2:TargetGroup: :UUID} CloudWatch Alarm, wenn die Anzahl der Verbindungen zwischen dem Load Balancer und den registrierten Instances nicht erfolgreich hergestellt werden konnte.
EC2 Amazon-Instanz — alle OSs	CPUUtilization* > 95% für 5 Minuten, 6 aufeinanderfolgende Male.	${EC2::InstanceId}: CPU zu hoch CloudWatch Alarm. Eine hohe CPU-Auslastung ist ein Indikator für eine Änderung des Anwendungsstatus wie Deadlocks, Endlosschleifen, böswillige Angriffe und andere Anomalien. Dies sind Alarme. Direct-Customer-Alerts

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
EC2 Amazon-Instanz — alle OSs	StatusCheckFailed > 0% für 5 Minuten, dreimal hintereinander.	$ {EC2::InstanceId}: Statusprüfung fehlgeschlagen CloudWatch Alarm. Status Check Failed gibt an, dass eine EC2 Amazon-Instance mit der angegebenen ID eine oder mehrere ihrer automatisierten Statusprüfungen nicht bestanden hat. Dies bedeutet, dass bei der Instance ein Problem auftritt, das verhindert, dass sie ordnungsgemäß funktioniert oder erreichbar ist.
EC2 Amazon-Instanz — Linux	Mindestens mem_used_percent >= 95% für 5 Minuten, 6 Mal hintereinander.	$ {EC2::InstanceId}: Speicherplatz frei CloudWatch Alarm. Memory Free gibt an, dass der verfügbare Arbeitsspeicher (RAM) auf der angegebenen EC2 Amazon-Instance unter einen definierten Schwellenwert gefallen ist. Dies kann zu Speicherproblemen und Systemabstürzen führen und weist darauf hin, dass die Instance möglicherweise mehr RAM benötigt. Dies sind Direct-Customer-Alerts Alarme.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
EC2 Amazon-Instanz — Linux	Durchschnittlich swap_used _percent **>=** 95% für 5 Minuten, 6 Mal hintereinander.	$ {EC2::InstanceId}: Kostenlos tauschen CloudWatch Alarm. Average swap_used_percent auf einer EC2 Amazon-Instance gibt an, dass der durchschnittliche Prozentsatz des zugewiese nen Swap-Speichers, der derzeit verwendet wird, einen vordefinierten Schwellen wert überschritten hat. Dies kann zu Leistungseinbußen, Engpässen und Speicherp roblemen führen. Dies sind Alarme Direct-Cu stomer-Alerts.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
EC2 Amazon-Instanz — Linux	Maximaler Anteil von disk_used_percent >= 95% für 5 Minuten, 6 Mal hintereinander.	$ {EC2::InstanceId}: Zu hohe Festplattennutzung — $ {EC2: :Disk: :UUID} CloudWatch Alarm. Disk Usage Too High bedeutet, dass die Festplattenauslastung auf einem bestimmten Amazon EC2 oder auf dem identifizierten Laufwerk fast voll ausgelastet ist. Dies kann zu Leistungseinbußen, Anwendungsfehlern und Systeminstabilität führen. Dies sind Direct-Customer-Alerts Alarme.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
EC2 Amazon-Instanz — Windows	Mindestens verwendeter Arbeitsspeicher in% der zugesandten Byte >= 95% für 5 Minuten, 6 Mal hintereinander.	$ {EC2::InstanceId}: Speicherplatz frei CloudWatch Alarm. Memory Free gibt an, dass der verfügbare Arbeitsspeicher (RAM) auf der angegebenen EC2 Amazon-Instance unter einen definierten Schwellenwert gefallen ist. Dies kann zu Speicherproblemen und Systemabstürzen führen und weist darauf hin, dass die Instance möglicherweise mehr RAM benötigt. Dies sind Direct-Customer-Alerts Alarme.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
EC2 Amazon-Instanz — Windows	Maximaler LogicalDisk Prozentsatz an freiem Speicherplatz <= 5% für 5 Minuten, 6 Mal hintereinander.	$ {EC2::InstanceId}: Zu hohe Festplattennutzung — $ {EC2: :Disk: :UUID} CloudWatch Alarm. Zeigt an, dass der Prozentsatz des freien Speicherplatzes auf einer logischen Festplatte (einer Dateisystempartition) innerhalb einer Amazon EC2 Windows-Instance einen vordefinierten Schwellenwert überschritten hat. Ein Mangel an Festplattenspeicher kann zu Engpässen auf der Festplatte führen Dies sind Direct-Customer-Alerts Alarme.
Amazon EFS	AMSEFSBurstCreditBalanceExhausted. BurstCreditBalance weniger als 1000 für fünfzehn Minuten.	$ {EFS::FileSystemId}: EFS: Burst-Guthabenbilanz CloudWatch Alarm auf BurstCreditBalance dem Amazon EFS-Dateisystem.
Amazon EFS	AMSEFSClientConnectionsLimit. ClientConnections > 24.000 für fünfzehn Minuten.	$ {EFS::FileSystemId}: EFS: Limit für Client-Verbindungen CloudWatch Alarm auf ClientConnections dem Amazon EFS-Dateisystem.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon EFS	AMSEFSThroughputUtilization Limit. EFS-Durchsatzauslastung > 80% für eine Stunde.	$ {EFS::FileSystemId}: EFS: Limit für die Durchsatz auslastung CloudWatch Alarm zur Durchsatzauslastung des Amazon EFS-Dateisystems.
Amazon EFS	AMSEFSPercentIOLimit. Prozent IOLimit > 95 für fünfundsiebzig Minuten.	$ {EFS::FileSystemId}: EFS: Prozent IOLimit CloudWatch Alarm für den Prozentsatz IOLimit des Amazon EFS-Dateisystems.
Amazon EKS	Weitere Informationen finden Sie unter Amazon EKSBasiswarnungen bei der Überwachung und dem Incident-Management für Amazon EKS in AMS Accelerate.	
Elastic Load Balancing Balancing-Instanz	SpilloverCountBackendConnectionErrors > 1 für 1 Minute, 15 aufeinander erfolgende Male.	Klassischer Alarm mit LoadBalancer Spillover-Zählung CloudWatch Alarm bei zu vielen Anfragen, die abgelehnt wurden, weil die Surge-Warteschlange voll ist.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Elastic Load Balancing Balancing-Instanz	HTTPCode_ELB_5xx_Count Summe > 0 für 5 Minuten, 3 aufeinanderfolgende Male.	CloudWatch Alarm bei zu großer Anzahl von HTTP 5XX-Antwortcodes, die vom Load Balancer stammen.
Elastic Load Balancing Balancing-Instanz	SurgeQueueLength > 100 für 1 Minute, 15 aufeinanderfolgende Male.	Klassischer Alarm bei LoadBalancer Überspann ungswarteschleife. CloudWatch Alarm, wenn zu viele Anfragen noch weitergel eitet werden müssen.
FSx für ONTAP	AMSFSXONTAPIOPSUti lization. FSX: ONTAP IOPS-Ausl astung > 80% für zwei Stunden.	$ {FSx::}: FSX:ONTAP IOPS-Auslastung FileSystemId CloudWatch Alarm bei der IOPS-Nutzungsbegrenzung der für ONTAP-Instance. FSx
FSx für ONTAP	AMSFSXONTAPThrough putNutzung. FSX: ONTAP Durchsatz auslastung > 80% für zwei Stunden.	$ {FSx::FileSystemId}: FSX:ONTAP Durchsatz auslastung CloudWatch Alarm bezüglich der Durchsatzgrenze für das ONTAP-Volume FSx .
FSx für ONTAP	AMSFSXONTAPVolumeI nodeUtilization. FSX: ONTAP Inode-Aus lastung > 80% für zwei Stunden.	$ {FSx::} :$ {: :ONTAP::F ileSystemId} FSX:ONTAP FSx Inode-Auslastung VolumeId CloudWatch Alarm bei der Begrenzung der Dateikapa zitätsauslastung des Volumes für ONTAP. FSx

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
FSx für ONTAP	AMSFSXONTAPVolumeCapacityUtilization. FSX: ONTAP Volumenauslastung > 80% für zwei Stunden.	$ {FSx::FileSystemId} :$ {: :ONTAP::} FSx VolumeId CloudWatch Alarm bei der Kapazitätsauslastung des Volumes FSx für ONTAP.
FSx für Windows-Dateiserver	AMSFSXWindowsThroughputUtilization. FSX: Windows-Durchsatzauslastung > 80% für zwei Stunden.	$ {FSx::FileSystemId}: fsx:Windows-Durchsatzauslastung CloudWatch Alarm bei der Durchsatzbegrenzung der FSx Windows-Dateiserver-Instanz.
FSx für Windows-Dateiserver	AMSFSXWindowsIOPSUtilization. FSX: Windows-IOPS-Auslastung > 80% für zwei Stunden.	$ {FSx::FileSystemId}: fsx:Windows-IOPS-Auslastung CloudWatch Alarm bei der IOPS-Nutzungsbegrenzung der FSx Windows-Dateiserver-Instanz.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
GuardDuty Dienst	Nicht zutreffend; alle Ergebnisse (Bedrohungszwecke) werden überwacht. Jeder Befund entspricht einer Warnung. Änderungen der GuardDuty Ergebnisse. Zu solchen Änderungen gehören beispielsweise neu generierte Ergebnisse oder alle nachfolgenden Vorkommen dieser vorhandenen Ergebnisse.	Eine Liste der unterstützten Suchtypen GuardDuty finden Sie unter GuardDuty Aktive Suchtypen.
Gesundheitswesen	AWS Health Dashboard	Benachrichtigungen werden gesendet, wenn sich der Status von AWS Health Dashboard (AWS Health) - Ereignissen in Bezug auf von AMS überwachte Dienste ändert. Weitere Informationen finden Sie unter Unterstützte Dienste.
IAM	Das Amazon EC2 IAM-Instance-Profil ist nicht vorhanden. Das IAM-Instance-Profil fehlt.	Anweisungen zum Ersetzen eines Amazon EC2 IAM-Instance-Profils finden Sie in der IAM-Dokumentation unter Replace IAM role.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
IAM	Das Amazon EC2 IAM-Instanzprofil hat zu viele Richtlinien. Das IAM-Instance-Profil hat 10 Richtlinien und zusätzliche Richtlinien können nicht hinzugefügt werden.	• Ändern Sie das AWS Dienstkontingent für IAM, um die Anzahl der verwalteten Richtlinien pro Rolle auf 20 zu erhöhen. Informationen zu Servicekontingenten finden Sie unter Dienstkontingente anzeigen. • Senken Sie die Anzahl der verwalteten Richtlinien unter das aktuelle IAM-Kontingent, indem Sie nicht benötigte verwaltete Richtlinien für die mit diesen Instanzen verknüpfte IAM-Rolle entfernen. Achten Sie darauf, dass Sie die von AMS geforderten Richtlinien einhalten. • Senken Sie die Anzahl der verwalteten Richtlinien unter das aktuelle IAM-Kontingent, indem Sie die Richtlinien für die diesen Instances zugeordnete IAM-Rolle konsolidieren. Achten Sie darauf, dass Sie die von AMS geforderten Richtlinien einhalten. Die für AMS erforderlichen Richtlinien finden Sie im AMS Accelerate-Benutzerhandbuch

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
		:Details zur Änderung von IAM-Berechtigungen.
Macie	Neu generierte Benachrichtigungen und Aktualisierungen vorhandener Benachrichtigungen. Macie stellt fest, dass sich die Ergebnisse geändert haben. Zu solchen Änderungen gehören beispielsweise neu generierte Ergebnisse oder alle nachfolgenden Vorkommen dieser vorhandenen Ergebnisse.	Amazon Macie Macie-Warnung. Eine Liste der unterstützten Amazon Macie Macie-Warnungstypen finden Sie unter Analysieren der Amazon Macie Macie-Ergebnisse. Beachten Sie, dass Macie nicht für alle Konten aktiviert ist.
NATGateways	PacketsDropCount : Alarm, wenn packetsdropcount über einen Zeitraum von 15 Minuten > 0 ist	NatGateway PacketsDropCount Ein Wert größer 0 kann auf ein vorübergehendes Problem mit dem NAT-Gateway hindeuten, das immer wieder auftritt.
NATGateways	ErrorPortAllocation : Alarm, wenn NAT-Gateways für einen Testzeitraum von mehr als 15 Minuten keinen Port zuweisen konnten	NatGateway ErrorPortAllocation Die Anzahl, wie oft der NAT-Gateway einen Quell-Port nicht zuordnen konnte. Ein Wert größer als Null bedeutet, dass zu viele Verbindungen gleichzeitig geöffnet sind.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
OpenSearch Cluster	ClusterStatus Das rote Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander.	ClusterStatus Rot CloudWatch Alarmanlage. Der AWS KMS Verschlüsselungsschlüssel, der zum Verschlüsseln ruhender Daten in Ihrer Domain verwendet wird, ist deaktiviert. Reaktivieren Sie es, um den normalen Betrieb wiederherzustellen. Weitere Informationen finden Sie unter Red Cluster Status.
OpenSearch Domäne	KMSKeyFehler >= 1 für 1 Minute, 1 Mal hintereinander.	KMS-Schlüsselfehler CloudWatch Alarm. Mindestens ein primärer Shard und dessen Replikate sind keinem Knoten zugewiesen. Weitere Informationen finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service.
OpenSearch Domäne	KMSKeyUnzugänglich >= 1 für 1 Minute, 1 Mal hintereinander.	Fehler beim Zugriff auf den KMS-Schlüssel CloudWatch Alarm. Mindestens ein primärer Shard und dessen Replikate sind keinem Knoten zugewiesen. Weitere Informationen finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
OpenSearch Domäne	ClusterStatus Das gelbe Maximum ist >= 1 für 1 Minute, 1 Mal hinterein ander.	ClusterStatus Gelb Mindestens ein Replikat-Shard ist nicht einem Knoten zugewiesen. Weitere Informati onen finden Sie unter Gelber Clusterstatus.
OpenSearch Domäne	FreeStorageSpace Der Mindestwert ist <= 20480 für 1 Minute, 1 Mal hinterein ander.	Wenig freier Speicherplatz Ein Knoten in Ihrem Cluster hat nur noch 20 GiB freien Speicherplatz. Weitere Informationen finden Sie unter Mangel an verfügbarem Speicherplatz.
OpenSearch Domäne	ClusterIndexWritesBlocked >= 1 für 5 Minuten, 1 Mal hintereinander.	Blockierte Schreibvorgänge im Clusterindex Der Cluster blockiert Schreibanforderungen. Weitere Informationen hierzu finden Sie unter ClusterBl ockException.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
OpenSearch Domäne	Knoten mindestens < x für 1 Tag, 1 aufeinanderfolgende Zeit.	Knoten ausgefallen x ist die Anzahl der Knoten in Ihrem Cluster. Dieser Alarm gibt an, dass mindestens ein Knoten in Ihrem Cluster für einen Tag nicht erreichbar war. Weitere Informationen finden Sie unter Fehlgeschlagene Clusterknoten.
OpenSearch Domäne	CPUUtilization Durchschnitt >= 80% für 15 Minuten, dreimal hintereinander.	Hohe CPU-Auslastung im Datenknoten 100 % CPU-Auslastung sind nicht ungewöhnlich, aber ständig hohe Durchschnittswerte sind problematisch. Erwägen Sie, die Größe vorhandener Instanztypen anzupassen oder Instanzen hinzuzufügen.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
OpenSearch Domäne	JVMMemoryDruck maximal >= 80% für 5 Minuten, dreimal hinterein ander.	Hohe Speicherauslastung im Datenknoten Der Cluster könnte Fehler aufgrund von unzureichendem Speicherplatz erhalten, wenn die Nutzung zunimmt. Ziehen Sie eine vertikale Skalierun g in Betracht. OpenSearch verwendet die Hälfte des RAM einer Instance für den Java-Heap bis zu einer Heap-Größ e von 32 GiB. Sie können Instances bis zu 64 GiB RAM vertikal skalieren. Dann können Sie eine horizontale Skalierung durchführen, indem Sie Instances hinzufügen.
OpenSearch Domäne	Meister CPUUtilization Durchschnitt >= 50% für 15 Minuten, dreimal hinterein ander.	Master-Nodes: Hohe CPU-Auslastung Erwägen Sie die Verwendun g größerer Instance-Typen für Ihre dedizierten Master-Knoten. Aufgrund ihrer Rolle für die Cluster-Stabilität und Blau/Grün-Bereitstellungen sollten dedizierte Master-Kn oten eine geringere durchschn ittliche CPU-Auslastung als Datenknoten haben.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
OpenSearch Domäne	Meistern Sie JVMMemory den Druck maximal >= 80% für 15 Minuten, 1 Mal hintereinander.	Hohe JVM-Speicherauslastung der Masterknoten Erwägen Sie die Verwendung größerer Instance-Typen für Ihre dedizierten Master-Knoten. Aufgrund ihrer Rolle für die Cluster-Stabilität und Blau/Grün-Bereitstellungen sollten dedizierte Master-Knoten eine geringere durchschnittliche CPU-Auslastung als Datenknoten haben.
OpenSearch Instanz	AutomatedSnapshotFailure Das Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander.	Automatischer Snapshot-Fehler CloudWatch Alarm. Ein automatisierter Snapshot ist fehlgeschlagen. Dieser Fehler ist häufig das Ergebnis eines roten Cluster-Integritätsstatus. Weitere Informationen finden Sie unter Status des roten Clusters.
Amazon RDS	Durchschnittliche CPU-Auslastung > 90% für 15 Minuten, 2 aufeinanderfolgende Male.	$ {RDS:: DBInstance Identifier}: CPUUtilization CloudWatch Alarme.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon RDS	Summe von DiskQueueDepth > 75% für 1 Minute, 15 aufeinanderfolgende Male.	$ {RDS:: DBInstance Kennung}: DiskQueue CloudWatch Alarme.
Amazon RDS	Durchschnittlich FreeStorageSpace < 1.073.741.824 Byte für 5 Minuten, 2 aufeinanderfolgende Male.	$ {RDS:: Identifier}: DBInstance FreeStorageSpace CloudWatch Alarme.
Amazon RDS	Warnung „Niedriger Speicherplatz“ Wird ausgelöst, wenn der zugewiesene Speicherplatz für die DB-Instance erschöpft ist.	RDS-EVENT-0007, Einzelheiten finden Sie unter Verwenden der Amazon RDS-Ereignisbenachrichtigung.
Amazon RDS	DB-Instance schlägt fehl Die DB-Instance ist aufgrund einer inkompatiblen Konfiguration oder eines zugrunde liegenden Speicherproblems ausgefallen. Starten Sie a point-in-time-restore für die DB-Instance.	RDS-EVENT-0031, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon RDS	Es wurde kein RDS-0034-Failover versucht. Amazon RDS führt das angeforderte Failover nicht aus, da erst vor Kurzem ein Failover auf dieser DB-Instance erfolgt ist.	RDS-EVENT-0034, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Ungültige Parameter für die RDS — 0035 DB-Instance Beispielsweise konnte MySQL nicht gestartet werden, weil ein speicherbezogener Parameter für diese Instance-Klasse zu hoch gesetzt ist. Ihre Aktion wäre also, den Speicherparameter zu ändern und die DB-Instance neu zu starten.	RDS-EVENT-0035, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Ungültige IDs Subnetz-DB-Instance Die DB-Instance befindet sich in einem inkompatiblen Netzwerk. Einige der angegebenen Subnetze IDs sind ungültig oder existieren nicht.	Dienstereignis. RDS-EVENT-0036, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon RDS	Fehler beim Lesen der Replikation der RDS-0045 DB-Instance Bei der Read-Replikation ist ein Fehler aufgetreten. Weitere Informationen finden Sie in der Ereignismeldung. Informationen zur Behebung von Read Replica-Fehlern finden Sie unter Problembehandlung bei MySQL Read Replica-Problemen.	RDS-EVENT-0045, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	RDS-0057 Fehler beim Erstellen des Statspack-Benutzerkontos Die Replikation auf der Read Replica wurde beendet.	Serviceereignis. RDS-EVENT-0057, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Die Lesereplikation der RDS-0058 DB-Instance wurde beendet Fehler beim Erstellen des Statspack-Benutzerkontos PERFSTAT. Löschen Sie das Konto, bevor Sie die Statspack-Option hinzufügen.	Serviceereignis. RDS-EVENT-0058, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon RDS	Start der Wiederherstellung der DB-Instance Die SQL Server-DB-Instance stellt ihre Spiegelung wieder her. Die Leistung ist beeinträchtigt, bis die Spiegelung wiederhergestellt ist. Datenbank mit einem anderen Wiederherstellungsmodell als FULL gefunden. Das Wiederherstellungsmodell wurde wieder auf FULL umgestellt und die Wiederherstellung mit Spiegelung wurde gestartet. (<dbname>: <recovery model found>[,...])	Serviceveranstaltung. RDS-EVENT-0066 Weitere Informationen finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Ein Failover für das DB-Cluster ist fehlgeschlagen.	RDS-EVENT-0069, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon RDS	S3-Bucket zur Wiederherstellung ungültiger Berechtigungen Die IAM-Rolle, die Sie zum Zugriff auf den Amazon S3-Bucket für die SQL Server-nativen Backups und Wiederherstellungen verwenden, ist falsch konfiguriert. Weitere Informationen finden Sie unter Einrichtung für systemeigenes Backup und Wiederherstellung.	Serviceereignis. RDS-EVENT-0081 Weitere Informationen finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Aurora konnte die Sicherungsdaten aus einem Amazon S3-Bucket nicht kopieren.	RDS-EVENT-0082, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Warnung bei niedrigem Speicherplatz, wenn die DB-Instance mehr als 90% des zugewiesenen Speichers verbraucht hat.	Serviceereignis. RDS-EVENT-0089 Weitere Informationen finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Benachrichtigungsdienst, wenn die Skalierung für den Aurora Serverless DB-Cluster fehlgeschlagen ist.	Dienstereignis. RDS-EVENT-0143 Weitere Informationen finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon RDS	Die DB-Instance hat den Status Ungültig. Es sind keine Aktionen erforderlich. Die Auto Scaling wird später erneut versucht.	RDS-EVENT-0219, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Die DB-Instance hat den Schwellenwert für den Speicher vollständig erreicht, und die Datenbank wurde heruntergefahren.	RDS-EVENT-0221, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Dieses Ereignis weist darauf hin, dass die automatische Skalierung des Amazon RDS-Instance-Speichers nicht skaliert werden kann. Es kann mehrere Gründe geben, warum die automatische Skalierung fehlgeschlagen ist.	RDS-EVENT-0223, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Das Auto Scaling von Speicher hat eine ausstehende Skalierungsspeicheraufgabe ausgelöst, die den maximalen Speicherschwellenwert erreichen würde.	RDS-EVENT-0224, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Der Speichertyp der DB-Instance ist der derzeit in der Availability Zone nicht verfügbar. Die Auto Scaling wird später erneut versucht.	RDS-EVENT-0237, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Amazon RDS	Amazon RDS konnte keine Kapazität für den Proxy bereitstellen, da in Ihren Subnetzen nicht genügend IP-Adressen verfügbar sind.	RDS-EVENT-0243, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon RDS	Der Speicherplatz für Ihren AWS-Konto hat das zulässige Speicherkontingent überschritten.	RDS-EVENT-0254, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
Amazon-Redshift-Cluster	Der Zustand des Clusters, wenn er sich nicht im Wartungsmodus befindet < 1 für 5 Minuten	RedshiftClusterHealthStatus Weitere Informationen finden Sie unter Amazon Redshift mithilfe von CloudWatch Metriken überwachen.
Site-to-Site VPN	VPNTunnelRunter TunnelState <= 0 für 1 Minute, 20 Mal hintereinander.	$ {AWS::EC2::VpnConnectionId} — Inaktiv VPNTunnel TunnelState ist 0, wenn beide Tunnel ausgefallen sind, .5, wenn ein Tunnel aktiv ist, und 1,0, wenn beide Tunnel aktiv sind.

Dienst//Ressourcentyp	Quelle der Warnung und Auslösebedingung	Name und Hinweise der Warnung
Systemmanager-Agent	EC2 Instanzen, die nicht von Systems Manager verwaltet werden Der SSM-Agent ist nicht installiert. Der SSM-Agent ist auf der Instanz installiert, aber der Agentendienst läuft nicht. Der SSM-Agent hat keine Netzwerkroute zum AWS Systems Manager Manager-Dienst.	Es gibt weitere Bedingungen, die zu Störungen des Systems Manager Agent führen können. Weitere Informationen finden Sie unter Problembehandlung bei der Verfügbarkeit verwalteter Knoten.

Informationen zu Abhilfemaßnahmen finden Sie unter. Automatische AMS-Behebung von Warnmeldungen

Sehen Sie sich Andrews Video an, um mehr zu erfahren (7:03)

Benachrichtigungen über anwendungsbezogene Vorfälle in AMS

Verwenden Sie anwendungsorientierte automatische Benachrichtigungen zu Vorfällen, um Ihr Kommunikationserlebnis für Supportfälle, die AMS in Ihrem Namen erstellt, individuell zu gestalten. Wenn Sie diese Funktion verwenden, ruft AMS benutzerdefinierte Workload-Einstellungen von ab, AWS Service Catalog AppRegistryum Ihre AMS-Incident-Kommunikation mit Metadaten zu Ihren Anwendungen anzureichern und den Schweregrad der von AMS in Ihrem Namen erstellten Support-Fälle individuell anzupassen. Um diese Funktion nutzen zu können, müssen Sie zuerst AWS Service Catalog AppRegistry einsteigen.

Weitere Informationen zu den Standardüberwachungsstandards von AMS Accelerate finden Sie unter. Überwachung und Eventmanagement in AMS Accelerate

Integrieren Sie Anwendungen AppRegistry und erstellen Sie sie

Informationen zum AppRegistry Onboarding finden Sie unter Erste Schritte mit AppRegistry im AWS Service Catalog AppRegistry Administratorhandbuch. Verwenden Sie nach dem Onboarding eine der folgenden Methoden, um Anwendungen zu erstellen:

1. AWS Konsole: Weitere Informationen zum Erstellen einer Anwendung AppRegistry über die AWS Konsole finden Sie im AWS Service Catalog AppRegistry Administratorhandbuch unter Anwendungen erstellen.
2. CloudFormation: Sie können Ihre AppRegistry Anwendung genauso definieren wie jede andere Ressource. Weitere Informationen finden Sie unter AWS Service Catalog AppRegistry Ressourcentyp-Referenz im CloudFormation -Benutzerhandbuch.
3. AMS-Automatisierung: Um den Registrierungsprozess für Anträge zu vereinfachen, stellt Ihnen AMS das SSM-Automatisierungsdokument `AWSManagedServices-CreateAppRegistryApplication` zur Verfügung. Um diese Methode zu verwenden, rufen Sie das Dokument von der AWS Systems Manager Konsole aus unter oder mit dem auf https://console.aws.amazon.com/systems-manager/, AWS CLI wie im folgenden Beispiel beschrieben.

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
```

```
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

Erstellen Sie Tags, um die Anreicherung von Kundenvorgängen zu ermöglichen

Sie müssen Ihre Anwendungen taggen, bevor AMS auf Anwendungsmetadaten zugreifen kann. In der folgenden Tabelle sind die erforderlichen Tags aufgeführt.

Tags mit dem Präfix `ams:rt:` werden über Resource Tagger angewendet.

Tag-Schlüssel	Tag-Wert
ams-verwaltet	true
ams:rt:ams-managed	true

Passen Sie den Schweregrad der AMS-Supportfälle für Ihre Anwendungen an

Sie können den Schweregrad der von AMS erstellten Supportfälle anpassen, indem Sie angeben, wie wichtig Ihre Anwendung für Ihr Unternehmen ist. Diese Einstellung wird durch eine Attributgruppe gesteuert, die Ihrer Anwendung in zugeordnet ist AppRegistry. Der Name der Attributgruppe muss dem folgenden Muster entsprechen:

```
AMS.<ApplicationName>.CommunicationOptions
```

Im vorherigen Muster `ApplicationName` muss der mit dem Namen übereinstimmen, der AppRegistry bei der Erstellung der Anwendung verwendet wurde.

Beispielinhalt:

```
{
```

```
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

Dies bestimmt die Schemaversion, die Sie verwenden, und die Teilmenge der verfügbaren Funktionen.

Schemaversion	Funktion
1,0	Maßgeschneiderter Schweregrad für Supportfälle basierend auf dem Kritikalitätswert

Kritikalität

Die Wichtigkeit dieser Anwendung bestimmt den Schweregrad der von den automatisierten AMS-Systemen erstellten Supportfälle.

Zulässige Werte:

```
low|normal|high|urgent|critical
```

Weitere Informationen zu Schweregraden finden Sie SeverityLevelin der AWS Support API-Referenz.

Erforderlich: Ja

Überprüfen Sie die erforderlichen Berechtigungen

Um diese Funktion nutzen zu können, benötigt AMS Zugriff auf die folgenden Berechtigungen: AWS Identity and Access Management

- Ich bin: ListRoleTags
- ich bin: ListUserTags
- Ressourcengruppen, die API taggen: GetResources
- Servicekatalog-App-Registrierung: GetApplication
- Servicekatalog-App-Registrierung: ListAssociatedAttributeGroups
- Servicekatalog-App-Registrierung: GetAttributeGroup

> **Important**
>
> Stellen Sie sicher, dass es keine IAM-Richtlinie oder Service Control Policy (SCP) gibt, die die vorherigen Aktionen ablehnt.

Die API-Aufrufe werden von der Rolle ausgeführt. `ams-access-admin` Das Folgende ist ein Beispiel dafür, was Sie sehen könnten:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

Beschleunigen Sie den Alarm Manager

AMS Accelerate wendet mithilfe des tagbasierten Alarm Managers Alarme auf Ihre AWS Ressourcen an, um eine grundlegende Überwachungsstrategie zu implementieren und sicherzustellen, dass all Ihre AWS Ressourcen überwacht und geschützt werden. Durch die Integration mit dem tagbasierten Alarm Manager können Sie die Konfiguration Ihrer AWS Ressourcen an deren Typ, Plattform und andere Tags anpassen, um sicherzustellen, dass die Ressourcen überwacht werden. Alarm Manager wird während des Onboardings auf Ihrem Accelerate-Konto bereitgestellt.

Wie funktioniert Alarm Manager

Wenn Ihr Konto in AMS Accelerate integriert wird, werden zwei JSON-Dokumente, sogenannte Konfigurationsprofile, in Ihrem Konto in bereitgestellt. AWS AppConfig Beide Profildokumente befinden sich in der Alarm Manager-Anwendung und in der AMS Accelerate-Infrastrukturumgebung.

Die beiden Konfigurationsprofile heißen AMSManagedAlarms (das Standardkonfigurationsprofil) und CustomerManagedAlarms(das Anpassungskonfigurationsprofil).

- Standardkonfigurationsprofil:
  - Die Konfiguration in diesem Profil enthält die Standardkonfiguration, die AMS Accelerate in allen Kundenkonten bereitstellt. Diese Konfiguration enthält die standardmäßige AMS Accelerate-Überwachungsrichtlinie, die Sie nicht ändern sollten, da AMS Accelerate dieses Profil jederzeit aktualisieren und alle von Ihnen vorgenommenen Änderungen löschen kann.
  - Wenn Sie eine dieser Definitionen ändern oder deaktivieren möchten, finden Sie weitere Informationen unter Ändern der Standardkonfiguration des Beschleunigungsalarms undDeaktivieren der Standardkonfiguration für den Beschleunigungsalarm.

- Konfigurationsprofil zur Anpassung:
  - Jede Konfiguration in diesem Profil wird vollständig von Ihnen verwaltet. AMS Accelerate überschreibt dieses Profil nicht, es sei denn, Sie fordern es ausdrücklich an.
  - Sie können in diesem Profil beliebige benutzerdefinierte Alarmdefinitionen angeben, und Sie können auch Änderungen an der von AMS Accelerate verwalteten Standardkonfiguration angeben. Weitere Informationen erhalten Sie unter Ändern der Standardkonfiguration des Beschleunigungsalarms und Deaktivieren der Standardkonfiguration für den Beschleunigungsalarm.
  - Wenn Sie dieses Profil aktualisieren, setzt Alarm Manager Ihre Änderungen automatisch für alle relevanten Ressourcen in Ihrem Konto durch. AWS Beachten Sie, dass Ihre Änderungen zwar automatisch übernommen werden, es jedoch bis zu 60 Minuten dauern kann, bis sie wirksam werden.
  - Sie können dieses Profil mit den AWS-Managementkonsole oder CLI/SDK AWS-Tools aktualisieren. Anweisungen zum Aktualisieren einer Konfiguration finden Sie im AWS AppConfig Benutzerhandbuch.
  - Das Anpassungsprofil ist zunächst leer. Zusätzlich zur Standardkonfiguration werden jedoch alle im Profildokument enthaltenen Alarmdefinitionen durchgesetzt.

Alle vom Alarm Manager erstellten CloudWatch Alarme enthalten den Tag-Schlüssel ams:alarm-manager:managed und den Tag-Wert true. Dadurch wird sichergestellt, dass der Alarm Manager nur die Alarme verwaltet, die er erzeugt, und dass er Ihre eigenen Alarme nicht beeinträchtigt. Sie können diese Tags mithilfe der CloudWatch ListTagsForResourceAmazon-API sehen.

> **Important**
>
> Wenn benutzerdefinierte Alarmdefinitionen und Standardalarmdefinitionen mit derselben ConfigurationID angegeben werden (siheAccelerate Configuration-Profil: Überwachung), haben die benutzerdefinierten Definitionen Vorrang vor Standardregeln.

Erste Schritte mit Accelerate Alarm Manager

Wenn Sie AMS Accelerate nutzen, wird Ihre Konfiguration standardmäßig für bereitgestellt AWS AppConfig, wodurch eine Alarm-Basislinie für Ihre Ressourcen definiert wird. Die Alarmdefinitionen werden nur auf Ressourcen mit den Tags ams:rt: * angewendet. Wir empfehlen, diese Tags wie folgt

anzuwendenBeschleunigen Sie Resource Tagger: Sie richten eine grundlegende Resource Tagger-Konfiguration ein, damit AMS Accelerate weiß, welche Ressourcen Sie verwalten möchten.

Verwenden Sie Resource Tagger, um den Tag-Schlüssel ams:rt:ams-managed mit dem Tag-Wert true auf alle Ressourcen anzuwenden, die AMS Accelerate überwachen soll.

Im Folgenden finden Sie ein Beispiel für ein Resource Tagger-Anpassungsprofil, mit dem Sie sich für die Überwachung all Ihrer EC2 Amazon-Instances entscheiden können. Allgemeine Informationen finden Sie unter Beschleunigen Sie Resource Tagger.

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Informationen zur Anwendung dieser Resource Tagger-Konfiguration finden Sie unter. Die Resource Tagger-Konfiguration anzeigen oder Änderungen daran vornehmen

Beschleunigen Sie die Alarm Manager-Tags

Wenn Sie AMS Accelerate nutzen, wird Ihre Konfiguration standardmäßig für bereitgestellt AWS AppConfig, wodurch eine Alarm-Basislinie für Ihre Ressourcen definiert wird. Die Alarmdefinitionen werden nur auf Ressourcen mit den Tags ams:rt: * angewendet. Wir empfehlen, diese Tags wie folgt anzuwendenBeschleunigen Sie Resource Tagger: Sie richten eine grundlegende Resource Tagger-Konfiguration ein, damit AMS Accelerate weiß, welche Ressourcen Sie verwalten möchten.

Verwenden Sie Resource Tagger, um den Tag-Schlüssel ams:rt:ams-managed mit dem Tag-Wert true auf alle Ressourcen anzuwenden, die AMS Accelerate überwachen soll.

Themen

Beschleunigen Sie Tags mit Resource Tagger

Der tagbasierte Alarm Manager verwaltet den Lebenszyklus von CloudWatch Alarmen pro Ressource. Er setzt jedoch voraus, dass die verwalteten Ressourcen über spezifische, von AMS Accelerate definierte Tags verfügen. Gehen Sie wie folgt vor, um den Resource Tagger zu verwenden, um den Standardsatz von AMS-verwalteten Alarmen sowohl auf Linux- als auch auf Windows-basierte Instanzen anzuwenden.

1. Rufen Sie in Ihrem Konto die AppConfigKonsole auf.
2. Wählen Sie die ResourceTagger Anwendung aus.
3. Wählen Sie die Registerkarte Konfigurationsprofile und wählen Sie dann CustomerManagedTags.
4. Klicken Sie auf Erstellen, um ein neues Profil zu erstellen.
5. Wählen Sie JSON aus und definieren Sie Ihre Konfiguration. Weitere Beispiele für Filter- und Plattformdefinitionen finden Sie unterBeschleunigen Sie Resource Tagger.

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
           {
               "Key": "ams:rt:ams-managed",
               "Value": "true"
           }
       ]
   }
}
```

```
}
```

6. Klicken Sie auf Gehostete Konfigurationsversion erstellen.
7. Klicken Sie auf Bereitstellung starten.
8. Definieren Sie die folgenden Bereitstellungsdetails:

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
               Deployment Strategy: AMSNoBakeDeployment
```

9. Klicken Sie auf Bereitstellung starten.

Ihre Instanzen werden mit markiert`"ams:rt:ams-managed": "true"`, wodurch sichergestellt wird, dass zusätzliche `"ams:rt:ams-monitoring-policy": "ams-monitored"` und auf die Instanzen angewendet `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"` werden. Diese Tags führen dann dazu, dass die entsprechenden Alarme für die Instanz erstellt werden. Unter Überwachung in Accelerate finden Sie weitere Informationen zu diesem Verfahren.

Sehen Sie sich Himanshus Video an, um mehr zu erfahren (11:04)

Beschleunigen Sie Tags ohne Resource Tagger

Der tagbasierte Alarm Manager verwaltet den Lebenszyklus von CloudWatch Alarmen pro Ressource. Er setzt jedoch voraus, dass die verwalteten Ressourcen über spezifische, von AMS Accelerate definierte Tags verfügen. AMS Accelerate bietet ein Standardkonfigurationsprofil, das davon ausgeht, dass Ihre Tags von Resource Tagger angewendet wurden.

Wenn Sie eine alternative Methode zum Anwenden von Tags auf Ihre Ressourcen verwenden möchten, z. B. CloudFormation Terraform und nicht Resource Tagger, müssen Sie den Resource Tagger deaktivieren, damit er keine Tags auf Ihre Ressourcen anwendet und mit der von Ihnen gewählten Tagging-Methode konkurriert. Anweisungen zum Ändern Ihres benutzerdefinierten Resource Tagger-Konfigurationsprofils zur Aktivierung des schreibgeschützten Modus finden Sie unter. Verhindern, dass Resource Tagger Ressourcen verändert

Nachdem der Resource Tagger in den schreibgeschützten Modus versetzt und das Konfigurationsprofil bereitgestellt wurde, verwenden Sie die von Ihnen gewählte Tagging-Methode, um Tags auf Ihre Ressourcen anzuwenden. Beachten Sie dabei die folgenden Richtlinien:

Ressourcentyp	Tag-Schlüssel	Tag-Wert
Alle unterstützten Ressourcen (in dieser Tabelle beschrieben)	ams:rt: ams-monitoring-policy	ams-überwacht
EC2 Instanzen (Linux)	ams:rt: ams-monitoring-policy-platform	ams-monitored-linux
EC2 Instanzen (Windows)	ams:rt: ams-monitoring-policy-platform	ams-monitored-windows
OpenSearch Domäne mit KMS	ams:rt: ams-monitoring-with-kms	ams-monitored-with-kms
OpenSearch Domäne mit dediziertem Master-Knoten	ams:rt: ams-monitoring-with-master	ams-monitored-with-master

Ressourcen, die über diese Tag-Schlüssel und Werte verfügen, werden vom AMS Accelerate Alarm Manager verwaltet.

Beschleunigen Sie Tags mit CloudFormation

> **Note**
>
> Stellen Sie sicher, dass Sie Resource Tagger zuerst in den schreibgeschützten Modus versetzt haben, bevor Sie Tags verwenden. CloudFormation Andernfalls kann Resource Tagger die Tags auf der Grundlage des Konfigurationsprofils ändern. Informationen zur Einstellung von Resource Tagger in den schreibgeschützten Modus und Richtlinien zur Bereitstellung eigener Tags finden Sie unter. Beschleunigen Sie Tags ohne Resource Tagger

Um Tags anzuwenden CloudFormation, können Sie Tags auf Stack-Ebene (siehe CloudFormation Resource Tags) oder auf individueller Ressourcenebene (z. B. unter EC2 Instanz-Tags erstellen) anwenden.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie AMS Accelerate-Alarmmanagement-Tags auf eine EC2 Amazon-Instance anwenden können, die von verwaltet wird CloudFormation:

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Im Folgenden finden Sie ein Beispiel dafür, wie Sie AMS Accelerate-Alarmmanagement-Tags auf eine Auto Scaling Scaling-Gruppe anwenden können, die von verwaltet wird CloudFormation. Beachten Sie, dass die Auto Scaling Scaling-Gruppe ihre Tags an EC2 Amazon-Instances weitergibt, die von ihr erstellt wurden:

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Beschleunigen Sie Tags mit Terraform

> **Note**
>
> Stellen Sie sicher, dass Sie Resource Tagger zuerst in den schreibgeschützten Modus versetzt haben, bevor Sie Tags verwenden. CloudFormation Andernfalls kann Resource Tagger die Tags basierend auf dem Konfigurationsprofil ändern. Informationen zur Einstellung von Resource Tagger in den schreibgeschützten Modus und Richtlinien zur Bereitstellung eigener Tags finden Sie unter. Beschleunigen Sie Tags ohne Resource Tagger

Eine Beschreibung der Verwaltung von Ressourcen-Tags mit Terraform finden Sie in der Terraform-Dokumentation Resource Tagging.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie AMS Accelerate-Alarmmanagement-Tags auf eine von Terraform verwaltete EC2 Amazon-Instance anwenden können.

```
resource "aws_instance" "test_linux_instance" {
     # ...ami and other properties...

     instance_type = "t3.micro"

     tags = {
       "aws:rt:ams-monitoring-policy" = "ams-monitored"
       "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
     }
   }
```

Im Folgenden finden Sie ein Beispiel dafür, wie Sie AMS-Alarmmanagement-Tags auf eine von Terraform verwaltete Auto Scaling Scaling-Gruppe anwenden können. Beachten Sie, dass die Auto Scaling Scaling-Gruppe ihre Tags an EC2 Instances weitergibt, die von ihr erstellt wurden:

```
 resource "aws_autoscaling_group" "test_asg" {
 name = "terraform-test"
 # ...other properties...

 tags = {
   "aws:rt:ams-monitoring-policy" = "ams-monitored"
   "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
 }
}
```

Beschleunigen Sie die Alarm Manager-Konfigurationsprofile

Wenn Ihr Konto in AMS Accelerate integriert ist, werden zwei JSON-Dokumente, sogenannte Konfigurationsprofile, in Ihrem Konto mit bereitgestellt AWS AppConfig (siehe Was ist AWS AppConfig). Beide Profildokumente befinden sich in der Alarm Manager-Anwendung und in der AMS Accelerate-Infrastrukturumgebung.

Themen

Accelerate Configuration-Profil: Überwachung

Sowohl das Standardkonfigurationsprofildokument als auch das Dokument mit dem Anpassungskonfigurationsprofil haben dieselbe Struktur:

```
  {
    "<ResourceType>": {
        "<ConfigurationID>": {
            "Enabled": true,

            "Tag": {
                "Key": "...",
                "Value": "..."
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType: Bei diesem Schlüssel muss es sich um eine der folgenden unterstützten Zeichenketten handeln. Die Konfiguration in diesem JSON-Objekt bezieht sich nur auf den angegebenen AWS Ressourcentyp. Unterstützte Ressourcentypen

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::RDS::DBCluster
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationId: Dieser Schlüssel muss im Profil eindeutig sein und benennt den folgenden Konfigurationsblock eindeutig. Wenn zwei Konfigurationsblöcke im selben ResourceTypeBlock dieselbe ConfigurationID haben, wird der Block wirksam, der zuletzt im Profil erscheint. Wenn Sie in Ihrem Anpassungsprofil eine ConfigurationID angeben, die mit der im Standardprofil angegebenen identisch ist, wird der im Anpassungsprofil definierte Konfigurationsblock wirksam.
  - Aktiviert: (optional, default=true) Geben Sie an, ob der Konfigurationsblock wirksam werden soll. Setzen Sie dies auf false, um einen Konfigurationsblock zu deaktivieren. Ein deaktivierter Konfigurationsblock verhält sich so, als ob er nicht im Profil vorhanden wäre.
  - Tag: Geben Sie das Tag an, für das diese Alarmdefinition gilt. Für jede Ressource (des entsprechenden Ressourcentyps), die diesen Tag-Schlüssel und diesen Tag-Wert hat, wird ein CloudWatch Alarm mit der angegebenen Definition erstellt. Dieses Feld ist ein JSON-Objekt mit den folgenden Feldern:
    - Schlüssel: Der Schlüssel des Tags, der zugeordnet werden soll. Denken Sie daran, dass, wenn Sie Resource Tagger verwenden, um die Tags auf die Ressource anzuwenden, der Schlüssel für das Tag immer mit ams:rt: beginnt.
    - Wert: Der Wert des Tags, der zugeordnet werden soll.

- AlarmDefinition: Definiert den Alarm, der erstellt werden soll. Dies ist ein JSON-Objekt, dessen Felder unverändert an den CloudWatch `PutMetricAlarm` API-Aufruf übergeben werden (mit Ausnahme von Pseudoparametern; weitere Informationen finden Sie unter). Beschleunigtes Konfigurationsprofil: Substitution von Pseudoparametern Informationen darüber, welche Felder erforderlich sind, finden Sie in der Dokumentation. PutMetricAlarm

  ODER

  CompositeAlarmDefinition: Definiert einen zusammengesetzten Alarm, der erstellt werden soll. Wenn Sie einen zusammengesetzten Alarm erstellen, geben Sie einen Regelausdruck für den Alarm an, der den Alarmstatus anderer Alarme berücksichtigt, die Sie erstellt haben. Dies ist ein JSON-Objekt, dessen Felder unverändert an das `CloudWatchPutCompositeAlarm` übergeben werden. Der zusammengesetzte Alarm geht nur dann in den ALARM-Status über, wenn alle Bedingungen der Regel erfüllt sind. Die im Regelausdruck eines zusammengesetzten Alarms angegebenen Alarme können Metrikalarme und andere zusammengesetzte Alarme umfassen. Informationen darüber, welche Felder erforderlich sind, finden Sie in der PutCompositeAlarmDokumentation.

  Beide Optionen bieten die folgenden Felder:

  - AlarmName: Geben Sie den Namen des Alarms an, den Sie für die Ressource erstellen möchten. Dieses Feld hat dieselben Regeln wie in der PutMetricAlarmDokumentation angegeben. Da der Alarmname jedoch in einer Region eindeutig sein muss, hat der Alarm Manager eine zusätzliche Anforderung: Sie müssen den Pseudoparameter mit der eindeutigen Kennung im Namen des Alarms angeben (andernfalls fügt Alarm Manager den eindeutigen Bezeichner der Ressource an den Anfang des Alarmnamens an). Für den AWS::EC2::InstanceRessourcentyp müssen Sie beispielsweise `${EC2::InstanceId}` den Alarmnamen angeben, oder er wird implizit am Anfang des Alarmnamens hinzugefügt. Eine Liste der Identifikatoren finden Sie unter. Beschleunigtes Konfigurationsprofil: Substitution von Pseudoparametern

    Alle anderen Felder entsprechen den Angaben in der PutMetricAlarmoder der PutCompositeAlarmDokumentation.

  - AlarmRule: Geben Sie an, welche anderen Alarme ausgewertet werden sollen, um den Status dieses zusammengesetzten Alarms zu ermitteln. Für jeden Alarm, auf den Sie verweisen, müssen sie entweder in Ihrem Konto vorhanden sein CloudWatch oder im Alarm Manager-Konfigurationsprofil angegeben sein.

> **Important**
>
> Sie können entweder AlarmDefinitionoder CompositeAlarmDefinitionin Ihrem Alarm Manager-Konfigurationsdokument angeben, aber beide können nicht gleichzeitig verwendet werden.

Im folgenden Beispiel erzeugt das System einen Alarm, wenn zwei angegebene metrische Alarme ihren Schwellenwert überschreiten:

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

> **Important**
>
> Wenn Alarm Manager aufgrund einer fehlerhaften Konfiguration keinen Alarm erstellen oder löschen kann, sendet er die Benachrichtigung an das SNS-Thema Direct-Customer-Alerts. Dieser Alarm wird aufgerufen. AlarmDependencyError
> Wir empfehlen dringend, dass Sie Ihr Abonnement für dieses SNS-Thema bestätigt haben. Um Nachrichten zu erhalten, die zu einem Thema veröffentlicht wurden, müssen Sie einen Endpunkt für das Thema abonnieren. Einzelheiten finden Sie unter Schritt 1: Ein Thema erstellen.

> **Note**
>
> Wenn Alarme bei der Erkennung von Anomalien erstellt werden, erstellt Alarm Manager automatisch die erforderlichen Anomalieerkennungsmodelle für die angegebenen Messwerte. Wenn Alarme bei der Anomalieerkennung gelöscht werden, löscht Alarm Manager die zugehörigen Anomalieerkennungsmodelle nicht.
> Amazon CloudWatch begrenzt die Anzahl der Modelle zur Erkennung von Anomalien, die Sie in einer bestimmten AWS Region verwenden können. Wenn Sie das Modellkontingent überschreiten, erstellt Alarm Manager keine neuen Alarme zur Erkennung von Anomalien. Sie müssen entweder ungenutzte Modelle löschen oder mit Ihrem AMS-Partner zusammenarbeiten, um eine Erhöhung des Limits zu beantragen.
> Viele der von AMS Accelerate bereitgestellten Basisalarmdefinitionen führen das SNS-Thema MMS-Thema als Ziel auf. Dies dient zur Verwendung im AMS Accelerate-Überwachungsdienst und ist der Transportmechanismus, über den Ihre Alarmbenachrichtigungen an AMS Accelerate weitergeleitet werden. Geben Sie MMS-Topic nicht als Ziel für Alarme an, die nicht in der Baseline enthalten sind (und deren Überschreibungen), da der Service unbekannte Alarme ignoriert. Dies führt nicht dazu, dass AMS Accelerate auf Ihre benutzerdefinierten Alarme reagiert.

Beschleunigtes Konfigurationsprofil: Substitution von Pseudoparametern

In jedem der Konfigurationsprofile können Sie Pseudoparameter angeben, die an Ort und Stelle wie folgt ersetzt werden:

- Global — irgendwo im Profil:
  - $ {AWS::AccountId}: Ersetzt durch Ihre AWS Konto-ID
  - $ {AWS::Partition}: Ersetzt durch die Partition der Ressource, in AWS-Region der sich die Ressource befindet (dies ist 'aws' für die meisten Regionen); weitere Informationen finden Sie im Eintrag für die Partition in der ARN-Referenz.
  - $ {AWS::Region}: Ersetzt durch den Namen der Region, in der Ihre Ressource bereitgestellt wird (zum Beispiel us-east-1)
- In einem Block vom Typ AWS::EC2::InstanceRessource:
  - $ {EC2::InstanceId}: (Identifier) wurde durch die Instance-ID Ihrer EC2 Amazon-Instance ersetzt.
  - $ {EC2::InstanceName}: ersetzt durch den Namen Ihrer EC2 Amazon-Instance.
- In einem Block vom Ressourcentyp AWS::EC2::Instance: :Disk:

  - $ {EC2::InstanceId}: (Identifier) Ersetzt durch die Instance-ID Ihrer EC2 Amazon-Instance.
  - $ {EC2::InstanceName}: Ersetzt durch den Namen Ihrer EC2 Amazon-Instance.
  - $ {EC2: :Disk: :Device}: (Identifier) Ersetzt durch den Namen der Festplatte. (Nur Linux, auf vom CloudWatch Agenten verwalteten Instanzen).
  - $ {EC2: :Disk::FSType}: (identifier) Ersetzt durch den Dateisystemtyp der Festplatte. (Nur Linux, auf Instanzen, die von der verwaltet werden CloudWatchAgent).
  - $ {EC2: :Disk: :Path}: (Identifier) Ersetzt durch den Festplattenpfad. Unter Linux ist dies der Einhängepunkt der Festplatte (zum Beispiel/), während dies unter Windows die Laufwerksbezeichnung ist (z. B. c:/) (nur auf einer vom CloudWatch Agenten verwalteten Instanz).
  - $ {EC2: :Disk: :UUID}: (Identifier) Ersetzt durch eine generierte UUID, die die Festplatte eindeutig identifiziert. Diese muss im Namen des Alarms angegeben werden, da ein Alarm unter AWS::EC2::Instance::Disk Ressourcentyp einen Alarm pro Volume erzeugt. Durch die Angabe von $ {EC2: :Disk: :UUID} bleibt die Eindeutigkeit der Alarmnamen erhalten.
- In einem Block vom Typ Ressource: AWS::EKS::Cluster
  - $ {EKS::ClusterName}: (Identifier) wurde durch den Namen Ihres EKS-Clusters ersetzt.
- In einem AWS::OpenSearch::DomainRessourcentypblock:
  - $ {OpenSearch::DomainName}: (Identifier) wurde durch den Namen Ihrer EKS-Domain ersetzt.
- In einem Block vom Typ AWS::ElasticLoadBalancing::LoadBalancerRessource:
  - $ {ElasticLoadBalancing::LoadBalancer: :Name}: (Identifier) wurde durch den Namen Ihres V1 Load Balancer ersetzt.
- In einem AWS::ElasticLoadBalancingV2::LoadBalancerRessourcentypblock:
  - $ {ElasticLoadBalancingV2:LoadBalancer: :Arn}: (Identifier) wurde durch den ARN Ihres V2 Load Balancer ersetzt.
  - $ {ElasticLoadBalancingV2:LoadBalancer: :Name}: (Identifier) wurde durch den Namen Ihres V2 Load Balancer ersetzt.
  - $ {ElasticLoadBalancingV2:::LoadBalancer:FullName}: (Identifier) wurde durch den vollständigen Namen Ihres V2 Load Balancer ersetzt.
- In einem TargetGroup Ressourcentyp-Block AWS::ElasticLoadBalancingV2::LoadBalancer::
  - $ {ElasticLoadBalancingV2:::TargetGroup:FullName}: (Identifier) wird durch den Zielgruppennamen Ihres V2 Load Balancer ersetzt.
  - $ {ElasticLoadBalancingV2:: :UUID}TargetGroup: (Identifier) wurde durch eine generierte UUID für Ihren V2 Load Balancer ersetzt.

- In einem Block vom Typ Ressource: AWS::EC2::NatGateway
  - $ {NatGateway::NatGatewayId}: (Identifier) wurde durch die NAT-Gateway-ID ersetzt.
- In einem AWS: :RDS:: DBInstance Ressourcentypblock:
  - $ {RDS:: DBInstance Identifier}: (Identifier) wurde durch Ihre RDS-DB-Instance-ID ersetzt.
- In einem AWS: :RDS:: DBCluster Ressourcentypblock:
  - $ {RDS:: DBCluster Identifier}: (Identifier) wurde durch Ihre RDS-DB-Cluster-ID ersetzt.
- In einem Block vom Typ AWS::Redshift::ClusterRessource:
  - $ {Redshift::ClusterIdentifier}: (Identifier) wurde durch Ihre Redshift-Cluster-ID ersetzt.
- In einem Block vom Typ AWS::Synthetics::CanaryRessource:
  - $ {Synthetics::CanaryName}: (Identifier) wurde durch den Namen Ihres CloudWatch Synthetics Canary ersetzt.
- In einem AWS:::EC2: VPNConnection Ressourcentypblock:
  - $ {AWS::EC2::VpnConnectionId}: (Identifier) wurde durch Ihre VPN-ID ersetzt.
- In einem Block vom Typ AWS::EFS::FileSystemRessource:
  - $ {EFS::FileSystemId}: (Identifier) Ersetzt durch die Dateisystem-ID Ihres EFS-Dateisystems.
- In einem AWS::FSx::FileSystem: :ONTAP-Ressourcentypblock:
  - $ {FSx::FileSystemId}: (Identifier) Ersetzt durch die Dateisystem-ID Ihres FSX-Dateisystems.
  - $ {FSx::FileSystem: :Throughput}: Ersetzt durch den Durchsatz Ihres FSX-Dateisystems.
  - $ {FSx::FileSystem: :Iops}: Ersetzt durch die IOPS des FSX-Dateisystems.
- In einem AWS::FSx::FileSystem: :ONTAP: :Volume-Ressourcentypblock:
  - $ {FSx::FileSystemId}: (Identifier) Ersetzt durch die Dateisystem-ID Ihres FSX-Dateisystems.
  - $ {FSx: :ONTAP::VolumeId}: (identifier) Ersetzt durch die Volume-ID.
- In einem AWS::FSx::FileSystem: :Windows-Ressourcentypblock:
  - $ {FSx::FileSystemId}: (Identifier) Ersetzt durch die Dateisystem-ID Ihres FSX-Dateisystems.
  - $ {FSx::FileSystem: :Throughput}: Ersetzt durch den Durchsatz Ihres FSX-Dateisystems.

> **Note**
>
> Alle mit Identifier markierten Parameter werden als Präfix für den Namen der erstellten Alarme verwendet, sofern Sie diese Kennung nicht im Alarmnamen angeben.

Beispiele für die Konfiguration von Beschleunigungsalarmen

Im folgenden Beispiel erzeugt das System einen Alarm für jede Festplatte, die an die entsprechende Linux-Instanz angeschlossen ist.

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    },
                    {
                        "Name": "path",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Im folgenden Beispiel erzeugt das System einen Alarm für jede Festplatte, die an die entsprechende Windows-Instanz angeschlossen ist.

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Ihre Accelerate Alarm Manager-Konfiguration anzeigen

Sowohl die AMSManagedAlarme als auch CustomerManagedAlarmskönnen AppConfig mit überprüft werden GetConfiguration.

Das Folgende ist ein Beispiel für den `GetConfiguration` Anruf:

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- Anwendung: Dies AppConfig ist die logische Einheit zur Bereitstellung von Funktionen; für den Alarm Manager ist dies `AMSAlarmManager`
- Umgebung: Das ist die AMSInfrastructure Umgebung
- Konfiguration: Für die Anzeige von AMS Accelerate-Basisalarmen lautet der Wert`AMSManagedAlarms`; für die Anzeige von Kundenalarmdefinitionen ist die Konfiguration `CustomerManagedAlarms`
- Client-ID: Dies ist eine eindeutige Anwendungsinstanz-ID, bei der es sich um eine beliebige Zeichenfolge handeln kann
- Die Alarmdefinitionen können in der angegebenen Ausgabedatei eingesehen werden, in diesem Fall `outfile.json`

Sie können anhand der vergangenen Bereitstellungen in der AMSInfrastructure Umgebung sehen, welche Version der Konfiguration für Ihr Konto bereitgestellt wurde.

Konfiguration des Accelerate-Alarms ändern

Um neue Alarmdefinitionen hinzuzufügen oder zu aktualisieren, können Sie entweder ein Konfigurationsdokument Verwenden CloudFormation zur Bereitstellung von Accelerate-Konfigurationsänderungen bereitstellen oder die CreateHostedConfigurationVersionAPI aufrufen.

Dies ist ein Linux-Befehlszeilenbefehl, der den Parameterwert in Base64 generiert, was der AppConfig CLI-Befehl erwartet. Weitere Informationen finden Sie in der AWS CLI Dokumentation Binary/Blob (Binary Large Object).

Beispiel:

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- Anwendungs-ID: ID der Anwendung AMS AlarmManager; Sie können dies mit dem API-Aufruf herausfinden. ListApplications
- Konfigurationsprofil-ID: ID der Konfiguration CustomerManagedAlarms; Sie können dies mit dem ListConfigurationProfilesAPI-Aufruf herausfinden.
- Inhalt: Base64-Zeichenfolge des Inhalts, der erstellt werden soll, indem ein Dokument erstellt und in Base64 kodiert wird: cat alarms-v2.json | base64 (siehe Binary/Blob (Binary Large Object)).

Inhaltstyp: MIME-Typ, da Alarmdefinitionen in JSON geschrieben werden. `application/json`

> **Important**
>
> Beschränken Sie den Zugriff auf die StartDeployment und StopDeployment API-Aktionen auf vertrauenswürdige Benutzer, die sich mit den Verantwortlichkeiten und Konsequenzen der Implementierung einer neuen Konfiguration für Ihre Ziele auskennen.

Weitere Informationen zur Verwendung von AppConfig AWS-Funktionen zum Erstellen und Bereitstellen einer Konfiguration finden Sie unter Arbeiten mit AWS AppConfig.

Ändern der Standardkonfiguration des Beschleunigungsalarms

Sie können das Standardkonfigurationsprofil zwar nicht ändern, aber Sie können die Standardeinstellungen überschreiben, indem Sie in Ihrem Anpassungsprofil einen Konfigurationsblock mit derselben ConfigurationID wie der Standardkonfigurationsblock angeben. Wenn Sie dies tun, überschreibt Ihr gesamter Konfigurationsblock den Standardkonfigurationsblock, für den die Tagging-Konfiguration angewendet werden soll.

Betrachten Sie zum Beispiel das folgende Standardkonfigurationsprofil:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
```

```
                "Threshold": 5,
                ...
            }
        }
    }
}
```

Um den Schwellenwert für diesen Alarm auf 10 zu ändern, müssen Sie die gesamte Alarmdefinition angeben, nicht nur die Teile, die Sie ändern möchten. Sie könnten beispielsweise das folgende Anpassungsprofil angeben:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
            }
        }
    }
}
```

> **Important**
>
> Denken Sie daran, Ihre Konfigurationsänderungen zu implementieren, nachdem Sie sie vorgenommen haben. In SSM AppConfig müssen Sie nach der Erstellung eine neue Version der Konfiguration bereitstellen.

Implementieren von Accelerate-Alarm-Konfigurationsänderungen

Nachdem Sie eine Anpassung abgeschlossen haben, müssen Sie sie entweder mit AppConfig oder bereitstellen CloudFormation.

Themen

Wird AppConfig zur Bereitstellung von Accelerate-Alarm-Konfigurationsänderungen verwendet

Sobald die Anpassung abgeschlossen ist, verwenden Sie, AppConfig um Ihre Änderungen mit zu implementieren StartDeployment.

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- Anwendungs-ID: ID der Anwendung`AMSAlarmManager`. Sie finden diese mithilfe des ListApplicationsAPI-Aufrufs.
- Umgebungs-ID: Sie finden diese mit dem ListEnvironmentsAPI-Aufruf.
- ID der Bereitstellungsstrategie: Sie finden diese mit dem ListDeploymentStrategiesAPI-Aufruf.
- Konfigurationsprofil-ID: ID von`CustomerManagedAlarms`; Sie finden diese ID mit dem ListConfigurationProfilesAPI-Aufruf.
- Konfigurationsversion: Die Version des Konfigurationsprofils, das bereitgestellt werden soll.

> **Important**
>
> Alarm Manager wendet die in den Konfigurationsprofilen angegebenen Alarmdefinitionen an. Alle manuellen Änderungen, die Sie mit dem AWS-Managementkonsole oder dem CloudWatch CLI/SDK an den CloudWatch Alarmen vornehmen, werden automatisch rückgängig gemacht. Stellen Sie daher sicher, dass Ihre Änderungen über den Alarm Manager definiert sind. Um zu verstehen, welche Alarme vom Alarm Manager erstellt werden, können Sie nach `ams:alarm-manager:managed` dem Tag mit dem Wert suchen. `true`

Beschränken Sie den Zugriff auf die StartDeploymentund StopDeploymentAPI-Aktionen auf vertrauenswürdige Benutzer, die sich mit den Verantwortlichkeiten und Konsequenzen der Implementierung einer neuen Konfiguration für Ihre Ziele auskennen.

Weitere Informationen zur Verwendung von AppConfig AWS-Funktionen zum Erstellen und Bereitstellen einer Konfiguration finden Sie in der AppConfig AWS-Dokumentation.

Verwenden CloudFormation zur Bereitstellung von Accelerate-Konfigurationsänderungen

Wenn Sie Ihr `CustomerManagedAlarms` Konfigurationsprofil mithilfe von bereitstellen möchten CloudFormation, können Sie die folgenden CloudFormation Vorlagen verwenden. Geben Sie Ihre gewünschte JSON-Konfiguration in das `AMSAlarmManagerConfigurationVersion.Content` Feld ein.

Wenn Sie die Vorlagen in einem CloudFormation Stack oder Stack-Set bereitstellen, schlägt die Bereitstellung der `AMSResourceTaggerDeployment` Ressource fehl, wenn Sie das erforderliche JSON-Format für die Konfiguration nicht eingehalten haben. Einzelheiten Accelerate Configuration-Profil: Überwachung zum erwarteten Format finden Sie unter.

Hilfe zur Bereitstellung dieser Vorlagen als CloudFormation Stack oder Stack-Set finden Sie in der entsprechenden CloudFormation AWS-Dokumentation unten:

- Einen Stack auf der CloudFormation AWS-Konsole erstellen
- Einen Stack mit AWS CLI erstellen
- Ein Stack-Set erstellen

Note

Wenn Sie eine Konfigurationsversion mithilfe einer dieser Vorlagen bereitstellen und anschließend den CloudFormation Stack/das Stack-Set löschen, bleibt die Version der Vorlagenkonfiguration die aktuell bereitgestellte Version, und es erfolgt keine weitere Bereitstellung. Wenn Sie zu einer Standardkonfiguration zurückkehren möchten, müssen Sie entweder manuell eine leere Konfiguration bereitstellen (d. h. nur {}) oder Ihren Stack auf eine leere Konfiguration aktualisieren, anstatt den Stack zu löschen.

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

Rollback: Alarmänderungen beschleunigen

Sie können Alarmdefinitionen über denselben Bereitstellungsmechanismus rückgängig machen, indem Sie eine frühere Version des Konfigurationsprofils angeben und den Vorgang ausführen StartDeployment.

Aufbewahrung von Accelerate-Alarmen

Wenn von AMS überwachte Ressourcen gelöscht werden, werden alle von Alarm Manager für diese Ressourcen erstellten Alarme automatisch von Alarm Manager gelöscht. Wenn Sie bestimmte Alarme aus Prüfungs-, Konformitäts- oder historischen Gründen aufbewahren müssen, verwenden Sie die Funktion zur Aufbewahrung von Kennzeichnungen in Alarm Manager.

Um einen Alarm auch nach dem Löschen der überwachten Ressource beizubehalten, fügen Sie der benutzerdefinierten Konfiguration des Alarms ein `"ams:alarm-manager:retain"` Tag hinzu, wie im folgenden Beispiel gezeigt.

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

Ein mit dem `"ams:alarm-manager:retain"` Tag konfigurierter Alarm wird nicht automatisch von Alarm Manager gelöscht, wenn die überwachte Ressource beendet wird. Der gespeicherte Alarm bleibt CloudWatch auf unbestimmte Zeit bestehen, bis Sie ihn manuell mithilfe von entfernen. CloudWatch

Deaktivieren der Standardkonfiguration für den Beschleunigungsalarm

AMS Accelerate stellt das Standardkonfigurationsprofil für Ihr Konto bereit, das auf den Basisalarmen basiert. Diese Standardkonfiguration kann jedoch deaktiviert werden, indem eine der Alarmdefinitionen überschrieben wird. Sie können eine Standardkonfigurationsregel deaktivieren, indem Sie die ConfigurationID der Regel in Ihrem Anpassungskonfigurationsprofil überschreiben und das aktivierte Feld mit dem Wert false angeben.

Zum Beispiel, wenn die folgende Konfiguration im Standardkonfigurationsprofil vorhanden war:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

Sie könnten diese Tagging-Regel deaktivieren, indem Sie Folgendes in Ihr Anpassungskonfigurationsprofil aufnehmen:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

Um diese Änderungen vorzunehmen, muss die CreateHostedConfigurationVersionAPI mit dem JSON-Profildokument aufgerufen werden (siheKonfiguration des Accelerate-Alarms ändern) und anschließend bereitgestellt werden (sieheImplementieren von Accelerate-Alarm-Konfigurationsänderungen). Beachten Sie, dass Sie beim Erstellen der neuen Konfigurationsversion auch alle zuvor erstellten benutzerdefinierten Alarme, die Sie möchten, in das JSON-Profildokument aufnehmen müssen.

> **Important**
>
> Wenn AMS Accelerate das Standardkonfigurationsprofil aktualisiert, wird es nicht anhand Ihrer konfigurierten benutzerdefinierten Alarme kalibriert. Überprüfen Sie daher die Änderungen an den Standardalarmen, wenn Sie sie in Ihrem Anpassungskonfigurationsprofil überschreiben.

Zusätzliche CloudWatch Alarme für Accelerate erstellen

Sie können zusätzliche CloudWatch Alarme für AMS Accelerate erstellen, indem Sie benutzerdefinierte CloudWatch Metriken und Alarme für EC2 Amazon-Instances verwenden.

Erstellen Sie Ihr Anwendungsüberwachungsskript und Ihre benutzerdefinierte Metrik. Weitere Informationen und Zugriff auf Beispielskripts finden Sie unter Monitoring Memory and Disk Metrics for Amazon EC2 Linux Instances.

Die CloudWatch Überwachungsskripte für EC2 Linux-Amazon-Instances zeigen, wie benutzerdefinierte CloudWatch Metriken erstellt und verwendet werden. Diese Perl-Beispielskripts umfassen ein voll funktionsfähiges Beispiel, bei dem Speicher-, Auslagerungs- und Speicherplatz-Auslastungsmetriken für eine Linux-Instance gemeldet werden.

> **Important**
>
> AMS Accelerate überwacht keine von Ihnen erstellten CloudWatch Alarme.

Anzahl der von Alarm Manager for Accelerate überwachten Ressourcen anzeigen

Alarm Manager sendet jede Stunde Metriken im `AMS/AlarmManager` Namespace an Amazon CloudWatch. Metriken werden nur für Ressourcentypen ausgegeben, die von Alarm Manager unterstützt werden.

Metrikname	Dimensionen	Beschreibung
ResourceCount	Komponente, ResourceType	Anzahl der Ressourcen (des angegebenen Ressourcentyps), die in dieser Region eingesetzt werden. Einheiten: Anzahl
ResourcesMissingManagedAlarms	Komponente, ResourceType	Anzahl der Ressourcen (des angegebenen Ressourcentyps), für die verwaltete Alarme erforderlich sind, aber Alarm Manager hat die Alarme noch nicht angewendet. Einheiten: Anzahl

Metrikname	Dimensionen	Beschreibung
Unmanaged Resources	Komponente, ResourceType	Anzahl der Ressourcen (des angegebenen Ressourcentyps), auf die von Alarm Manager keine verwalteten Alarme angewendet wurden. In der Regel entsprachen diese Ressourcen keinem Alarm Manager-Konfigurationsblock oder sind ausdrücklich von Konfigurationsblöcken ausgeschlossen. Einheiten: Anzahl
MatchingResourceCount	Komponente ResourceType, ConfigClauseName	Anzahl der Ressourcen (des angegebenen Ressourcentyps), die dem Alarm Manager-Konfigurationsblock entsprechen. Damit eine Ressource dem Konfigurationsblock entspricht, muss der Block aktiviert sein und die Ressource muss dieselben Tags haben, die im Konfigurationsblock angegeben sind. Einheiten: Anzahl

Diese Messwerte können auch als Grafiken im AMS-Alarm-Manager-Reporting-Dashboard angezeigt werden. Um das Dashboard zu sehen, wählen Sie in der Managementkonsole AMS-Alarm-Manager-Reporting-Dashboard aus. AWS CloudWatch In den Diagrammen in diesem Dashboard werden standardmäßig die Daten für die letzten 12 Stunden angezeigt.

AMS Accelerate sendet CloudWatch Alarme an Ihr Konto, um einen deutlichen Anstieg der Anzahl nicht verwalteter Ressourcen zu erkennen, z. B. Ressourcen, die von AMS Alarm Manager von der Verwaltung ausgeschlossen wurden. AMS Operations untersucht die Zunahme nicht verwalteter Ressourcen, die Folgendes überschreiten: entweder drei Ressourcen desselben Typs oder einen Anstieg von 50% gegenüber allen Ressourcen desselben Typs. Wenn die Änderung nicht beabsichtigt zu sein scheint, kann AMS Operations Sie kontaktieren, um die Änderung zu überprüfen.

Automatische AMS-Behebung von Warnmeldungen

Nach der Überprüfung behebt AWS Managed Services (AMS) automatisch bestimmte Warnmeldungen gemäß den in diesem Abschnitt beschriebenen Bedingungen und Prozessen.

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
Statusprüfung fehlgeschlagen	Mögliche Hardwarefehler oder ein Fehlerstatus der Instanz.	Das System hat in den letzten 15 Minuten mindestens einmal einen ausgefallenen Status erkannt.	Die automatische AMS-Problembehebung überprüft zunächst, ob auf die Instanz zugegriffen werden kann. Wenn auf die Instanz nicht zugegriffen werden kann, wird die Instanz gestoppt und neu gestartet. Das Stop-and-Start-Verfahren ermöglicht es der Instanz, auf neue zugrunde liegende Hardware zu migrieren. Weitere Informationen finden Sie im folgenden Abschnitt „Automatisierung der EC2 Fehlerkorrektur bei der Statusprüfung“.
AMSLinuxDiskUsage	Wird ausgelöst, wenn die Festplattenbelegung eines Bereitstellungspunkts (zugewiesener Speicherplatz auf einem Volume) auf Ihrer EC2 Instance voll ausgelastet ist.	Der Schwellenwert lag in den letzten 30 Minuten sechsmal über dem definierten Wert.	Die automatische AMS-Wiederherstellung löscht zunächst temporäre Dateien. Wenn dadurch nicht genügend Festplattenspeicher frei wird, wird das Volume erweitert, um Ausfallzeiten zu vermeiden, wenn das Volume voll wird.
AMSWindowsDiskUsage	Wenn die Festplattenbelegung eines Bereitstellungspunkts	Der Schwellenwert lag in den letzten 30 Minuten	Die automatische AMS-Wiederherstellung löscht zunächst temporäre

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
	(zugewiesener Speicherplatz auf einem Volume) auf Ihrer EC2 Instance aufgebraucht ist.	sechsmal über dem definierten Wert.	Dateien. Wenn dadurch nicht genügend Festplattenspeicher frei wird, wird das Volume erweitert, um Ausfallzeiten zu vermeiden, wenn das Volume voll wird.

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-EVENT-0089	Die DB-Instance hat mehr als 90% ihres zugewiesenen Speichers verbraucht.	Der Speicher ist zu mehr als 90% zugewiesen.	Die automatische AMS-Problembehebung überprüft zunächst, ob sich die Datenbank in einem modifizierbaren und verfügbaren Zustand befindet oder ob der Speicher voll ist. Anschließend wird versucht, den zugewiesenen Speicher, die IOPS und den Speicherdurchsatz mithilfe eines Changesets zu erhöhen. CloudFormation Wenn eine Stack-Drift bereits erkannt wird, wird sie auf die RDS-API zurückgegriffen, um Ausfallzeiten zu vermeiden. Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-EVENT-0007	Der der DB-Instance zugewiesene Speicherplatz ist erschöpft. Um das Problem zu lösen, weisen Sie zusätzlichen Speicher zu.	Der Speicherplatz ist zu 100% zugewiesen.	Die automatische AMS-Problembehebung überprüft zunächst, ob sich die Datenbank in einem modifizierbaren und verfügbaren Zustand befindet oder ob der Speicherplatz voll ist. Anschließend wird versucht, den zugewiesenen Speicher, die IOPS und den Speicherdurchsatz mithilfe eines Changesets zu erhöhen. CloudFormation Wenn eine Stack-Drift bereits erkannt wird, wird sie auf die RDS-API zurückgegriffen, um Ausfallzeiten zu vermeiden. Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-EVENT-0224	Der angeforderte zugewiesene Speicher erreicht oder überschreitet den konfigurierten maximalen Speichers chwellenwert.	Der maximale Speichers chwellenwert für die DB-Instance wurde ausgeschöpft oder ist größer oder gleich dem angeforderten zugewiesenen Speicher.	Die automatische AMS-Problembehebung überprüft zunächst, ob die angeforderte Menge an RDS-Speicher den maximalen Speicherschwellenwert überschreitet. Falls bestätigt, versucht AMS, den maximalen Speicherschwellenwert mit einem CloudFormation Changeset oder einer direkten RDS-API, falls Ressourcen nicht bereitgestellt werden, um 30% zu erhöhen. CloudFormation Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Name der Warnung	Beschreibung	Schwellenwerte	Aktion
RDS-Speicherkapazität	Im zugewiesenen Speicher für die DB-Instance verbleiben weniger als 1 GB.	Der Speicherplatz ist zu 99% zugewiesen.	Die automatische AMS-Problembehebung überprüft zunächst, ob sich die Datenbank in einem modifizierbaren und verfügbaren Zustand befindet oder ob der Speicherplatz voll ist. Anschließend wird versucht, den zugewiesenen Speicher, die IOPS und den Speicherdurchsatz mithilfe eines Changesets zu erhöhen. CloudFormation Wenn eine Stack-Drift bereits erkannt wird, wird sie auf die RDS-API zurückgegriffen, um Ausfallzeiten zu vermeiden. Diese Funktion kann deaktiviert werden, indem der RDS-DB-Instance das folgende Tag hinzugefügt wird: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

EC2 Fehler bei der Statusüberprüfung: Hinweise zur Automatisierung der Problembehebung

So funktioniert die automatische AMS-Problembehebung bei EC2 fehlgeschlagenen Statusprüfungen:

- Wenn Ihre EC2 Amazon-Instance nicht mehr erreichbar ist, muss die Instance gestoppt und erneut gestartet werden, damit sie auf neue Hardware migriert und wiederhergestellt werden kann.
- Wenn die Ursache des Problems im Betriebssystem liegt (fehlende Geräte in fstab, Kernelfehler usw.), kann die Automatisierung Ihre Instance nicht wiederherstellen.
- Wenn Ihre Instance zu einer Auto Scaling Scaling-Gruppe gehört, ergreift die Automatisierung keine Aktion — die AutoScalingGroup Skalierungsaktion ersetzt die Instance.
- Wenn für Ihre Instance EC2 Auto Recovery aktiviert ist, werden bei der Behebung keine Maßnahmen ergriffen.

EC2 Automatisierung der Behebung der Volumennutzung

So funktioniert die automatische Behebung von Problemen mit der EC2 Volumennutzung durch AWS Managed Services (AMS):

- Die Automatisierung überprüft zunächst, ob die Volumenerweiterung erforderlich ist und ob sie durchgeführt werden kann. Wenn die Erweiterung als angemessen erachtet wird, kann die Automatisierung die Volumenkapazität erhöhen. Dieser automatisierte Prozess bringt den Bedarf an Wachstum mit kontrollierter, begrenzter Expansion in Einklang.
- Vor der Erweiterung eines Volumes führt die Automatisierung Säuberungsaufgaben (Windows: Disk Cleaner, Linux: Logrotate + Simple Service Manager Agent Log entfernen) auf der Instanz aus, um Speicherplatz freizugeben.

> **Note**
>
> Die Bereinigungsaufgaben werden nicht auf Instanzen der EC2 „T“ -Familie ausgeführt, da sie für die kontinuierliche Funktionalität auf CPU-Guthaben angewiesen sind.

- Unter Linux unterstützt die Automatisierung nur die Erweiterung der Dateisysteme vom Typ EXT2 EXT3, EXT4 und XFS.
- Unter Windows unterstützt die Automatisierung nur das New Technology File System (NTFS) und das Resilient File System (ReFS).

- Die Automatisierung erweitert keine Volumes, die Teil von Logical Volume Manager (LVM) oder eines RAID-Arrays sind.
- Durch die Automatisierung werden die Instance-Speicher-Volumes nicht erweitert.
- Die Automatisierung ergreift keine Maßnahmen, wenn das betroffene Volumen bereits größer als 2 TiB ist.
- Die Erweiterung durch Automatisierung ist auf maximal dreimal pro Woche und insgesamt auf das Fünffache während der gesamten Lebensdauer des Systems begrenzt.
- Durch die Automatisierung wird das Volumen nicht erhöht, wenn die vorherige Erweiterung innerhalb der letzten sechs Stunden stattgefunden hat.

Wenn diese Regeln verhindern, dass die Automatisierung Maßnahmen ergreift, kontaktiert AMS Sie über eine ausgehende Serviceanfrage, um die nächsten zu ergreifenden Maßnahmen festzulegen.

Automatisierung der Behebung von Ereignissen bei geringem Speicherplatz in Amazon RDS

So funktioniert die automatische Behebung von AWS Managed Services (AMS) bei Problemen mit unzureichendem Speicherplatz in Amazon RDS:

- Bevor versucht wird, den Amazon RDS-Instance-Speicher zu erweitern, führt die Automatisierung mehrere Prüfungen durch, um sicherzustellen, dass sich die Amazon RDS-Instance in einem modifizierbaren und verfügbaren oder speichervollen Zustand befindet.
- Wenn CloudFormation Stack-Drift erkannt wird, erfolgt die Behebung über die Amazon RDS-API.
- Die Behebungsaktion wird in den folgenden Szenarien nicht ausgeführt:
  - Der Amazon RDS-Instance-Status ist nicht „verfügbar“ oder „Speicher voll“.
  - Der Amazon RDS-Instance-Speicher kann derzeit nicht geändert werden (z. B. wenn der Speicher in den letzten sechs Stunden geändert wurde).
  - Für die Amazon RDS-Instance ist die automatische Speicherskalierung aktiviert.
  - Die Amazon RDS-Instance ist keine Ressource innerhalb eines CloudFormation Stacks.
- Die Behebung ist auf eine Erweiterung alle sechs Stunden und nicht mehr als drei Erweiterungen innerhalb eines fortlaufenden Zeitraums von vierzehn Tagen begrenzt.
- Wenn diese Szenarien eintreten, meldet sich AMS mit einem ausgehenden Vorfall an Sie, um die nächsten Maßnahmen festzulegen.

Verwenden von Amazon EventBridge Managed Rules in AMS

AMS Accelerate verwendet Amazon EventBridge Managed Rules. Eine verwaltete Regel ist ein einzigartiger Regeltyp, der direkt mit AMS verknüpft ist. Diese Regeln ordnen eingehende Ereignisse zu und senden sie zur Verarbeitung an Ziele. Verwaltete Regeln sind von AMS vordefiniert und enthalten Ereignismuster, die vom Service für die Verwaltung von Kundenkonten benötigt werden. Sofern nicht anders definiert, kann nur der Service, für den sie verantwortlich ist, diese verwalteten Regeln verwenden.

Die verwalteten AMS Accelerate-Regeln sind mit dem `events.managedservices.amazonaws.com` Service Principal verknüpft. Diese verwalteten Regeln werden über die AWSServiceRoleForManagedServices_Eventsdienstbezogene Rolle verwaltet. Um diese Regeln zu löschen, ist eine besondere Bestätigung durch den Kunden erforderlich. Weitere Informationen finden Sie unter Löschen verwalteter Regeln für AMS.

Weitere Informationen zu Regeln finden Sie unter Regeln im EventBridge Amazon-Benutzerhandbuch.

Von AMS bereitgestellte Amazon EventBridge Managed Rules

Von Amazon EventBridge verwaltete Regeln

Regelname	Beschreibung	Definition

AmsAccessRolesRule	Diese Regel berücksichtigt Änderungen in bestimmten AMS Accelerate-Rollen und -Richtlinien.	<pre>{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",</pre>

Regelname	Beschreibung	Definition

```
                    "ams-access-admin-operations",
                    "ams-access-operations",
                    "ams-access-read-only",
                    "ams-access-security-analyst",
                    "ams-access-security-analyst-
read-only"
                ]
            },
            {
                "policyArn": [
                    "arn:*:iam::*:policy/ams-ac
cess-allow-pass-role",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-cloudshell-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-operations-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
        ]
    },
},
}
```

Regelname	Beschreibung	Definition

AMSCoreRegel	Diese Regel leitet alle CloudWatch Amazon-Ereignisse AWS Config respektvoll an die AMS Config-Problembehebungs- und AMS-Überwachungsdienste weiter. Die AWS Config Ereignisse erzeugen und lösen sich auf. AWS Systems Manager OpsItems Die CloudWatch Amazon-Ereignisse überwachen CloudWatch Alarme.	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],
		    }
		}</pre>

Verwaltete Regeln für AMS erstellen

Sie müssen Amazon EventBridge Managed Rules nicht manuell erstellen. Wenn Sie in der AWS Management Console, der oder der AWS CLI AWS API bei AMS einsteigen, erstellt AMS sie für Sie.

Verwaltete Regeln für AMS bearbeiten

AMS erlaubt Ihnen nicht, die verwalteten Regeln zu bearbeiten. Name und Ereignismuster für jede verwaltete Regel sind von AMS vordefiniert.

Verwaltete Regeln für AMS löschen

Sie müssen die verwalteten Regeln nicht manuell löschen. Wenn Sie in der AWS Management Console, der oder der AWS API aus AMS aussteigen AWS CLI, bereinigt AMS die Ressourcen und löscht alle verwalteten Regeln, die AMS gehören, für Sie.

Falls AMS die verwalteten Regeln beim Offboarding nicht entfernt, können Sie die verwalteten Regeln auch über die EventBridge Amazon-Konsole, die AWS CLI oder die AWS API manuell löschen. Dazu müssen Sie zunächst Ihr Konto bei AMS verlassen und das Löschen der verwalteten Regeln erzwingen.

Vertrauenswürdiger Remediator in AMS

Trusted Remediator ist eine AWS Managed Services Services-Lösung, die die Problembehebung und Empfehlungen automatisiert. AWS Trusted AdvisorAWS Compute Optimizer Trusted Remediator erstellt Empfehlungen, wann Trusted Advisor und Compute Optimizer zeigt Ihnen Möglichkeiten auf, Kosten zu senken, die Systemverfügbarkeit zu verbessern, die Leistung zu optimieren oder Sicherheitslücken für Sie zu schließen. AWS-Konten Mit Trusted Remediator können Sie diese Empfehlungen zu Sicherheit, Leistung, Kostenoptimierung, Fehlertoleranz und Servicebeschränkungen auf sichere, standardisierte Weise umsetzen und dabei etablierte Best Practices verwenden. Trusted Remediator ermöglicht Ihnen die Konfiguration einer Behebungslösung und wird automatisch nach einem von Ihnen erstellten Zeitplan ausgeführt, wodurch der Behebungsprozess vereinfacht wird. Mit diesem optimierten Ansatz werden Probleme konsistent, effizient und ohne manuelles Eingreifen behoben.

Die wichtigsten Vorteile von Trusted Remediator

Im Folgenden sind die wichtigsten Vorteile von Trusted Remediator aufgeführt:

- Verbesserte Sicherheit, Leistung und Kostenoptimierung: Trusted Remediator hilft Ihnen dabei, die allgemeine Sicherheitslage Ihrer Konten zu verbessern, die Ressourcennutzung zu optimieren und die Betriebskosten zu senken.

- Self-Service-Einrichtung und Konfiguration: Sie können Trusted Remediator so konfigurieren, dass es Ihren Anforderungen und Präferenzen entspricht.
- Automatisierte Behebung von Trusted Advisor Prüfungen und AWS Compute Optimizer Empfehlungen: Nach der Konfiguration führt Trusted Remediator automatisch die Behebungsmaßnahmen für ausgewählte Prüfungen aus. Durch diese Automatisierung entfällt die Notwendigkeit manueller Eingriffe.
- Implementierung bewährter Verfahren: Abhilfemaßnahmen basieren auf etablierten bewährten Verfahren, sodass Probleme auf standardisierte und effektive Weise angegangen werden.
- Geplante Ausführung: Sie können den Zeitplan für die Behebung wählen, der Ihren day-to-day betrieblichen Arbeitsabläufen entspricht.

Trusted Remediator ermöglicht es Ihnen, identifizierte Probleme in Ihren AWS Umgebungen proaktiv anzugehen und hilft Ihnen dabei, bewährte Verfahren einzuhalten und eine sichere, leistungsstarke und kostengünstige Cloud-Infrastruktur aufrechtzuerhalten.

So funktioniert Trusted Remediator

Im Folgenden wird der Trusted Remediator-Arbeitsablauf veranschaulicht:

Trusted Remediator bewertet Trusted Advisor und empfiehlt Compute Optimizer für Sie AWS-Konten und erstellt diese. AWS Systems Manager OpsItems OpsCenter Anschließend können Sie Trusted Remediator-Automatisierungsdokumente verwenden, um das Problem automatisch oder manuell zu beheben. OpsItems Im Folgenden finden Sie Einzelheiten zu den einzelnen Behebungstypen:

- Automatisierte Behebung: Trusted Remediator führt das Automatisierungsdokument aus und überwacht den Lauf. Nach Abschluss des Automatisierungsdokuments löst Trusted Remediator das Opsitem auf.
- Manuelle Korrektur: Trusted Remediator erstellt das, damit Sie es überprüfen können. OpsItem Nach der Überprüfung starten Sie das Automatisierungsdokument.

Behebungsprotokolle werden in einem Amazon S3 S3-Bucket gespeichert. Sie können die Daten im S3-Bucket verwenden, um benutzerdefinierte QuickSight Dashboards für die Berichterstattung zu erstellen. AMS stellt auf Anfrage auch Berichte für Trusted Remediator bereit. Um diese Berichte zu erhalten, wenden Sie sich an Ihren CSDM. Weitere Informationen finden Sie unter Trusted Remediator-Berichte.

Wichtige Begriffe für Trusted Remediator

Die folgenden Begriffe sollten Sie kennen, wenn Sie Trusted Remediator in AMS verwenden:

- AWS Trusted Advisor und AWS Compute Optimizer: Cloud-Optimierungsdienste bereitgestellt von AWS. Trusted Advisor und Compute Optimizer untersuchen Ihre AWS Umgebung und geben Empfehlungen auf der Grundlage von Best Practices in den folgenden sechs Kategorien:
  - Kostenoptimierung
  - Performance
  - Sicherheit
  - Fehlertoleranz
  - Operative Exzellenz
  - Service Limits

  Weitere Informationen erhalten Sie unter AWS Trusted Advisor und AWS Compute Optimizer.
- Trusted Remediator: Eine AMS-Problembehebungslösung für Trusted AdvisorPrüfungen und Empfehlungen. AWS Compute Optimizer Trusted Remediator hilft Ihnen dabei, Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen mit bekannten Best Practices sicher zu beheben, um Sicherheit und Leistung zu verbessern und Kosten zu senken. Trusted Remediator ist einfach einzurichten und zu konfigurieren. Sie konfigurieren einmal und Trusted Remediator führt die Problembehebungen nach Ihrem bevorzugten Zeitplan (täglich oder wöchentlich) durch.
- AWS Systems Manager SSM-Dokument: Eine JSON- oder YAML-Datei, die die Aktionen definiert, die auf Ihren Ressourcen AWS Systems Manager ausgeführt werden. AWS Das SSM-Dokument dient als deklarative Spezifikation zur Automatisierung betrieblicher Aufgaben über mehrere AWS Ressourcen und Instanzen hinweg.
- AWS Systems Manager OpsCenter OpsItem: Eine Cloud-Ressource für das betriebliche Problemmanagement, mit der Sie betriebliche Probleme in Ihrer AWS Umgebung verfolgen und lösen können. OpsItems bietet eine zentrale Ansicht und ein Verwaltungssystem für betriebliche Daten und Probleme in allen AWS-Services Ressourcen. Jedes Problem OpsItem stellt ein betriebliches Problem dar, z. B. ein potenzielles Sicherheitsrisiko, ein Leistungsproblem oder einen betrieblichen Vorfall.
- Konfiguration: Eine Konfiguration ist eine Reihe von Attributen, die in gespeichert sind AWS AppConfig, eine Fähigkeit von AWS Systems Manager. Die Trusted Remediator-Anwendung AWS AppConfig hilft bei der Konfiguration von Behebungen auf Kontoebene. Sie können die AWS AppConfig Konsole oder die API verwenden, um Konfigurationen zu bearbeiten.

- Ausführungsmodus: Der Ausführungsmodus ist ein Konfigurationsattribut, das festlegt, wie die Behebung für jedes Trusted Advisor Prüfergebnis ausgeführt wird. Es gibt vier unterstützte Ausführungsmodi: Automatisiert, Manuell, Bedingt, Inaktiv.
- Überschreiben von Ressourcen: Diese Funktion verwendet Ressourcen-Tags, um eine Konfiguration für bestimmte Ressourcen zu überschreiben.
- Protokoll der Behebungselemente: Eine Protokolldatei im S3-Protokoll-Bucket von Trusted Remediator Remediator. Das Behebungselementprotokoll wird erstellt, wenn die Behebung erstellt wird. OpsItems Diese Protokolldatei enthält manuelle Ausführungskorrekturen OpsItems und automatische Ausführungskorrekturen. OpsItems Verwenden Sie diese Protokolldatei, um alle Behebungselemente nachzuverfolgen.
- Protokoll zur automatisierten Problembehebung: Eine Protokolldatei im S3-Protokoll-Bucket der Trusted Remediator-Korrektur. Das Protokoll zur automatischen Problembehebung wird erstellt, wenn die automatisierte Ausführung eines SSM-Dokuments abgeschlossen ist. Dieses Protokoll enthält SSM-Ausführungsdetails für die automatische Behebung der Ausführung. OpsItems Verwenden Sie diese Protokolldatei, um automatisierte Problembehebungen nachzuverfolgen.

Erste Schritte mit Trusted Remediator in AMS

Trusted Remediator ist in AMS ohne zusätzliche Kosten erhältlich. Trusted Remediator unterstützt Konfigurationen mit einem Konto und mehreren Konten.

Integrieren Sie Trusted Remediator

Um Ihre AMS-Konten bei Trusted Remediator zu integrieren, senden Sie eine E-Mail an Ihre Cloud-Architekten oder Cloud Service Delivery Manager ()CSDMs. Geben Sie in der E-Mail folgende Informationen an:

- AWS-Konten: Die zwölfstellige Konto-Identifikationsnummer. Alle Konten, die Sie bei Trusted Remediator registrieren möchten, müssen demselben Accelerate-Kunden gehören.
  - Delegiertes Administratorkonto: Das Konto, das für Trusted Advisor die Compute Optimizer-Prüfkonfiguration für einzelne oder mehrere Konten verwendet wird.
  - Mitgliedskonten: Dies sind die Konten, die mit dem delegierten Administratorkonto verknüpft sind. Diese Konten erben die Konfigurationen des delegierten Administratorkontos. Sie können ein Mitgliedskonto oder mehrere Mitgliedskonten haben.

> **Note**
>
> Mitgliedskonten erben die Konfigurationen des delegierten Administratorkontos. Wenn Sie unterschiedliche Konfigurationen für bestimmte Konten benötigen, integrieren Sie mehrere delegierte Administratorkonten mit Ihren bevorzugten Konfigurationen. Planen Sie die Kontostruktur und die Konfigurationen mit Ihren Cloud-Architekten, bevor Sie an Bord gehen.

- AWS-Regionen: Der AWS-Regionen Ort, an dem sich Ihre Ressourcen befinden. Eine Liste von finden Sie AWS-Regionen unter AWS-Services Nach Regionen geordnet.
- Behebungszeitplan und -zeit: Ihr bevorzugter Behebungszeitplan (täglich oder wöchentlich). Trusted Remediator sammelt Trusted Advisor Prüfungen und leitet die Behebung zum geplanten Zeitpunkt ein. Sie können beispielsweise den Zeitplan für die Problembehebung auf jeden Sonntag um 1:00 Uhr (australische Eastern Standard Time) festlegen.
- Benachrichtigungs-E-Mail: Trusted Remediator verwendet die Benachrichtigungs-E-Mail, um Sie täglich darüber zu informieren, ob es Abhilfemaßnahmen gibt. Der Betreff der Benachrichtigungs-E-Mail lautet „Trusted Remediator Remediation Summary“ und der Inhalt enthält Informationen zu Trusted Remediator-Korrekturen, die in den letzten 24 Stunden durchgeführt wurden.

> **Note**
>
> Überprüfen Sie Ihre Anwendungen und Ressourcen nach jeder geplanten Problembehebung. Wenn Sie zusätzlichen Support benötigen, wenden Sie sich an AMS.

Nachdem Sie Ihre Onboard-Anfrage mit den erforderlichen Angaben bei Ihrer CA oder CSDM eingereicht haben, leitet AMS Ihre Konten bei Trusted Remediator ein. Trusted Remediator verwendet eine Fähigkeit von AWS AppConfig AWS Systems Manager, um die Konfiguration für die Prüfungen zu definieren. Trusted Advisor Bei diesen Konfigurationen handelt es sich um eine Reihe von Attributen, die in AWS AppConfig gespeichert sind. Um zu verhindern, dass Ihre Ressourcen unbefugt belastet werden, werden alle unterstützten Trusted Advisor Prüfungen auf Inaktiv gesetzt, wenn Konten in Trusted Remediator integriert werden. Nach dem Onboarding können Sie die Konfigurationen über die AWS AppConfig Konsole oder API verwalten. Diese Konfigurationen helfen Ihnen dabei, bestimmte Trusted Advisor Prüfungen automatisch zu korrigieren oder die verbleibenden Prüfungen zu bewerten und manuell zu korrigieren. Die Konfigurationen sind in hohem Maße anpassbar, sodass Sie Konfigurationen für jede Trusted Advisor Prüfung anwenden können. Weitere

Informationen finden Sie unter Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator.

Wählen Sie die Prüfungen und Empfehlungen aus, die behoben werden sollen

Standardmäßig ist der Wiederherstellungsausführungsmodus für alle Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen in Ihrer Konfiguration inaktiv. Dies verhindert unbefugte Problembehebungen und schont Ressourcen. AMS stellt kuratierte Dokumente zur SSM-Automatisierung zur Behebung von Schecks zur Trusted Advisor Verfügung.

Gehen Sie wie folgt vor, um die Prüfungen auszuwählen, die Sie mit Trusted Remediator korrigieren möchten:

1. Sehen Sie sich die Liste der unterstützten Trusted Advisor und Compute Optimizer Optimizer-Empfehlungen oder den Namen der zugehörigen SSM-Automatisierungsdokumente an, um zu entscheiden, welche Prüfungen und Empfehlungen Sie mit Trusted Remediator korrigieren möchten.
2. Aktualisieren Sie Ihre Konfiguration, um die Problembehebung für Ihre ausgewählten Trusted Advisor Prüfungen zu aktivieren. Anweisungen zur Auswahl von Prüfungen finden Sie unterKonfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator.

Verfolgen Sie Ihre Abhilfemaßnahmen in Trusted Remediator

Nachdem Sie Ihre Konfiguration auf Kontoebene aktualisiert haben, erstellt Trusted Remediator für jede Problembehebung neue Änderungen. OpsItems Trusted Remediator führt das SSM-Dokument zur automatisierten Behebung gemäß Ihrem Behebungsplan aus. OpsItems Anweisungen, wie Sie alle Behebungsmaßnahmen OpsItems von der Systems Manager OpsCenter Manager-Konsole aus anzeigen können, finden Sie unterBehebungen in Trusted Remediator nachverfolgen.

Führen Sie manuelle Korrekturen in Trusted Remediator aus

Sie können Prüfungen manuell korrigieren. Trusted Advisor Wenn Sie eine manuelle Korrektur einleiten, erstellt Trusted Remediator eine manuelle Ausführung. OpsItem Sie müssen das Dokument zur SSM-Automatisierung überprüfen und initiieren, um das Problem zu beheben. OpsItems Weitere Informationen finden Sie unter Führen Sie manuelle Korrekturen in Trusted Remediator aus.

Compute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden

In der folgenden Tabelle sind die unterstützten Compute Optimizer Optimizer-Empfehlungen, SSM-Automatisierungsdokumente, vorkonfigurierte Parameter und das erwartete Ergebnis der Automatisierungsdokumente aufgeführt. Überprüfen Sie das erwartete Ergebnis, um mögliche Risiken auf der Grundlage Ihrer Geschäftsanforderungen besser zu verstehen, bevor Sie ein SSM-Automatisierungsdokument zur Behebung von Prüfungen aktivieren.

Stellen Sie sicher, dass die entsprechende Konfigurationsregel für jede Compute Optimizer Optimizer-Prüfung für die unterstützten Prüfungen vorhanden ist, für die Sie die Problembehebung aktivieren möchten. Weitere Informationen finden Sie unter AWS Compute Optimizer Für Trusted Advisor Prüfungen anmelden.

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Passende Dimensionierung		
Empfehlungen Amazon EC2 Amazon-Instances	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Der EC2 Amazon-Instance-Typ wurde gemäß den Empfehlungen von Compute Optimizer aktualisiert. Es werden die optimalsten Optionen ausgewählt, wobei dieselben Plattformparameter (Architektur, Hypervisor, Netzwerkschnittstelle, Virtualisierungstyp usw.) beibehalten werden, sofern die Option vorhanden ist.	• MinimumDaysSinceLastChange: Der Parameter zur Angabe der Mindestanzahl von Tagen seit der letzten Änderung des Instanztyps. Der Standardwert ist 7 Tage. Keine Einschränkungen • AMIBeforeResize erstellen: Um das Instance-AMI vor der Größenänderung als Backup zu erstellen, setzen Sie den Wert auf „True“. Um kein Backup zu erstellen, setzen Sie den Wert auf „False“. Die Standardeinstellung ist „True“. Keine Einschränkungen

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Amazon EBS-Volumenempfehlungen	AWSManagedServices-ModifyEBSVolume Das Amazon EBS-Volume wird gemäß den Empfehlungen von Compute Optimizer geändert. Die Änderung kann Volumetyp, Größe, IOPS und Volume-Generierung (gp2, gp3 usw.) umfassen.	• CreateSnapshot: Um vor dem Ändern des Volumes einen Snapshot zu erstellen, setzen Sie den Wert auf „True“. Um keinen Snapshot zu erstellen, setzen Sie ihn auf „False“. Die Standarde instellung ist „True“. Keine Einschränkungen • VolumeType: Der gewünschte Datenträgertyp. Wenn kein Typ angegeben ist, wird der vorhanden e Typ beibehalten. Keine Einschränkungen • VolumeSize: Die gewünschte Größe des Volumes in GiB. Die Größe des Zielvolumes muss größer oder gleich der vorhanden en Größe des Volumes sein. Wenn keine Größe angegeben ist, wird die vorhandene Größe beibehalt en. Keine Einschränkungen • Iops: Die angeforderte Anzahl von I/O Vorgängen pro Sekunde (IOPS). Dieser Parameter ist nur für io1-, io2- und gp3-Volumes gültig. Keine Einschränkungen • Durchsatz: Der Durchsatz, der für ein Volumen bereitgestellt werden

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		muss, mit einem Maximum von 1000 MiB/s. Dieser Parameter ist nur für GP3-Volumes gültig. Keine Einschränkungen • RemediateStackDrift: Wenn eine Abweichung durch eine Änderung der Lautstärke verursacht wird, wird die Einstellung auf „True“ gesetzt, um die Behebung von Abweichungen einzuleiten. Um nicht zu versuchen, Abweichungen zu beheben, setzen Sie den Wert auf „Falsch“. Die Standardeinstellung ist „True“. Keine Einschränkungen
Empfehlungen für Lambda-Funktionen	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda Funktionsspeicher optimiert gemäß den Empfehlungen von Compute Optimizer.	RecommendedMemorySize : Benutzerdefinierte Speichergröße, falls diese von den empfohlenen Optionen abweicht. Keine Einschränkungen
Ungenutzte Ressourcen		

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Amazon EBS-Volume im Leerlauf	AWSManagedServices-DeleteUnusedEBSVolume Ein nicht angehängtes Amazon EBS-Volume wird gelöscht.	• CreateSnapshot: Um vor dem Löschen des Volumes einen Snapshot zu erstellen, legen Sie den Wert auf „True“ fest. Um keinen Snapshot zu erstellen, setzen Sie ihn auf „False“. Die Standardeinstellung ist „True“. Keine Einschränkungen • MinimumUnattachedDays: Mindestens unangehängte Tage des zu löschenden Amazon EBS-Volumes, bis zu 62 Tage. Die Standardeinstellung ist 7. Keine Einschränkungen
Inaktive EC2 Amazon-Instance	AWSManagedServices-StopEC2Instanzen Die inaktive EC2 Amazon-Instance wird gestoppt.	ForceStopWithInstanceStore: Um den Stopp für Instances zu erzwingen, die den Instance-Speicher verwenden, setzen Sie den Wert auf „True“. Um den Stopp nicht zu erzwingen, setzen Sie den Wert auf „False“. Der Standardwert 'False' verhindert, dass die Instanz beendet wird. Keine Einschränkungen

Option zur Optimierung	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Amazon RDS-Instance im Leerlauf	AWSManagedServices-StopIdleRDSInstance Stoppen Sie eine Amazon RDS-Instance im Leerlauf. Unterstützte Engines sind: MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL. Dieses Dokument gilt nicht für Aurora MySQL und Aurora PostgreSQL. Die Instanz wird für bis zu 7 Tage gestoppt und automatisch neu gestartet.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor von Trusted Remediator unterstützte Prüfungen

In der folgenden Tabelle sind die unterstützten Trusted Advisor Prüfungen, SSM-Automatisierungsdokumente, vorkonfigurierte Parameter und das erwartete Ergebnis der Automatisierungsdokumente aufgeführt. Überprüfen Sie das erwartete Ergebnis, um mögliche Risiken auf der Grundlage Ihrer Geschäftsanforderungen besser zu verstehen, bevor Sie ein Dokument zur SSM-Automatisierung zur Behebung von Prüfungen aktivieren.

Stellen Sie sicher, dass die entsprechende Konfigurationsregel für jede Trusted Advisor Prüfung für die unterstützten Prüfungen vorhanden ist, für die Sie die Problembehebung aktivieren möchten. Weitere Informationen finden Sie unter AWS Trusted Advisor Checks anzeigen, die von bereitgestellt werden AWS Config. Wenn eine Prüfung über entsprechende AWS Security Hub CSPM Steuerelemente verfügt, stellen Sie sicher, dass die Security Hub-Steuerung aktiviert ist. Weitere Informationen finden Sie unter Steuerelemente in Security Hub aktivieren. Informationen zur Verwaltung vorkonfigurierter Parameter finden Sie unter Konfiguration der Trusted Advisor Advisor-Prüfbehebung in Trusted Remediator.

Trusted Advisor Prüfungen zur Kostenoptimierung werden von Trusted Remediator unterstützt

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Z4 AUBRNSmz Nicht zugeordnete elastische IP-Adressen	AWSManagedServices-TrustedRemediatorReleaseElasticIP Gibt eine elastische IP-Adresse frei, die keiner Ressource zugeordnet ist.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c18d2gz150 — Amazon-Instances wurden gestoppt EC2	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime — EC2 Amazon-Instances, die für eine bestimmte Anzahl von Tagen gestoppt wurden, werden beendet.	• AMIBeforeKündigung erstellen: Um das Instance-AMI als Backup zu erstellen, bevor Sie die EC2 Amazon-Instance beenden, wählen Sie`true`. Um vor dem Beenden kein Backup zu erstellen, wählen Sie. `false` Der Standardwert ist `true`. • AllowedDays: Die Anzahl der Tage, an denen sich die Instanz im gestoppten Zustand befindet, bevor sie beendet wird. Der Standardwert ist 30. Keine Einschränkungen
c18d2gz128 Amazon-ECR-Repository ohne konfigurierte Lebenszyklus-Richtlinie	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Erstellt eine Lebenszyklusrichtlinie für das angegebene Repository, falls noch keine Lebenszyklusrichtlinie vorhanden ist.	ImageAgeLimit: Die maximale Altersgrenze in Tagen (1—365) für „jedes“ Bild im Amazon ECR-Repository. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
DAvU99Dc4C Nicht ausgelastete Amazon EBS-Volumes	AWSManagedServices-DeleteUnusedEBSVolume Löscht nicht ausgelastete Amazon EBS-Volumes, wenn die Volumes in den letzten 7 Tagen nicht angehängt wurden. Ein Amazon EBS-Snapshot wird standardmäßig erstellt.	• CreateSnapshot: Wenn auf gesetzt`true`, erstellt die Automatisierung einen Snapshot des Amazon EBS-Volumes, bevor es gelöscht wird. Die Standardeinstellung lautet `true`. Gültige Werte sind `true` und `false` (Groß- und Kleinschreibung beachten). • MinimumUnattachedDays: Mindestdauer des zu löschenden EBS-Volumes ohne Anhängen, bis zu 62 Tage. Wenn diese Einstellung auf gesetzt ist`0`, überprüft das SSM-Dokument nicht den Zeitraum, in dem das Volumen nicht angehängt wurde, und löscht das Volume, wenn das Volume derzeit nicht angehängt ist. Der Standardwert ist. 7 Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
hj M8 LMh88u Load Balancer im Leerlauf	AWSManagedServices-DeleteIdleClassicLoadBalancer Löscht einen Classic Load Balancer im Leerlauf, wenn er unbenutzt ist und keine Instances registriert sind.	IdleLoadBalancerDays: Die Anzahl der Tage, an denen der Classic Load Balancer 0 angeforderte Verbindungen hat, bevor er als inaktiv eingestuft wird. Die Standardeinstellung ist sieben Tage. Wenn die auto Ausführung aktiviert ist, löscht die Automatisierung inaktive Classic Load Balancer, wenn keine aktiven Back-End-Instances vorhanden sind. Für alle Classic Load Balancer im Leerlauf, die über aktive Back-End-Instances, aber keine fehlerfreien Back-End-Instances verfügen, wird keine auto Korrektur verwendet und OpsItems für die manuelle Korrektur wird eine automatische Korrektur erstellt.
TI 39 Half U8 Amazon RDS-DB-Instances im Leerlauf	AWSManagedServices-StopIdleRDSInstance Die Amazon RDS-DB-Instance, die sich in den letzten sieben Tagen im Leerlauf befand, wurde gestoppt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
COr6dfpM05 AWS Lambda aufgrund der Speichergröße überdimensionierte Funktionen	AWSManagedServices-ResizeLambdaMemory AWS Lambda Die Speichergröße der Funktion wird auf die empfohlene Speichergröße von angepasst. Trusted Advisor	RecommendedMemorySize: Die empfohlene Speicherzuweisung für die Lambda-Funktion. Der Wertebereich liegt zwischen 128 und 10240. Wenn die Größe der Lambda-Funktion vor der Ausführung der Automatisierung geändert wurde, werden die Einstellungen möglicherweise von dieser Automatisierung mit dem von empfohlenen Wert überschrieben. Trusted Advisor
QCH7dWOUx1 EC2 Amazon-Instances mit geringer Auslastung	AWSManagedServices-StopEC2Instance (Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus.) EC2 Amazon-Instances mit geringer Auslastung werden gestoppt.	ForceStopWithInstanceStore: Auf setzen, `true` um das Stoppen von Instances mithilfe des Instance-Speichers zu erzwingen. Ansonsten auf `false` festlegen. Der Standardwert von `false` verhindert, dass die Instanz gestoppt wird. Gültige Werte sind wahr oder falsch (Groß- und Kleinschreibung beachten). Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
QCH7dWOUx1 EC2 Amazon-Instances mit geringer Auslastung	AWSManagedServices-ResizeInstanceByOneLevel Die Größe der EC2 Amazon-Instance wird innerhalb desselben Instance-Familientyps um einen Instance-Typ nach unten geändert. Die Instance wird während der Größenänderung gestoppt und gestartet und nach Abschluss der Ausführung des SSM-Dokuments wieder in den Ausgangszustand versetzt. Diese Automatisierung unterstützt keine Größenänderung von Instances, die sich in einer Auto Scaling Scaling-Gruppe befinden.	• MinimumDaysSinceLastChange: Mindestanzahl von Tagen seit der letzten Änderung des Instance-Typs. Wenn der Instanztyp innerhalb einer bestimmten Zeit geändert wurde, wird der Instanztyp nicht geändert. Verwenden Sie`0`, um diese Überprüfung zu überspringen. Der Standardwert ist 7. • AMIBeforeGröße ändern: Um das Instanz-AMI vor der Größenänderung als Backup zu erstellen, wählen Sie`true`. Um kein Backup zu erstellen, wählen Sie`false`. Der Standardwert ist `false`. Gültige Werte sind `true` und `false` (Groß- und Kleinschreibung beachten). • ResizeIfStopped: Um mit der Änderung der Instanzgröße fortzufahren, auch wenn sich die Instance im gestoppten Zustand befindet, wählen Sie`true`. Um die Größe der Instanz nicht automatisch zu ändern, wenn sie gestoppt ist, wählen Sie`false`. Gültige Werte sind `true` und `false` (Groß- und Kleinschreibung beachten). Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
QCH7dWOUx1 EC2 Amazon-Instances mit geringer Auslastung	AWSManagedServices-TerminateInstance EC2 Amazon-Instances mit geringer Auslastung werden beendet, wenn sie nicht Teil einer Auto Scaling Scaling-Gruppe sind und der Kündigungsschutz nicht aktiviert ist. Ein AMI wird standardmäßig erstellt.	AMIBeforeKündigung erstellen: Setzen Sie diese Option auf `true` oder, `false` um ein Instance-AMI als Backup zu erstellen, bevor Sie die EC2 Instance beenden. Der Standardwert ist `true`. Gültige Werte sind `true` und `false` (Groß- und Kleinschreibung beachten). Keine Einschränkungen
G31sq1e9u Nicht ausgelastete Amazon Redshift-Cluster	AWSManagedServices-PauseRedshiftCluster Der Amazon Redshift Redshift-Cluster ist angehalten.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1cj39rr6v Konfiguration zum Abbruch unvollständiger mehrteiliger Uploads in Amazon S3	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Der Amazon S3 S3-Bucket ist mit einer Lebenszyklusregel konfiguriert, um mehrteilige Uploads abzubrechen, die nach bestimmten Tagen unvollständig bleiben.	DaysAfterInitiation: Die Anzahl der Tage, nach denen Amazon S3 einen unvollständigen mehrteiligen Upload stoppt. Die Standardeinstellung ist auf 7 Tage festgelegt. Keine Einschränkungen
c1z7kmr00n Amazon-Empfehlungen zur EC2 Kostenoptimierung für Instances	Verwenden Sie EC2 Amazon-Instance-Empfehlungen und Idle EC2 Amazon-Instance vonCompute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1z7kmr02n Amazon EBS-Empfehlungen zur Kostenoptimierung für Volumen	Verwenden Sie Amazon EBS-Volumenempfehlungen und Amazon EBS-Volume im Leerlauf von. Compute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1z7kmr03n Empfehlungen zur Amazon RDS-Kostenoptimierung für DB-Instances	Verwenden Sie die Amazon RDS-Instance im Leerlauf vonCompute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1z7kmr05n AWS Lambda Empfehlungen zur Kostenoptimierung für Funktionen	Verwenden Sie Lambda-Funktionsempfehlungen vonCompute Optimizer Optimizer-Empfehlungen, die von Trusted Remediator unterstützt werden.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor Sicherheitsüberprüfungen, die von Trusted Remediator unterstützt werden

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
12 Fnkpl8Y5	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey	Vorkonfigurierte Parameter sind nicht zulässig.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Exposed Access Keys	Der offengelegte IAM-Zugriffsschlüssel ist deaktiviert.	Anwendungen, die mit einem offengelegten IAM-Zugriffsschlüssel konfiguriert sind, können sich nicht authentifizieren.
Hs4Ma3G127 - API-Gateway-REST- und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein AWS Security Hub CSPM APIGatewayEntsprechender Check: 1.	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging Die Ausführungsprotokollierung ist auf der API-Phase aktiviert.	LogLevel: Protokollierungsebene zur Aktivierung der Ausführungsprotokollierung, `ERROR` — Die Protokollierung ist nur für Fehler aktiviert. `INFO` - Die Protokollierung ist für alle Ereignisse aktiviert. Sie müssen API Gateway die Berechtigung zum Lesen und Schreiben von Protokollen CloudWatch für Ihr Konto erteilen, um das Ausführungsprotokoll zu aktivieren. Weitere Informationen finden Sie unter CloudWatch Protokollierung für REST APIs in API Gateway einrichten.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G129 — API Gateway REST-API-Stufen sollten die Ablaufverfolgung aktiviert haben AWS X-Ray AWS Security Hub CSPM APIGatewayEntsprechender Check: 3.	AWSManagedServices-EnableApiGateWayXRayTracing X-Ray-Tracing ist auf der API-Phase aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G202 - API-Gateway-REST-API-Cache-Daten sollten im Ruhezustand verschlüsselt werden AWS Security Hub CSPM Entsprechender APIGatewayScheck: 5.	AWSManagedServices-EnableAPIGatewayCacheEncryption Aktivieren Sie die Verschlüsselung im Ruhezustand für API-Gateway-REST-API-Cachedaten, wenn in der API-Gateway-REST-API-Stufe der Cache aktiviert ist.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G177 - Entsprechende AWS Security Hub CSPM Prüfung — Auto Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Integritätsprüfungen verwenden 1. AutoScaling	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck Elastic Load Balancing Health Checks sind für die Auto Scaling Group aktiviert.	HealthCheckGracePeriod: Die Zeit in Sekunden, die Auto Scaling wartet, bevor der Integritätsstatus einer Amazon Elastic Compute Cloud-Instance überprüft wird, die in Betrieb genommen wurde. Die Aktivierung von Elastic Load Balancing Health Checks kann dazu führen, dass eine laufende Instance ersetzt wird, wenn einer der Elastic Load Balancing Load Balancer, die der Auto Scaling Scaling-Gruppe zugeordnet sind, sie als fehlerhaft meldet. Weitere Informationen finden Sie unter Einen Elastic Load Balancing Load Balancer zu Ihrer Auto Scaling Scaling-Gruppe hinzufügen
Hs4Ma3G245 — CloudFormation Stacks sollten in Amazon Simple Notification Service integriert werden AWS Security Hub CSPM Entsprechender CloudFormationScheck: 1.	AWSManagedServices-EnableCFNStackNotification Ordnen Sie einen CloudFormation Stack einem Amazon SNS SNS-Thema für die Benachrichtigung zu.	BenachrichtigungARNs: Die ARNs Amazon SNS SNS-Themen, die mit ausgewählten CloudFormation Stacks verknüpft werden sollen. Um die auto Korrektur zu aktivieren, muss der `NotificationARNs` vorkonfigurierte Parameter angegeben werden.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G210 — Bei Distributionen sollte die Protokollierung aktiviert sein CloudFront Entsprechender AWS Security Hub CSPM Scheck CloudFront: 2.	AWSManagedServices-EnableCloudFrontDistributionLogging Die Protokollierung ist für CloudFront Amazon-Distributionen aktiviert.	• BucketName: Der Name des Amazon S3 S3-Buckets, in dem Sie Zugriffsprotokolle speichern möchten. • S3KeyPrefix: Das Präfix für den Standort im S3-Bucket für die CloudFront Amazon-Verteilungsprotokolle. • IncludeCookies: Gibt an, ob Cookies in die Zugriffsprotokolle aufgenommen werden sollen. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: • BucketName • S3KeyPrefix • IncludeCookies Informationen zu diesen Behebungsbeschränkungen finden Sie unter Wie aktiviere ich die Protokollierung für meine Distribution? CloudFront

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G109 — CloudTrail Die Überprüfung der Protokolldatei sollte aktiviert sein AWS Security Hub CSPM Entsprechender CloudTrailCheck: 4.	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation Aktiviert die Überprüfung des CloudTrail Trail-Logs.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G108 — CloudTrail Trails sollten in Amazon Logs integriert werden CloudWatch Entsprechender AWS Security Hub CSPM CloudTrailScheck: 5.	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail ist in CloudWatch Logs integriert.	• CloudWatchLogsLogGroupName: Name der CloudWatch Logs-Protokollgruppe, an die CloudTrail Logs übermittelt werden. Sie müssen eine Protokollgruppe verwenden, die in Ihrem Konto vorhanden ist. • CloudWatchLogsRoleName: Name der IAM-Rolle, von der der CloudWatch Logs-Endpunkt annehmen soll, in die Protokollgruppe eines Benutzers zu schreiben. Sie müssen eine Rolle verwenden, die in Ihrem Konto vorhanden ist. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G217 — CodeBuild Projektum gebungen sollten über eine Protokoll ierungsko nfiguration verfügen AWS Entsprechender AWS Security Hub CSPM CodeBuild Scheck: 4.	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig Aktiviert die Protokollierung für das CodeBuild Projekt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G306 - Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein Entsprech ender AWS Security Hub CSPM Check: DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Entfernt den öffentlichen Zugriff aus dem manuellen Cluster-Snapshot von Amazon DocumentDB.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G308 — Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Check: DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Aktiviert den Löschschutz für den Amazon DocumentDB-Cluster.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G323 - Bei DynamoDB-Tabellen sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Check: DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection Aktiviert den Löschschutz für DynamoDB-Tabellen, die nicht von AMS stammen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
EPS02JT06W — Öffentliche Amazon EBS-Snapshots	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot Der öffentliche Zugriff für Amazon EBS Snapshot ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G118 - VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder ausgehenden Verkehr zulassen AWS Security Hub CSPM Entsprechender EC2Scheck: 2.	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Alle Eingangs- und Ausgangsregeln in der Standardsicherheitsgruppe werden entfernt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G117 — Angehängte EBS-Volumes sollten im Ruhezustand verschlüsselt werden AWS Security Hub CSPM Entsprechender EC2Check: 3.	AWSManagedServices-EncryptInstanceVolume Das angehängte Amazon EBS-Volume auf der Instance ist verschlüsselt.	• KMSKeyID: AWS KMS Schlüssel-ID oder ARN zum Verschlüsseln des Volumes. • DeleteStaleNonEncryptedSnapshotBackups: Eine Markierung, die entscheidet, ob das Snapshot-Backup der alten unverschlüsselten Volumes gelöscht werden soll. Die Instanz wird im Rahmen der Problembehebung neu gestartet und ein Rollback ist möglich, wenn diese Einstellung auf „Hilft bei der Wiederherstellung“ gesetzt `DeleteStaleNonEncryptedSnapshotBackups` `false` ist.
Hs4Ma3G120 — Gestoppte EC2 Instanzen sollten nach einem bestimmten Zeitraum entfernt werden AWS Security Hub CSPM Entsprechender EC2Scheck: 4.	AWSManagedServices-TerminateInstance(Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus) EC2 Amazon-Instances, die für 30 Tage gestoppt wurden, werden beendet.	AMIBeforeKündigung erstellen:. Um das Instance-AMI vor dem Beenden der EC2 Instance als Backup zu erstellen, wählen Sie`true`. Um vor dem Beenden kein Backup zu erstellen, wählen Sie. `false` Der Standardwert ist `true`. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G120 — Gestoppte EC2 Instanzen sollten nach einem bestimmten Zeitraum entfernt werden AWS Security Hub CSPM Entsprechender EC2Scheck: 4.	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime — EC2 Amazon-Instances, die für die im Security Hub definierte Anzahl von Tagen gestoppt wurden (Standardwert ist 30), werden beendet.	AMIBeforeKündigung erstellen: Um das Instance-AMI vor dem Beenden der EC2 Instance als Backup zu erstellen, wählen Sie`true`. Um vor dem Beenden kein Backup zu erstellen, wählen Sie. `false` Der Standardwert ist `true`. Keine Einschränkungen
Hs4Ma3G121 — Die EBS-Standardverschlüsselung sollte aktiviert sein Entsprechender AWS Security Hub CSPM EC2Scheck: 7.	AWSManagedServices-EncryptEBSByDefault Die Amazon EBS-Verschlüsselung ist standardmäßig aktiviert für AWS-Region	Vorkonfigurierte Parameter sind nicht zulässig. Die standardmäßige Verschlüsselung ist eine regionsspezifische Einstellung. Wenn Sie es für eine Region aktivieren, können Sie es nicht für einzelne Volumes oder Snapshots in dieser Region deaktivieren.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G124 — EC2 Amazon-Instances sollten Instance Metadata Service Version 2 () verwenden IMDSv2 AWS Security Hub CSPM Entsprechender EC2Scheck: 8.	AWSManagedServices-TrustedRemediatorInstanz aktivieren EC2 IMDSv2 EC2 Amazon-Instances verwenden Instance Metadata Service Version 2 (IMDSv2).	• IMDSv1MetricCheckPeriod: Die Anzahl der Tage (42-455), in denen IMDSv1 Nutzungsmetriken analysiert CloudWatch werden sollen. Wenn die EC2 Amazon-Instance innerhalb des angegebenen Zeitraums erstellt wurde, beginnt die Analyse mit dem Erstellungsdatum der Instance. • HttpPutResponseHopLimit: Die maximale Anzahl von Netzwerk-Hops, die für das Instance-Metadaten-Token zulässig sind. Dieser Wert kann zwischen 2 Hops 1 und Hops konfiguriert werden. Ein Hop-Limit von 1 schränkt den Token-Zugriff auf Prozesse ein, die direkt auf der Instance ausgeführt werden, während ein Hop-Limit von von den auf der Instance ausgeführten Containern den Zugriff 2 ermöglicht. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G207 — EC2 Subnetze sollten öffentliche IP-Adressen nicht automatisch zuweisen AWS Security Hub CSPM Entsprechender EC2Scheck: 1.5	AWSManagedServices-UpdateAutoAssignPublicIpv4 Adressen VPC-Subnetze sind so konfiguriert, dass öffentliche IP-Adressen nicht automatisch zugewiesen werden.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G209 — Nicht verwendete Network Access Control Lists wurden entfernt Entsprechender AWS Security Hub CSPM EC2Scheck: 1.6	AWSManagedServices-DeleteUnusedNACL Löschen Sie ungenutzte Netzwerk-ACL	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G215 - Unbenutzte EC2 Amazon-Sicherheitsgruppen sollten entfernt werden Entsprechender AWS Security Hub CSPM EC2Scheck: 2.2	AWSManagedServices-DeleteSecurityGroups Löschen Sie nicht verwendete Sicherheitsgruppen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G247 — Amazon EC2 Transit Gateway sollte VPC-Anhangsanfragen nicht automatisch akzeptieren AWS Security Hub CSPM Entsprechender EC2Scheck: 2.3	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Deaktiviert die automatische Annahme von VPC-Anhangsanforderungen für das angegebene Amazon EC2 Transit Gateway, das nicht von AMS stammt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G235 — Für private ECR-Repositorien sollte die Tag-Unveränderlichkeit konfiguriert sein Entsprechender AWS Security Hub CSPM Check: ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability Setzt die Mutabilitätseinstellungen für das Image-Tag für das angegebene Repository auf IMMUTABLE.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G216 — Für ECR-Repositorys sollte mindestens eine Lebenszyklusrichtlinie konfiguriert sein Entsprechender AWS Security Hub CSPM Scheck: ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy Für das ECR-Repository ist eine Lebenszyklusrichtlinie konfiguriert.	LifecyclePolicyText: Der Richtlinientext für das JSON-Repository, der auf das Repository angewendet werden soll. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: LifecyclePolicyText

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G325 — Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog Das Auditprotokoll ist für den EKS-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G183 — Der Application Load Balancer sollte so konfiguriert sein, dass er HTTP-Header löscht AWS Security Hub CSPM Entsprechender Check: ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer ist für ungültige Header-Felder konfiguriert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G184 — Die Protokollierung von Application Load Balancers und Classic Load Balancers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: ELB.5	AWSManagedServices-EnableELBLogging (Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus) Die Protokollierung von Application Load Balancer und Classic Load Balancer ist aktiviert.	• BucketName: Der Bucket-Name (nicht der ARN). Stellen Sie sicher, dass die Bucket-Richtlinie für die Protokollierung korrekt konfiguriert ist. • S3KeyPrefix: Das Präfix für den Speicherort im Amazon S3 S3-Bucket für die Elastic Load Balancing Balancing-Protokolle. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden: • BucketName • S3KeyPrefix Der Amazon S3 S3-Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Erlaubnis erteilt, die Zugriffsprotokolle in den Bucket zu schreiben.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G184 — Die Protokollierung von Application Load Balancers und Classic Load Balancers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: ELB.5	AWSManagedServices-EnableELBLoggingV2 Die Protokollierung von Application Load Balancer und Classic Load Balancer ist aktiviert.	• TargetBucketTagKey: Der Tag-Name (Groß- und Kleinschreibung beachten), der zur Identifizierung des Amazon S3 S3-Ziel-Buckets verwendet wird. Verwenden Sie diesen Wert zusammen mit`TargetBucketTagValue`, um den Bucket zu taggen, der als Ziel-Bucket für die Zugriffsprotokollierung dienen soll. • TargetBucketTagValue: Der Tag-Wert (Groß- und Kleinschreibung beachten), der zur Identifizierung des Amazon S3 S3-Ziel-Buckets verwendet wird. Verwenden Sie diesen Wert zusammen mit`TargetBucketTagKey`, um den Bucket zu taggen, der als Ziel-Bucket für die Zugriffsprotokollierung dienen soll. • S3BucketPrefix: Das Präfix (logische Hierarchie) für den Amazon S3 S3-Bucket. Das von Ihnen angegebene Präfix darf die Zeichenfolge `AWSLogs` nicht enthalten. Weitere Informationen finden Sie unter Organisieren von Objekten mit Präfixen. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfig

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		urierten Parameter angegeben werden: • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix Der Amazon S3 S3-Bucket muss über eine Bucket-Richtlinie verfügen, die Elastic Load Balancing die Erlaubnis erteilt, die Zugriffsprotokolle in den Bucket zu schreiben.
Hs4Ma3G326 — Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess Die Amazon EMR-Einstellungen für den öffentlichen Zugriff sperren sind für das Konto aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G135 - AWS KMS Schlüssel sollten nicht ungewollt gelöscht werden Entsprechender AWS Security Hub CSPM Scheck: KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS Das Löschen des Schlüssels wurde abgebrochen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G299 — Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein Entsprechender AWS Security Hub CSPM Scheck: Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection Aktiviert den Löschschutz für den Amazon Neptune Neptune-Cluster.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G319 — Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein AWS Security Hub CSPM Entsprechender NetworkFirewallScheck: 9.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection- Aktiviert den Löschschutz für die AWS-Netzwerk-Firewall.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G223 — OpenSearch Domains sollten Daten verschlüsseln, die zwischen Knoten gesendet werden Entsprechender AWS Security Hub CSPM OpenSearchScheck: 3.	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption Die Node-zu-Knoten-Verschlüsselung ist für die Domain aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Nachdem die node-to-node Verschlüsselung aktiviert wurde, können Sie die Einstellung nicht deaktivieren. Erstellen Sie stattdessen einen manuellen Snapshot der verschlüsselten Domain, erstellen Sie eine weitere Domain, migrieren Sie Ihre Daten und löschen Sie dann die alte Domain.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G222 — OpenSearch Die Protokollierung von Domänenfehlern in Logs sollte aktiviert sein CloudWatch Entsprechender AWS Security Hub CSPM Check: Opensearch.4	AWSManagedServices-EnableOpenSearchLogging Die Fehlerprotokollierung ist für die Domain aktiviert. OpenSearch	CloudWatchLogGroupArn: Der ARN einer Amazon CloudWatch Logs-Protokollgruppe. Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden:. CloudWatchLogGroupArn Die CloudWatch Amazon-Ressourcenrichtlinie muss mit Berechtigungen konfiguriert werden. Weitere Informationen finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service-Benutzerhandbuch
Hs4Ma3G221 — Für OpenSearch Domains sollte die Audit-Protokollierung aktiviert sein Entsprechender Check AWS Security Hub CSPM : Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch Domains sind mit aktivierter Audit-Protokollierung konfiguriert.	CloudWatchLogGroupArn: Der ARN der CloudWatch Logs-Gruppe, in der Logs veröffentlicht werden sollen. Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden: CloudWatchLogGroupArn Die CloudWatch Amazon-Ressourcenrichtlinie muss mit Berechtigungen konfiguriert werden. Weitere Informationen finden Sie unter Aktivieren von Audit-Logs im Amazon OpenSearch Service-Benutzerhandbuch

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G220 — Verbindungen zu OpenSearch Domains sollten mit TLS 1.2 verschlüsselt werden Entsprechender AWS Security Hub CSPM Check: Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 Die TLS-Richtlinie ist auf `policy-min-TLS-1-2-2019-07` gesetzt und nur verschlüsselte Verbindungen über HTTPS (TLS) sind erlaubt.	Vorkonfigurierte Parameter sind nicht erlaubt. Für die Verwendung von TLS 1.2 sind Verbindungen zu OpenSearch Domänen erforderlich. Das Verschlüsseln von Daten während der Übertragung kann die Leistung beeinträchtigen. Testen Sie Ihre Anwendungen mit dieser Funktion, um das Leistungsprofil und die Auswirkungen von TLS zu verstehen.
Hs4Ma3G194 — Amazon RDS-Snapshot sollte privat sein Entsprechender AWS Security Hub CSPM Scheck: RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Der öffentliche Zugriff für Amazon RDS-Snapshot ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G192 — RDS-DB-Instances sollten den öffentlichen Zugriff verbieten, wie in der Konfiguration festgelegt PubliclyAccessible AWS AWS Security Hub CSPM Entsprechender Check: RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance Deaktivieren Sie den öffentlichen Zugriff auf die RDS-DB-Instance.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G189 — Die erweiterte Überwachung ist für Amazon RDS-DB-Instances konfiguriert Entsprechender AWS Security Hub CSPM Scheck: RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring Aktivieren Sie die erweiterte Überwachung für Amazon RDS-DB-Instances	• MonitoringInterval: Das Intervall in Sekunden zwischen den Punkten, an denen Enhanced Monitoring-Metriken für die DB-Instance erfasst werden. Gültige Intervalle sind 0, 1, 5, 10, 15, 30 und 60. Um die Erfassung von Metriken für erweiterte Überwachung zu deaktivieren, geben Sie 0 an. • MonitoringRoleName: Der Name der IAM-Rolle, die es Amazon RDS ermöglicht, erweiterte Überwachungsmetriken an Amazon CloudWatch Logs zu senden. Wenn keine Rolle angegeben ist, `rds-monitoring-role` wird die Standardrolle verwendet oder erstellt, falls sie nicht existiert. Wenn die erweiterte Überwachung vor der Ausführung der Automatisierung aktiviert ist, werden die Einstellungen möglicherweise durch diese Automatisierung mit den in den vorkonfigurierten Parametern konfigurierten MonitoringRoleName Werten MonitoringInterval und überschrieben.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G190 — Bei Amazon RDS-Clust ern sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: RDS.7	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection Der Löschschutz ist für Amazon RDS-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G198 — Für Amazon RDS-DB-In stances sollte der Löschschutz aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: RDS.8	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection Der Löschschutz ist für Amazon RDS-Instances aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G199 — RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch Entsprechender AWS Security Hub CSPM Scheck: RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports RDS-Protokollexporte sind für die RDS-DB-Instance oder den RDS-DB-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. AWSServiceRoleForRDS für die dienstverknüpfte Rolle ist erforderlich.
Hs4Ma3G160 — Die IAM-Authentifizierung sollte für RDS-Instances konfiguriert werden Entsprechender AWS Security Hub CSPM Scheck: RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management Die Authentifizierung ist für die RDS-Instanz aktiviert.	ApplyImmediately: Gibt an, ob die Änderungen in dieser Anfrage und alle ausstehenden Änderungen so schnell wie möglich asynchron angewendet werden. Um die Änderung sofort anzuwenden, wählen Sie`true`. Um die Änderung für das nächste Wartungsfenster zu planen, wählen Sie`false`. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G161 — Die IAM-Authentifizierung sollte für RDS-Cluster konfiguriert werden Entsprechender AWS Security Hub CSPM Scheck: RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication Die IAM-Authentifizierung ist für den RDS-Cluster aktiviert.	ApplyImmediately: Gibt an, ob die Änderungen in dieser Anfrage und alle ausstehenden Änderungen so schnell wie möglich asynchron angewendet werden. Um die Änderung sofort anzuwenden, wählen Sie. `true` Um die Änderung für das nächste Wartungsfenster zu planen, wählen Sie`false`. Keine Einschränkungen
Hs4Ma3G162 — Automatische RDS-Upgrades für kleinere Versionen sollten aktiviert sein Entsprechender AWS Security Hub CSPM Scheck: RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Die automatische Upgrade-Konfiguration für Nebenversionen für Amazon RDS ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Die Amazon RDS-Instance muss sich im `available` Status befinden, damit diese Korrektur durchgeführt werden kann.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G163 — RDS-DB-Cluster sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren Entsprechender AWS Security Hub CSPM Scheck: RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagtosnapshot` Die Einstellung für Amazon RDS-Cluster ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Amazon RDS-Instances müssen sich im Status „Verfügbar“ befinden, damit diese Korrektur durchgeführt werden kann.
Hs4Ma3G164 — RDS-DB-Instances sollten so konfiguriert werden, dass sie Tags in Snapshots kopieren Entsprechender AWS Security Hub CSPM Scheck: RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagsToSnapshot` Die Einstellung für Amazon RDS ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Amazon RDS-Instances müssen sich im Status „Verfügbar“ befinden, damit diese Korrektur durchgeführt werden kann.
RSS93 HQwa1 Öffentliche Amazon RDS-Snapshots	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Der öffentliche Zugriff für Amazon RDS-Snapshot ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G103 — Amazon Redshift Redshift-Cluster sollten den öffentlichen Zugriff verbieten Entsprechender AWS Security Hub CSPM Scheck: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster Der öffentliche Zugriff auf den Amazon Redshift Redshift-Cluster ist deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Durch die Deaktivierung des öffentlichen Zugriffs werden alle Clients blockiert, die aus dem Internet kommen. Und der Amazon Redshift Redshift-Cluster befindet sich für einige Minuten im Änderungsstatus, während die Behebung den öffentlichen Zugriff auf den Cluster deaktiviert.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G106 — Bei Amazon Redshift Redshift-Clustern sollte die Auditprotokollierung aktiviert sein Entsprechender AWS Security Hub CSPM Check: Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging Die Audit-Protokollierung ist für Ihren Amazon Redshift Redshift-Cluster während des Wartungsfensters aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter bereitgestellt werden. BucketName: Der Bucket muss sich im selben Bucket befinden. AWS-Region Der Cluster muss über die Berechtigungen „Read Bucket“ und „Put Object“ verfügen. Wenn die Redshift-Clusterprotokollierung vor der Ausführung der Automatisierung aktiviert ist, werden die Protokollierungseinstellungen möglicherweise durch diese Automatisierung mit den in den vorkonfigurierten Parametern konfigurierten `S3KeyPrefix` Werten `BucketName` und überschrieben.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G105 — Bei Amazon Redshift sollten automatische Upgrades auf Hauptversionen aktiviert sein Entsprechender AWS Security Hub CSPM Check: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade-Upgrades der Hauptversionen werden während des Wartungsfensters automatisch auf den Cluster angewendet. Es gibt keine unmittelbare Ausfallzeit für den Amazon Redshift Redshift-Cluster, aber Ihr Amazon Redshift Redshift-Cluster kann während seines Wartungsfensters Ausfallzeiten haben, wenn er auf eine Hauptversion aktualisiert wird.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
Hs4Ma3G104 — Amazon Redshift Redshift-Cluster sollten erweitertes VPC-Routing verwenden Entsprechender AWS Security Hub CSPM Check: Redshift.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting Verbessertes VPC-Routing ist für Amazon Redshift Redshift-Cluster aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G173 — Die Einstellung S3 Block Public Access sollte auf Bucket-Ebene aktiviert sein AWS Security Hub CSPM Entsprechender Check: S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Öffentliche Zugriffssperren auf Bucket-Ebene werden für den Amazon S3 S3-Bucket angewendet.	Vorkonfigurierte Parameter sind nicht zulässig. Diese Korrektur kann sich auf die Verfügbarkeit von S3-Objekten auswirken. Informationen darüber, wie Amazon S3 den Zugriff bewertet, finden Sie unter Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G230 — Die Protokollierung des S3-Bucket-Servers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: S3.9	AWSManagedServices-EnableBucketAccessLogging(Standard-SSM-Dokument für den auto und manuellen Ausführungsmodus) Die Protokollierung Amazon S3 S3-Serverzugriffs ist aktiviert.	• TargetBucket: Der Name des S3-Buckets zum Speichern von Serverzugriffsprotokollen. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte (bei Werten wird Groß- und Kleinschreibung beachtet). Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden , wählen Sie`SimplePrefix` . Um den partitionierten S3-Schlüssel für Protokollobjekte und EventTime für das partitionierte Präfix zu verwenden, wählen Sie. `PartitionedPrefixEventTime` Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte Präfix zu verwenden , wählen Sie. `PartitionedPrefixDeliveryTime` Gültige Werte sind `SimplePrefix` , `PartitionedPrefixEventTime` und `PartitionedPrefixDeliveryTime` . Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden:. TargetBucket

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G230 — Die Protokollierung des S3-Bucket-Servers sollte aktiviert sein AWS Security Hub CSPM Entsprechender Check: S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 — Die Amazon S3 S3-Bucket-Protokollierung ist aktiviert.	• TargetBucketTagKey: Der Tag-Name (Groß- und Kleinschreibung beachten) zur Identifizierung des Ziel-Buckets. Verwenden Sie dieses und TargetBucketTagValue, um den Bucket zu taggen, der als Ziel-Bucket für die Zugriffsprotokollierung verwendet werden soll. • TargetBucketTagValue: Der Tag-Wert (Groß- und Kleinschreibung beachten) zur Identifizierung des Ziel-Buckets. Verwenden Sie diesen Wert und TargetBucketTagKeymarkieren Sie den Bucket, der als Ziel-Bucket für die Zugriffsprotokollierung verwendet werden soll. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte (Werte unterscheiden Groß- und Kleinschreibung): Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden, wählen Sie SimplePrefix. Um den partitionierten S3-Schlüssel für Protokollobjekte und das partitionierte Präfix zu verwenden EventTime , wählen Sie. PartitionedPrefixEventTime Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Präfix zu verwenden, wählen Sie. PartitionedPrefixDeliveryTime Der Standardwert ist PartitionedPrefixEventTime. Um die auto Korrektur zu aktivieren, müssen die folgenden Parameter angegeben werden: TargetBucketTagKeyund TargetBucketTagValue. Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Pfx0 RwqBli Amazon S3 Bucket-Berechtigungen	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Blockieren des öffentlichen Zugriffs	Es sind keine vorkonfigurierten Parameter zulässig. Diese Prüfung besteht aus mehreren Warnkriterien. Diese Automatisierung behebt Probleme mit dem öffentlichen Zugriff. Die Behebung anderer Konfigurationsprobleme, die mit gekennzeichnet sind, wird Trusted Advisor nicht unterstützt. Diese Korrektur unterstützt die Wiederherstellung von AWS-Service erstellten S3-Buckets (z. B. cf-templates-000000000000).
Hs4Ma3G272 — Benutzer sollten keinen Root-Zugriff auf Notebook-Instanzen haben SageMaker AWS Security Hub CSPM Entsprechender SageMaker Scheck: 3.	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess Der Root-Zugriff für Benutzer ist für die SageMaker Notebook-Instanz deaktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Diese Korrektur führt zu einem Ausfall, wenn sich die SageMaker Notebook-Instanz im Status befindet. InService

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G179 — SNS-Themen sollten im Ruhezustand wie folgt verschlüsselt werden AWS KMS Entsprechender AWS Security Hub CSPM Scheck: SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest Das SNS-Thema ist mit serverseitiger Verschlüsselung konfiguriert.	KmsKeyId: Die ID eines AWS verwalteten Kundenhauptschlüssels (CMK) für Amazon SNS oder eines benutzerdefinierten CMK, der für die serverseitige Verschlüsselung (SSE) verwendet werden soll. Die Standardeinstellung ist auf eingestellt. `alias/aws/sns` Wenn ein benutzerdefinierter AWS KMS Schlüssel verwendet wird, muss er mit den richtigen Berechtigungen konfiguriert werden. Weitere Informationen finden Sie unter Serverseitige Verschlüsselung (SSE) für ein Amazon SNS SNS-Thema aktivieren
Hs4Ma3G158 — SSM-Dokumente sollten nicht öffentlich sein Entsprechender AWS Security Hub CSPM Scheck: SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing- Deaktiviert das öffentliche Teilen von SSM-Dokumenten.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Hs4Ma3G136 — Amazon SQS SQS-Warteschlangen sollten im Ruhezustand verschlüsselt werden Entsprechender AWS Security Hub CSPM Scheck: SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Nachrichten in Amazon SQS sind verschlüsselt.	• SqsManagedSseEnabled: Auf aktiviert, `true` um serverseitige Warteschlangenverschlüsselung mit Amazon SQS SQS-eigenen Verschlüsselungsschlüsseln zu aktivieren, eingestellt auf, `false` um serverseitige Warteschlangenverschlüsselung mit einem Schlüssel zu aktivieren. AWS KMS • KMSKeyID: Die ID oder der Alias eines AWS verwalteten Kundenhauptschlüssels (CMK) für Amazon SQS oder eines benutzerdefinierten CMK, der für die serverseitige Verschlüsselung der Warteschlange verwendet werden soll. Wird verwendet, falls nicht angegeben. alias/aws/sqs • KmsDataKeyReusePeriodSeconds: Die Zeitspanne in Sekunden, für die Amazon SQS einen Datenschlüssel wiederverwenden kann, um Nachrichten zu verschlüsseln oder zu entschlüsseln, bevor er erneut anruft. AWS KMS Eine Ganzzahl stellt Sekunden dar, und zwar zwischen 60 Sekunden (1 Minute) und 86 400 Sekunden (24 Stunden). Diese Einstellung wird ignoriert, wenn sie auf gesetzt `SqsManagedSseEnabled` ist. `true`

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Anonym SendMessage und ReceiveMessage Anfragen an die verschlüsselte Warteschlange werden abgelehnt. Alle Anfragen zu Warteschlangen mit aktiviertem SSE müssen HTTPS und Signature Version 4 verwenden.

Trusted Advisor von Trusted Remediator unterstützte Fehlertoleranzprüfungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz138 Amazon DynamoDB DynamoDB-Wiederherstellung Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Aktiviert die point-in-time Wiederherstellung für DynamoDB-Tabellen.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
R365s2qddf Amazon S3 Bucket-Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Die Amazon S3 S3-Bucket-Versionierung ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Diese Korrektur unterstützt nicht die Standardisierung AWS-Service erstellter S3-Buckets (zum Beispiel cf-templates-000000000000).

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
BueAdJ7nRP Amazon S3 Bucket-Protokollierung	AWSManagedServices-EnableBucketAccessLogging Die Amazon S3 S3-Bucket-Protokollierung ist aktiviert.	• TargetBucket: Der Name des S3-Buckets zum Speichern von Serverzugriffsprotokollen. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte. Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden , wählen Sie`SimplePrefix` . Um den partitionierten S3-Schlüssel für Protokollobjekte und das partitionierte Präfix zu verwenden EventTime , wählen Sie. `PartitionedPrefixEventTime` Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte Präfix zu verwenden, wählen Sie. `PartitionedPrefixDeliveryTime` Der Standardwert ist `PartitionedPrefixEventTime` . Gültige Werte sind und (Groß `SimplePrefix` - `PartitionedPrefixEventTime` und Kleinschreibung beachten`PartitionedPrefixDeliveryTime`). Um die auto Korrektur zu aktivieren, müssen die folgenden vorkonfigurierten Parameter angegeben werden:

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		• TargetBucket Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung.
F2ik5R6DEP Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ Die Bereitstellung in mehreren Verfügbarkeitszonen ist aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Während dieser Änderung kann es zu Leistungseinbußen kommen.
H7 IgTzj TYb Amazon-EBS-Snapshots	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot Amazon EBSsnapshots wurden gegründet.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
op QPADk ZvH RDS-Backups	AWSManagedServices-EnableRDSBackupRetention Die Aufbewahrung von Amazon RDS-Backups ist für die Datenbank aktiviert.	• BackupRetentionPeriod: Die Anzahl der Tage (1—35) für die Aufbewahrung automatisierter Backups. • ApplyImmediately: Gibt an, ob die Änderung der Aufbewahrung von RDS-Backups und alle ausstehenden Änderungen so schnell wie möglich asynchron angewendet werden. Wählen Sie `true`, ob die Änderung sofort angewendet werden `false` soll, oder ob Sie die Änderung für das nächste Wartungsfenster planen möchten. Wenn der `ApplyImmediately` Parameter auf gesetzt ist `true`, werden die ausstehenden Änderungen in der Datenbank zusammen mit der RDSBackup Aufbewahrungseinstellung übernommen.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1qf5bt013 Bei Amazon RDS-DB-Instances ist die automatische Speicherskalierung deaktiviert	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling- Die automatische Speicherskalierung ist für die Amazon RDS-DB-Instance aktiviert.	• MaxAllocatedStorageIncrease Percentage: Der prozentuale Anstieg des Stroms Allocated Storage, der MaxAllocatedStorage eingestellt werden soll. Die Standardeinstellung ist auf eingestellt26. Sie müssen den maximalen Speicherschwellenwert auf mindestens 10% über dem aktuell zugewiesenen Speicherplatz festlegen. Es hat sich bewährt, den maximalen Speicherschwellenwert auf mindestens 26% zu erhöhen. Einzelheiten finden Sie unter Automatisches Kapazitätsmanagement mit Amazon Relational Database Service Storage Autoscaling. Keine Einschränkungen
7q GXs KlUw Classic Load Balancer Balancer-Verbindungsabbau	AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining Das Entleeren von Verbindungen ist für Classic Load Balancer aktiviert.	ConnectionDrainingTimeout: Die maximale Zeit in Sekunden, um die bestehenden Verbindungen offen zu halten, bevor die Instances deregistriert werden. Die Standardeinstellung ist auf Sekunden festgelegt. 300 Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz106 Amazon EBS nicht im AWS Backup Plan enthalten	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS ist im AWS Backup Plan enthalten.	Bei der Problembehebung wird das Amazon EBS-Volume mit dem folgenden Tag-Paar versehen. Das Tag-Paar muss den tagbasierten Ressourcenauswahlkriterien für entsprechen. AWS Backup • TagKey • TagValue Keine Einschränkungen
c18d2gz107 Amazon DynamoDB-Tabelle nicht im Plan enthalten AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan Amazon DynamoDB Table ist im AWS Backup Plan enthalten.	Remediation kennzeichnet Amazon DynamoDB mit dem folgenden Tag-Paar. Das Tag-Paar muss den tagbasierten Ressourcenauswahlkriterien für entsprechen. AWS Backup • TagKey • TagValue Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz117 Amazon EFS nicht im AWS Backup Plan enthalten	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS ist im AWS Backup Plan enthalten.	Bei der Problembehebung wird Amazon EFS mit dem folgenden Tag-Paar versehen. Das Tag-Paar muss den tagbasierten Ressource nauswahlkriterien für entsprechen. AWS Backup • TagKey • TagValue Keine Einschränkungen
c18d2gz105 Network Load Balancer – Zonenüber greifender Lastausgleich	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Zonenübergreifendes Load Balancing ist auf dem Network Load Balancer aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt026 Der Amazon `synchronous_commit` RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `synchronous_commit` ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1qf5bt030 Der Amazon `innodb_flush_log_at_trx_commit` RDS-Parameter ist nicht 1	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `innodb_flush_log_at_trx_commit` ist 1 für Amazon RDS auf eingestellt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt031 Der Amazon `sync_binlog` RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `sync_binlog` ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt036 Die Amazon `innodb_default_row_format` RDS-Parametereinstellung ist unsicher	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `innodb_default_row_format` ist `DYNAMIC` für Amazon RDS auf eingestellt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c18d2gz144 EC2 Detaillierte Amazon-Überwachung nicht aktiviert	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Die detaillierte Überwachung ist für Amazon aktiviert EC2.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor Leistungsprüfungen werden von Trusted Remediator unterstützt

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
COr6dfpM06 AWS Lambda Funktionen sind im Hinblick auf die Speicherg röße nicht ausreichend bereitgestellt	AWSManagedServices-ResizeLa mbdaMemory Die Speichergröße der Lambda-Funktionen wird auf die empfohlen e Speichergröße von angepasst. Trusted Advisor	RecommendedMemorySize: Die empfohlene Speicherzuweisung für die Lambda-Funktion. Der Wertebere ich liegt zwischen 128 und 10240. Wenn die Größe der Lambda-Funktion vor der Ausführung der Automatisierung geändert wird, überschreibt diese Automatisierung möglicherweise die Einstellungen mit dem von empfohlenen Wert. Trusted Advisor
ZRxQlPsb6c EC2 Amazon-Instances mit hoher Auslastun g	AWSManagedServices-ResizeIn stanceByOneLevel Die Größe von EC2 Amazon-In stances wird um einen Instance-Typ höher im selben Instance-Familientyp geändert. Die Instances werden während der Größenänd erung gestoppt und gestartet und nach Abschluss der Ausführung wieder in den Ausgangszustand versetzt. Diese Automatisierung unterstützt keine Größenänderung von Instances, die sich in einer Auto Scaling Scaling-Gruppe befinden.	• MinimumDaysSinceLastChange: Die Mindestanzahl von Tagen seit der letzten Änderung des Instance-Typs. Wenn der Instanzty p innerhalb der angegebenen Zeit geändert wurde, wird der Instanzty p nicht geändert. Verwenden Sie0, um diese Überprüfung zu übersprin gen. Der Standardwert ist 7. • AMIBeforeGröße ändern: Um das Instanz-AMI vor der Größenänd erung als Backup zu erstellen, wählen Sie`true`. Um kein Backup zu erstellen, wählen Sie`false`. Der Standardwert ist `false`. Gültige Werte sind `true` und `false` (Groß- und Kleinschreibung beachten).

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		• ResizeIfStopped: Um mit der Änderung der Instanzgröße fortzufahren, auch wenn sich die Instance im gestoppten Zustand befindet, wählen Sie`true`. Um die Größe der Instanz nicht automatisch zu ändern, wenn sie gestoppt ist, wählen Sie`false`. Gültige Werte sind `true` und `false` (Groß- und Kleinschreibung beachten). Keine Einschränkungen
c1qf5bt021 Amazon `innodb_change_buffering` RDS-Parameter, der weniger als den optimalen Wert verwendet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Wert des `innodb_change_buffering` Parameters ist `NONE` für Amazon RDS auf festgelegt.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt025 Der Amazon `autovacuum` RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `autovacuum` ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1qf5bt028 Der Amazon `enable_indexonlyscan` RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `enable_indexonlyscan` ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt029 Der Amazon `enable_indexscan` RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `enable_indexscan` ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt032 Der Amazon `innodb_stats_persistent` RDS-Parameter ist ausgeschaltet	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `innodb_stats_persistent` ist für Amazon RDS aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen
c1qf5bt037 Der Amazon `general_logging` RDS-Parameter ist aktiviert	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Der Parameter `general_logging` ist für Amazon RDS ausgeschaltet.	Vorkonfigurierte Parameter sind nicht zulässig. Keine Einschränkungen

Trusted Advisor Von Trusted Remediator unterstützte Prüfungen von Service-Limits

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Ln7RR0L7J9 EC2VPC Elastic IP-Adresse	AWSManagedServices-UpdateVpcElasticIPQuota Ein neues Limit für EC2 elastische IP-Adressen von VPC wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
kM7QQ0L7J9 VPC-Internet-Gateways	AWSManagedServices-IncreaseServiceQuota- Ein neues Limit für VPC-Internet-Gateways wird angefordert. Standardmäßig wird das Limit um drei erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
JL7PP0L7J9 VPC	AWSManagedServices-IncreaseServiceQuota Ein neues Limit für VPC wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
FW7HH0L7J9 Auto Scaling-Gruppen	AWSManagedServices-IncreaseServiceQuota Ein neues Limit für Auto Scaling Scaling-Gruppen wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
3Njm0 DJQO9 RDS-Optionsgruppen	AWSManagedServices-IncreaseServiceQuota Ein neues Limit für Amazon RDS-Optionsgruppen wird beantragt. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.
EM8b3yLRTr ELB Application Load Balancers	AWSManagedServices-IncreaseServiceQuota Ein neues Limit für ELB Application Load Balancers wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem OK Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
8 WiQ K YSt25 ELB Network Load Balancers	AWSManagedServices-IncreaseServiceQuota Ein neues Limit für ELB Network Load Balancers wird angefordert. Standardmäßig wird das Limit um 3 erhöht.	Inkrement: Die Zahl, um die aktuelle Quote zu erhöhen. Der Standardwert ist 3. Wenn diese Automatisierung mehrmals ausgeführt wird, bevor die Trusted Advisor Prüfung mit dem 0K Status aktualisiert wird, kann es zu einer höheren Limiterhöhung kommen.

Trusted Advisor Prüfungen der betrieblichen Exzellenz werden von Trusted Remediator unterstützt

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c18d2gz125 Amazon API Gateway protokolliert keine Ausführungsprotokolle	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging Die Ausführungsprotokollierung ist auf der API-Phase aktiviert.	Vorkonfigurierte Parameter sind nicht zulässig. Sie müssen API Gateway die Berechtigung zum Lesen und Schreiben von Protokollen CloudWatch für Ihr Konto erteilen, um das Ausführungsprotokoll zu aktivieren. Weitere Informationen finden Sie unter CloudWatch Protokollierung für REST APIs in API Gateway einrichten.
c18d2gz168	AWSManagedServices-TrustedRemediatorEnableELBDeletionP	Vorkonfigurierte Parameter sind nicht zulässig.

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
Elastic-Load-Balancing-Löschschutz ist für Load Balancer nicht aktiviert	rotection- Der Löschschutz ist für den Elastic Load Balancer aktiviert.	Keine Einschränkungen
c1qf5bt012 Amazon RDS Performance Insights ist ausgeschaltet	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights Performance Insights ist für Amazon RDS aktiviert.	• PerformanceInsightsRetentionPeriod: Die Anzahl der Tage, für die Performance Insights Insights-Daten aufbewahrt werden sollen. Gültige Werte: 7 oder Monat * 31, wobei Monat eine Anzahl von Monaten zwischen 1 und 23 ist. Beispiele: 93 (3 Monate* 31), 341 (11 Monate* 31), 589 (19 Monate* 31) oder731. • PerformanceInsightsKMSKeyID: Die AWS KMS Schlüssel-ID für die Verschlüsselung von Performance Insights Insights-Daten. Wenn Sie keinen Wert für PerformanceInsights KMSKey Id angeben, verwendet Amazon RDS Ihren AWS KMS Standardschlüssel. Keine Einschränkungen

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
c1fd6b96l4 Amazon S3 S3-Zugriffsprotokolle aktiviert	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 Die Protokollierung des Amazon S3 S3-Bucket-Zugriffs ist aktiviert.	• TargetBucketTagValue: Der Tag-Wert (Groß- und Kleinschreibung beachten) zur Identifizierung des Ziel-Buckets. Verwenden Sie ihn und TargetBucketTagKey markieren Sie den Bucket, der als Ziel-Bucket für die Zugriffsprotokollierung verwendet werden soll. • TargetObjectKeyFormat: Amazon S3 S3-Schlüsselformat für Protokollobjekte (bei Werten wird Groß- und Kleinschreibung beachtet). Um das einfache Format für S3-Schlüssel für Protokollobjekte zu verwenden, wählen Sie`SimplePrefix` . Um den partitionierten S3-Schlüssel für Protokollobjekte und EventTime für das partitionierte Präfix zu verwenden, wählen Sie. `PartitionedPrefixEventTime` Um den partitionierten S3-Schlüssel für Protokollobjekte und DeliveryTime für das partitionierte Präfix zu verwenden, wählen Sie. `PartitionedPrefixDeliveryTime` Gültige Werte sind `SimplePrefix` , `PartitionedPrefixEventTime` und `PartitionedPrefixDeliveryTime` .

Überprüfen Sie die ID und den Namen	Name des SSM-Dokuments und erwartetes Ergebnis	Unterstützte vorkonfigurierte Parameter und Einschränkungen
		Um die auto Korrektur zu aktivieren, muss der folgende vorkonfigurierte Parameter angegeben werden: TargetBucketTagKeyund. TargetBucketTagValue Der Ziel-Bucket muss sich im selben AWS-Region und AWS-Konto wie der Quell-Bucket befinden und über die richtigen Berechtigungen für die Protokollzustellung verfügen. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung.

Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator

Konfigurationen werden AWS AppConfig als Teil der Trusted Remediator-Anwendung gespeichert. Jede Trusted Advisor Prüfkategorie hat ein eigenes Konfigurationsprofil. Weitere Informationen zu Trusted Advisor Kategorien finden Sie unter Prüfkategorien anzeigen.

Sie können Behebungen pro Ressource oder pro Trusted Advisor Prüfung konfigurieren. Sie können Ausnahmen mithilfe von Ressourcen-Tags anwenden.

> **Note**
>
> Die Behebung von Trusted Advisor Ergebnissen ist derzeit mit konfiguriert AWS AppConfig, und diese Funktion wird heute vollständig unterstützt. AMS geht davon aus, dass sich dies in future ändern wird. Es ist eine bewährte Methode, Gebäudeautomationen zu vermeiden, die darauf angewiesen sind AWS AppConfig, da sich diese Methode ändern kann. Beachten Sie, dass Sie aus Kompatibilitätsgründen möglicherweise in future Automatisierungen

aktualisieren oder ändern müssen, die auf der aktuellen AWS AppConfig Implementierung basieren.
Das Feature-Flag Compute Optimizer -> EC2 Instances hat zusätzliche Parameter:

- allow-upscale Um das Hochskalieren von nicht optimierten Instances mit unzureichender Bereitstellung zu ermöglichen. EC2 Der Standardwert ist „false“.
- min-savings-opportunity-percentageDie Möglichkeit der automatischen Problembehebung in Prozent mit minimalen Einsparungen. Der Standardwert ist 10%

Standardkonfigurationen für die Problembehebung

Die Konfigurationen für einzelne Trusted Advisor Prüfungen werden als AWS AppConfig Flags gespeichert. Der Flag-Name stimmt mit dem Schecknamen überein. Jede Prüfkonfiguration enthält die folgenden Attribute:

- Ausführungsmodus: Legt fest, wie Trusted Remediator die Standardbehebung durchführt:
  - Automatisiert: Trusted Remediator korrigiert Ressourcen automatisch, indem es ein Dokument erstellt OpsItem, das SSM-Dokument ausführt und es nach erfolgreicher Ausführung wieder auflöst. OpsItem
  - Manuell: Ein OpsItem wird erstellt, aber das SSM-Dokument wird nicht automatisch ausgeführt. Sie überprüfen das SSM-Dokument OpsItem in der Konsole und führen es manuell aus. AWS Systems Manager OpsCenter
  - Bedingt: Die Wiederherstellung ist standardmäßig deaktiviert. Sie können es mithilfe von Tags für bestimmte Ressourcen aktivieren. Weitere Informationen finden Sie in den folgenden Abschnitten Passen Sie die Problembehebung mit Ressourcen-Tags individuell an undPassen Sie die Problembehebung mit Tags zum Überschreiben von Ressourcen individuell an.
  - Inaktiv: Es findet keine Korrektur statt und es OpsItem werden keine erstellt. Sie können den Ausführungsmodus für die Trusted Advisor Prüfung, die auf inaktiv gesetzt ist, nicht überschreiben.
- vorkonfigurierte Parameter: Geben Sie Werte für SSM-Dokumentparameter ein, die für die automatische Korrektur erforderlich sind, im Format von, getrennt durch ein Komma (`Parameter=Value`,). Informationen zu Trusted Advisor von Trusted Remediator unterstützte Prüfungen den unterstützten vorkonfigurierten Parametern für das zugehörige SSM-Dokument finden Sie für jede Prüfung.

- alternative-automation-document: Dieses Attribut hilft dabei, das vorhandene Automatisierungsdokument durch ein anderes unterstütztes Dokument zu überschreiben (falls für die jeweilige Prüfung verfügbar). Dieses Attribut ist standardmäßig nicht ausgewählt.

> **Note**
>
> Das `alternative-automation-document` Attribut unterstützt keine benutzerdefinierten Automatisierungsdokumente. Sie können die vorhandenen unterstützten Trusted Remediator-Automatisierungsdokumente verwenden, die unter aufgeführt sind. Trusted Advisor von Trusted Remediator unterstützte Prüfungen Zur Überprüfung gibt es `Qch7DwouX1` beispielsweise drei zugehörige SSM-Dokumente: AWSManagedServices-StopEC 2Instance, und AWSManagedServices-ResizeInstanceByOneLevel. AWSManagedServices-TerminateInstance Der Wert für `alternative-automation-document` kann entweder AWSManagedServices-ResizeInstanceByOneLevel oder sein AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance ist das SSM-Standarddokument, das behoben werden muss). `Qch7DwouX1`

Der Wert für jedes Attribut muss den Einschränkungen dieses Attributs entsprechen.

> **Tip**
>
> Bevor Sie die Standardkonfigurationen für Ihre Trusted Advisor Prüfungen anwenden, empfiehlt es sich, die in den folgenden Abschnitten beschriebenen Funktionen zur Kennzeichnung von Ressourcen und zur Außerkraftsetzung von Ressourcen in Betracht zu ziehen. Die Standardkonfigurationen gelten für alle Ressourcen innerhalb des Kontos, was möglicherweise nicht in allen Fällen wünschenswert ist.

Im Folgenden finden Sie ein Beispiel für einen Konsolen-Screenshot, bei dem der Ausführungsmodus auf Manuell gesetzt ist und die Attribute den jeweiligen Einschränkungen entsprechen.

Passen Sie die Problembehebung mit Ressourcen-Tags individuell an

Mit den manual-for-tagged-onlyAttributen automated-for-tagged-onlyund in der Prüfkonfiguration können Sie Ressourcen-Tags angeben, mit denen Sie festlegen können, wie Sie einzelne Prüfungen korrigieren möchten. Es hat sich bewährt, diese Methode zu verwenden, wenn Sie ein einheitliches Behebungsverhalten auf eine Gruppe von Ressourcen anwenden müssen, die dasselbe Tag oder dieselben Tags verwenden. Im Folgenden finden Sie Beschreibungen für diese Tags:

- automated-for-tagged-only: Geben Sie Ressourcen-Tags (ein oder mehrere Tag-Paare, durch Kommas getrennt) für Prüfungen an, die unabhängig vom Standardausführungsmodus automatisch behoben werden sollen.
- manual-for-tagged-only: Geben Sie Ressourcen-Tags (ein oder mehrere Tag-Paare, durch Kommas getrennt) für Problembehebungen an, die unabhängig vom Standardausführungsmodus manuell ausgeführt werden sollen.

Wenn Sie beispielsweise die automatische Behebung für alle Ressourcen aktivieren möchten, die nicht zur Produktion gehören, und die manuelle Korrektur für Produktionsressourcen erzwingen möchten, können Sie Ihre Konfiguration wie folgt festlegen:

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

Nachdem Sie die vorherigen Konfigurationen für Ihre Ressourcen eingerichtet haben, überprüfen Sie, ob das Behebungsverhalten wie folgt aussieht:

- Ressourcen, die mit 'Environment=Non-Production' gekennzeichnet sind, werden automatisch behoben.
- Ressourcen, die mit 'Environment=Production' gekennzeichnet sind, erfordern zur Behebung manuelles Eingreifen.
- Ressourcen ohne das Tag 'Environment' folgen dem Standard-Ausführungsmodus (in diesem Fall `Bedingt`). Es werden also keine Maßnahmen für die verbleibenden Ressourcen ergriffen).

Wenn Sie weitere Unterstützung bei Ihren Konfigurationen benötigen, wenden Sie sich an Ihren Cloud-Architekten.

Passen Sie die Problembehebung mit Tags zum Überschreiben von Ressourcen individuell an

Mithilfe von Tags zum Überschreiben von Ressourcen können Sie das Behebungsverhalten für einzelne Ressourcen unabhängig von ihren Tags anpassen. Indem Sie einer Ressource ein bestimmtes Tag hinzufügen, überschreiben Sie den Standardausführungsmodus für diese Ressource und die Trusted Advisor Prüfung. Das Resource-Override-Tag hat Vorrang vor der Standardkonfiguration und den Einstellungen für das Ressourcen-Tagging. Wenn Sie also für eine Ressource, die das Resource Override-Tag verwendet, den Standardausführungsmodus auf Automatisiert, Manuell oder Bedingt festlegen, überschreibt dies den Standardausführungsmodus und alle Konfigurationen für das Ressourcen-Tagging.

Gehen Sie wie folgt vor, um den Ausführungsmodus für eine Ressource zu überschreiben:

1. Identifizieren Sie die Ressourcen, für die Sie die Behebungskonfiguration überschreiben möchten.
2. Ermitteln Trusted Advisor Sie die Scheck-ID für den Scheck, den Sie überschreiben möchten. Den Scheck IDs für unterstützte Trusted Advisor Check-ins finden Sie unterTrusted Advisor von Trusted Remediator unterstützte Prüfungen.
3. Fügen Sie den Ressourcen ein Tag mit dem folgenden Schlüssel und Wert hinzu:

   - Tag-Schlüssel: `TR-`*`Trusted Advisor check ID`*`-Execution-Mode` (Groß- und Kleinschreibung beachten)

     Ersetzen Sie es im vorherigen Beispiel `Trusted Advisor check ID` mit einem Tag-Schlüssel durch den eindeutigen Bezeichner des Trusted Advisor Schecks, den Sie überschreiben möchten.

   - Tag-Wert: Verwenden Sie einen der folgenden Werte für den Tag-Wert:
     - Automatisiert: Trusted Remediator korrigiert automatisch die Ressource für diese Trusted Advisor Prüfung.
     - Manuell: Für die Ressource OpsItem wird eine erstellt, aber die Korrektur wird nicht automatisch durchgeführt. Sie überprüfen und führen die Problembehebung manuell über den aus. OpsItem
     - Inaktiv: Für diese Ressource und die angegebene Trusted Advisor Prüfung wurden keine Korrektur und OpsItem Erstellung durchgeführt.

Um beispielsweise ein Amazon EBS-Volume mit der Trusted Advisor Scheck-ID automatisch zu korrigieren, `DAvU99Dc4C` fügen Sie dem EBS-Volume ein Tag hinzu. Der Tag-Schlüssel ist `TR-DAvU99Dc4C-Execution-Mode` und der Tag-Wert ist. `Automated`

Im Folgenden finden Sie ein Beispiel für die Konsole, in der der Abschnitt „Tags“ angezeigt wird:

Entscheidungsworkflow für den Ausführungsmodus

Es gibt mehrere Ebenen, um den Ausführungsmodus für Ihre Ressourcen und jede Trusted Advisor Prüfung zu konfigurieren. Das folgende Diagramm zeigt, wie Trusted Remediator anhand Ihrer Konfigurationen entscheidet, welcher Ausführungsmodus verwendet werden soll:

Tutorials zur Konfiguration von Problembehebungen

Die folgenden Tutorials enthalten Beispiele für die Erstellung gängiger Problembehebungen in Trusted Remediator

Korrigieren Sie alle Ressourcen manuell

In diesem Beispiel wird die manuelle Korrektur für alle Amazon EBS-Volumes mit der Trusted Advisor Scheck-ID DAv U99Dc4C (Underused Amazon EBS Volumes) konfiguriert.

Konfigurieren Sie die manuelle Korrektur für Amazon EBS-Volumes mit der Prüf-ID U99Dc4C DAv

1. Öffnen Sie die Konsole unter appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Stellen Sie sicher, dass Sie sich mit dem delegierten Administratorkonto anmelden.
2. Wählen Sie Trusted Remediator aus der Liste der Anwendungen aus.
3. Wählen Sie das Konfigurationsprofil „Kostenoptimierung“ aus.
4. Wählen Sie das Kennzeichen Nicht ausgelastete Amazon EBS-Volumes aus.
5. Wählen Sie für den Ausführungsmodus Manuell aus.
6. Stellen Sie sicher, dass die manual-for-tagged-onlyAttribute automated-for-tagged-onlyund leer sind. Diese Attribute werden verwendet, um den Standard-Ausführungsmodus für Ressourcen mit passenden Tags zu überschreiben.

Im Folgenden finden Sie ein Beispiel für den Abschnitt Attribute mit leeren Werten für automated-for-tagged-onlyund manual-for-tagged-onlyund Manual für den Ausführungsmodus:

7. Wählen Sie Speichern, um den Wert zu aktualisieren, und wählen Sie dann Neue Version speichern, um die Änderungen zu übernehmen. Sie müssen Neue Version speichern auswählen, damit Trusted Remediator die Änderung erkennt.
8. Stellen Sie sicher, dass Ihre Amazon EBS-Volumes kein Tag mit dem Schlüssel `TR-DAvU99Dc4C-Execution-Mode` haben. Dieser Tag-Schlüssel überschreibt den Standard-Ausführungsmodus für dieses EBS-Volume.

Korrigieren Sie alle Ressourcen automatisch, mit Ausnahme der ausgewählten Ressourcen

In diesem Beispiel wird die automatische Problembehebung für alle Amazon EBS-Volumes mit der Trusted Advisor Scheck-ID DAv U99Dc4C (Nicht ausgelastete Amazon EBS-Volumes) konfiguriert, mit Ausnahme der angegebenen Volumes, die nicht behoben werden (als Inaktiv gekennzeichnet).

Automatische Problembehebung für Amazon EBS-Volumes mit der Prüf-ID DAv U99Dc4C konfigurieren, mit Ausnahme ausgewählter inaktiver Ressourcen

1. Öffnen Sie die Konsole unter appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Stellen Sie sicher, dass Sie sich mit dem delegierten Administratorkonto anmelden.
2. Wählen Sie Trusted Remediator aus der Liste der Anwendungen aus.
3. Wählen Sie das Konfigurationsprofil „Kostenoptimierung“ aus.
4. Wählen Sie das Kennzeichen Nicht ausgelastete Amazon EBS-Volumes aus.
5. Wählen Sie für den Ausführungsmodus Automatisiert aus.
6. Stellen Sie sicher, dass die manual-for-tagged-onlyAttribute automated-for-tagged-onlyund leer sind. Diese Attribute werden verwendet, um den Standard-Ausführungsmodus für Ressourcen mit passenden Tags zu überschreiben.

   Im Folgenden finden Sie ein Beispiel für den Abschnitt Attribute mit leeren Werten für automated-for-tagged-onlyund manual-for-tagged-onlyund Automatisiert für den Ausführungsmodus:

7. Wählen Sie Speichern, um den Wert zu aktualisieren, und wählen Sie dann Neue Version speichern, um die Änderungen zu übernehmen. Sie müssen Neue Version speichern auswählen, damit Trusted Remediator die Änderung erkennt.

   Zu diesem Zeitpunkt sind alle Amazon EBS-Volumes auf automatische Problembehebung eingestellt.

8. Automatische Problembehebung für ausgewählte Amazon EBS-Volumes außer Kraft setzen:

   a. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

   b. Wählen Sie Elastic Block Store, Volumes.

   c. Wählen Sie Tags aus.

   d. Wählen Sie Tags verwalten aus.

   e. Fügen Sie das folgende Tag hinzu:

      - Schlüssel: TR- DAv U99Dc4C-Ausführungsmodus
      - Wert: Inaktiv

      Im Folgenden finden Sie ein Beispiel für den Abschnitt „Tags“, in dem die Felder Schlüssel und Wert angezeigt werden:

   f. Wiederholen Sie die Schritte 2 bis 5 für alle Amazon EBS-Volumes, die Sie von der Problembehebung ausschließen möchten.

Korrigieren Sie markierte Ressourcen automatisch

In diesem Beispiel wird die automatische Problembehebung für alle Amazon EBS-Volumes mit dem Tag `Stage=NonProd` mit der Trusted Advisor Prüf-ID DAv U99Dc4C (Underused Amazon EBS Volumes) konfiguriert. Alle anderen Ressourcen ohne dieses Tag werden nicht behoben.

Automatische Problembehebung für Amazon EBS-Volumes mit dem Tag **`Stage=NonProd`** für die Scheck-ID U99Dc4C konfigurieren DAv

1. Öffnen Sie die Konsole unter appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Stellen Sie sicher, dass Sie sich mit dem delegierten Administratorkonto anmelden.

2. Wählen Sie Trusted Remediator aus der Liste der Anwendungen aus.
3. Wählen Sie das Konfigurationsprofil „Kostenoptimierung“ aus.
4. Wählen Sie das Kennzeichen Nicht ausgelastete Amazon EBS-Volumes aus.
5. Wählen Sie für den Ausführungsmodus die Option Conditional aus.
6. Legen Sie den Wert für automated-for-tagged-only auf `Stage=NonProd` fest. Dieses Attribut setzt den Standard `execution-mode` für Ressourcen mit passenden Tags außer Kraft. Stellen Sie sicher, dass die manual-for-tagged-onlyAttribute leer sind.

   Im Folgenden finden Sie ein Beispiel für den Abschnitt Attributes, der für den automated-for-tagged-onlyAusführungsmodus auf Stage= NonProd und Conditional gesetzt ist:

7. Legen Sie optional die vorkonfigurierten Parameter auf einen der folgenden Werte fest:

   - `CreateSnapshot=false`um keinen Snapshot des Amazon EBS-Volumes zu erstellen, bevor es gelöscht wurde
   - `MinimumUnattachedDays=10`um die Mindestdauer des zu löschenden Amazon EBS-Volumes ohne Anhängen auf 10 Tage festzulegen
   - `CreateSnapshot=false`, `MinimumUnattachedDays=10` für beide der oben genannten
8. Wählen Sie Speichern, um den Wert zu aktualisieren, und wählen Sie dann Neue Version speichern, um die Änderungen zu übernehmen. Sie müssen Neue Version speichern auswählen, damit Trusted Remediator die Änderung erkennt.
9. Stellen Sie sicher, dass Ihre Amazon EBS-Volumes kein Tag mit dem Schlüssel `TR-DAvU99Dc4C-Execution-Mode` haben. Dieser Tag-Schlüssel überschreibt den Standard-Ausführungsmodus für dieses EBS-Volume.

Arbeiten Sie mit Behebungen in Trusted Remediator

Behebungen in Trusted Remediator nachverfolgen

Gehen Sie wie folgt vor, um OpsItems Behebungen nachzuverfolgen:

1. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/
2. Wählen Sie Operations Management, OpsCenter.

3. (Optional) Filtern Sie die Liste nach Quelle=Trusted Remediator, um nur Trusted Remediator OpsItems in die Liste aufzunehmen.

   Im Folgenden finden Sie ein Beispiel für den OpsCenter Bildschirm, der nach Source=Trusted Remediator gefiltert wurde:

> **Note**
>
> Zusätzlich zur Anzeige OpsItems von können Sie die OpsCenter Behebungsprotokolle im AMS S3-Bucket einsehen. Weitere Informationen finden Sie unter Behebungsprotokolle in Trusted Remediator.

Führen Sie manuelle Korrekturen in Trusted Remediator aus

Trusted Remediator erstellt vier Prüfungen, OpsItems die für die manuelle Behebung konfiguriert sind. Sie müssen diese Prüfungen überprüfen und den Behebungsprozess manuell starten.

Gehen Sie wie folgt vor OpsItem, um das manuell zu korrigieren:

1. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/
2. Wählen Sie Operations Management, OpsCenter.
3. (Optional) Filtern Sie die Liste nach Quelle=Trusted Remediator, um nur Trusted Remediator OpsItems in die Liste aufzunehmen.
4. Wählen Sie die aus OpsItem , die Sie überprüfen möchten.
5. Überprüfen Sie die Betriebsdaten von OpsItem. Die Betriebsdaten umfassen die folgenden Elemente:

   - trustedAdvisorCheckKategorie: Die Kategorie der Trusted Advisor Scheck-ID. Zum Beispiel Fehlertoleranz
   - trustedAdvisorCheckID: Die eindeutige Trusted Advisor Scheck-ID.
   - trustedAdvisorCheckMetadaten: Die Metadaten der Ressource, einschließlich der Ressourcen-ID.
   - trustedAdvisorCheckName: Der Name des Trusted Advisor Schecks.

- trustedAdvisorCheckStatus: Der Status der Trusted Advisor Prüfung, die für die Ressource erkannt wurde.

6. Gehen Sie wie folgt vor OpsItem, um das Problem manuell zu beheben:

   a. Wählen Sie unter Runbooks eines der zugehörigen Runbooks (SSM-Dokumente) aus.

   b. Wählen Sie Ausführen.

   c. Wählen Sie für AutomationAssumeRole `arn:aws:iam::AWS-Konto ID:role/ams_ssm_automation_role` aus. Ersetzen Sie AWS-Konto ID durch die Konto-ID, unter der die Korrektur ausgeführt wird. Weitere Parameterwerte finden Sie in den Betriebsdaten.

      Um Ressourcen manuell zu korrigieren, AWS-Konto muss die Rolle oder der Benutzer, mit dem bzw. der sich authentifiziert hat, über die `iam:PassRole` Berechtigungen für die IAM-Rolle verfügen. `ams-ssm-automation-role` Weitere Informationen finden Sie unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen Benutzer AWS-Service oder wenden Sie sich an Ihren Cloud-Architekten.

   d. Wählen Sie Ausführen.

   e. Überwachen Sie den Fortschritt der Ausführung des SSM-Dokuments in der Spalte Aktueller Status und Ergebnisse.

   f. Wählen Sie nach Abschluss des Dokuments „Status festlegen“, „Gelöst“, um das OpsItem manuell zu lösen. Wenn das Dokument fehlgeschlagen ist, überprüfen Sie die Details und führen Sie das SSMdocument erneut aus. Wenn Sie zusätzliche Unterstützung bei der Fehlerbehebung benötigen, erstellen Sie eine Serviceanfrage.

   Um ein Problem zu lösen, OpsItem das nicht behoben wurde, wählen Sie „Status auf Gelöst setzen“.

7. Wiederholen Sie die Schritte 3 und 4 für alle verbleibenden manuellen OpsItems Problembehebungen.

Beheben Sie Fehler bei Behebungen in Trusted Remediator

Wenden Sie sich an AMS, wenn Sie Unterstützung bei manuellen Problembehebungen und Mängelbehebungsfehlern benötigen.

Gehen Sie wie folgt vor, um den Status und die Ergebnisse der Problembehebung einzusehen:

1. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/
2. Wählen Sie Operations Management, OpsCenter.
3. (Optional) Filtern Sie die Liste nach Quelle=Trusted Remediator, um nur Trusted Remediator OpsItems in die Liste aufzunehmen.
4. Wählen Sie die aus OpsItem , die Sie überprüfen möchten.
5. Überprüfen Sie im Abschnitt Automatisierungsausführungen den Namen und den Status des Dokuments sowie die Ergebnisse.
6. Sehen Sie sich die folgenden häufigen Automatisierungsfehler an. Wenn Ihre Probleme hier nicht aufgeführt sind, wenden Sie sich an Ihren CSDM, um Unterstützung zu erhalten.

Häufige Fehler bei der Problembehebung

Unter Automatisierungsausführungen sind keine Ausführungen aufgeführt

Keine Ausführungen im Zusammenhang mit dem deuten OpsItem möglicherweise darauf hin, dass die Ausführung aufgrund falscher Parameterwerte nicht gestartet werden konnte.

Fehlerbehebungsschritte

1. Überprüfen Sie in den Betriebsdaten den `trustedAdvisorCheckAutoRemediation` Eigenschaftswert.
2. Stellen Sie sicher, dass die Werte für DocumentNameund Parameter korrekt sind. Die richtigen Werte finden Sie in Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator den Einzelheiten zur Konfiguration der SSM-Parameter. Informationen zu den unterstützten Prüfungsparametern finden Sie unter Trusted Advisor von Trusted Remediator unterstützte Prüfungen
3. Stellen Sie sicher, dass die Werte im SSM-Dokument den zulässigen Mustern entsprechen. Um die Parameterdetails im Dokumentinhalt anzuzeigen, wählen Sie den Dokumentnamen im Abschnitt Runbooks aus.
4. Nachdem Sie die Parameter überprüft und korrigiert haben, führen Sie das SSM-Dokument erneut manuell aus.
5. Um zu verhindern, dass dieser Fehler erneut auftritt, stellen Sie sicher, dass Sie die Behebung mit den richtigen Parameterwerten in Ihrer Konfiguration konfigurieren. Weitere Informationen finden Sie unter Konfigurieren Sie Trusted Advisor die Problembehebung in Trusted Remediator.

Fehlgeschlagene Ausführungen bei Automatisierungsausführungen

Behebungsdokumente enthalten mehrere Schritte, die mit der AWS-Services Ausführung verschiedener Aktionen zusammenhängen. APIs Gehen Sie wie folgt vor, um eine bestimmte Ursache für den Fehler zu ermitteln:

Fehlerbehebungsschritte

1. Um die einzelnen Ausführungsschritte anzuzeigen, wählen Sie im Abschnitt Automatisierungsausführungen den Link Ausführungs-ID aus. Im Folgenden finden Sie ein Beispiel für die Systems Manager Manager-Konsole, in der die Ausführungsschritte für eine ausgewählte Automatisierung angezeigt werden:

2. Wählen Sie den Schritt mit dem Status Fehlgeschlagen aus. Im Folgenden finden Sie Beispiele für Fehlermeldungen:

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

     Dieser Fehler weist darauf hin, dass in den vorkonfigurierten Parametern der Wartungskonfiguration der falsche Bucket-Name angegeben wurde.

     Um diesen Fehler zu beheben, führen Sie die Automatisierung manuell mit dem richtigen Bucket-Namen aus. Um zu verhindern, dass dieses Problem erneut auftritt, aktualisieren Sie die Wartungskonfiguration mit dem richtigen Bucket-Namen.

   - `DB instance my-db-instance-1 is not in available status for modification.`

     Dieser Fehler weist darauf hin, dass die Automatisierung die erwarteten Änderungen nicht vornehmen konnte, da sich die DB-Instance in einem ungültigen Zustand befand.

     Um diesen Fehler zu beheben, führen Sie die Automatisierung manuell aus.

Behebungsprotokolle in Trusted Remediator

Trusted Remediator erstellt Protokolle im JSON-Format und lädt sie auf Amazon Simple Storage Service hoch. Die Protokolldateien werden in einen von AMS erstellten und benannten S3-Bucket hochgeladen. `ams-trusted-remediator-{your-account-id}-logs` AMS erstellt den S3-

Bucket im Delegated Administrator-Konto. Sie können die Protokolldateien importieren, QuickSight um benutzerdefinierte Behebungsberichte zu erstellen.

Weitere Informationen finden Sie unter Trusted Remediator-Integration mit QuickSight.

Protokoll der Behebungselemente

Trusted Remediator erstellt das`Remediation item log`, wenn eine Behebung OpsItem erstellt wird. Dieses Protokoll enthält manuelle und automatisierte OpsItem Problembehebungen. OpsItem Sie können den verwenden`Remediation item log`, um den Überblick über alle Behebungen nachzuverfolgen.

Speicherort des Korrekturelementprotokolls für Compute Optimizer Optimizer-Empfehlungen

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Speicherort für das Protokoll des Behebungselements für Prüfungen Trusted Advisor

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`- `*`Resource ID`*`.json`

URL der Beispieldatei für das Behebungselement

`s3:///ams-trusted-remediator-`*`111122223333`*`-logs/remediation_items/`*`2023-02-06`*`/`*`1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json`*

Protokollformat für Compute Optimizer Remediation-Elemente

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Protokollformat für das Behebungselement

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
   "RemediationTime": Remediation creation time,
   "ExecutionMode": Automated or Manual,
   "OpsItemID": OpsItem ID
}
```

Compute Optimizer Remediation-Artikelprotokollformat, Beispielinhalt

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor Protokollformat des Behebungselements, Beispielinhalt

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

Protokoll zur Ausführung automatisierter Problembehebungen, Compute Optimizer und Trusted Advisor

Trusted Remediator erstellt das`Automated remediation execution log`, wenn ein automatisierter SSM-Dokumentenlauf abgeschlossen ist. Dieses Protokoll enthält SSM-

Ausführungsdetails nur für die automatisierte Problembehebung. OpsItem Sie können diese Protokolldatei verwenden, um automatisierte Problembehebungen nachzuverfolgen.

Compute Optimizer — Speicherort des automatisierten Behebungsprotokolls

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer recommendation ID`*`.json`

Trusted Advisor Speicherort des automatisierten Behebungsprotokolls

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Compute Optimizer — Beispiel für den Speicherort eines automatisierten Behebungsprotokolls

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json`

Trusted Advisor Beispiel für den Speicherort des automatisierten Behebungsprotokolls

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json`

Format eines Beispielinhalts im Format eines automatisierten Behebungsprotokolls

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"}
```

Protokoll der Mitgliedskonten

Trusted Remediator erstelltMember accounts log, wann Ihr Konto an- oder ausgegliedert wird. Sie können den verwendenMember accounts log, um die Konto-ID, den Onboarding-Status und die Ausführungszeit jedes Mitgliedskontos zu AWS-Regionen ermitteln.

Speicherort der Protokolle der Mitgliedskonten

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/configuration_logs/member_accounts.json`

URL der Beispieldatei für das Protokoll der Mitgliedskonten

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/configuration_logs/member_accounts.json`

Protokollformat für Mitgliedskonten

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": AWS-Region name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

Beispielinhalt im Protokollformat für Mitgliedskonten

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
```

```
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```


Trusted Remediator-Integration mit QuickSight

Sie können die in Amazon S3 gespeicherten Trusted Remediator-Protokolle integrieren, QuickSight um einen individuellen Problembehebungsbericht zu erstellen. QuickSight Die Integration ist optional. Mit dieser Funktion können Sie die Protokolle verwenden, um benutzerdefinierte Berichts-Dashboards zu erstellen. Um auf Anfrage Berichte für Trusted Remediator zu erhalten, wenden Sie sich an Ihren CSDM. Weitere Informationen zu verfügbaren Trusted Remediator-Berichten finden Sie unter. Trusted Remediator-Berichte

Weitere Informationen zur Visualisierung von Daten in QuickSight finden Sie unter Visualisieren von Daten in. QuickSight

Fügen Sie einen Datensatz QuickSight für das Problembehebungsprotokoll hinzu

Gehen Sie wie folgt vor, um einen Datensatz QuickSight für das Remediation-Elementprotokoll hinzuzufügen:

1. Melden Sie sich bei der QuickSight Konsole an. Sie können den QuickSight Bericht in einer beliebigen Version erstellen AWS-Region , die dies QuickSight unterstützt. Um die Leistung zu verbessern und die Kosten zu senken, empfiehlt es sich jedoch, den Bericht in der Region zu erstellen, in der sich der Trusted Remediator-Logging-Bucket befindet.
2. Wählen Sie Datasets aus.
3. Wählen Sie S3.
4. Geben Sie in der Neuen S3-Datenquelle die folgenden Werte ein:
   - Name der Datenquelle: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`.
   - Laden Sie eine Manifestdatei hoch: Erstellen Sie eine JSON-Datei mit dem folgenden Inhalt und verwenden Sie sie. Wenn Sie die Datei erstellen, ersetzen Sie `logging_bucket_name` den URIPrefixes Schlüssel.

     ```
     {
         "fileLocations": [
             {
                 "URIPrefixes": [
                     "s3://{logging_bucket_name}/remediation_items/"
                 ]
             }
         ],
         "globalUploadSettings": {
             "format": "JSON",
             "delimiter": ",",
             "textqualifier": "'",
             "containsHeader": "true"
         }
     }
     ```

   - Wählen Sie Connect aus.
   - Wählen Sie im Fenster Datensatzerstellung beenden die Option Visualisieren aus.

- QuickSight öffnet die neue Seite mit dem Analyseblatt. Sie sind jetzt bereit, mithilfe des Problemprotokolls zur Problembehebung eine neue Analyse zu erstellen.

Im Folgenden finden Sie eine Beispielanalyse:

Fügen Sie einen Datensatz QuickSight für das Protokoll zur Ausführung der automatisierten Problembehebung hinzu

1. Loggen Sie sich in die QuickSight Konsole ein. Sie können den QuickSight Bericht in einer beliebigen Version erstellen AWS-Region , die dies QuickSight unterstützt. Um die Leistung zu verbessern und die Kosten zu senken, empfiehlt es sich jedoch, den Bericht in der Region zu erstellen, in der sich der Trusted Remediator-Logging-Bucket befindet.
2. Wählen Sie Datasets aus.
3. Wählen Sie S3.
4. Geben Sie in der Neuen S3-Datenquelle die folgenden Werte ein:

   - Name der Datenquelle:`trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`.
   - Laden Sie eine Manifestdatei hoch: Erstellen Sie eine JSON-Datei mit dem folgenden Inhalt und verwenden Sie dann diese Datei. Wenn Sie die Datei erstellen, ersetzen Sie `logging_bucket_name` den URIPrefixes Schlüssel.

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
```

```
}
```

- Wählen Sie Connect aus.
- Wählen Sie im Fenster Datensatzerstellung beenden die Option Visualisieren aus.
- QuickSight öffnet die neue Seite mit dem Analyseblatt. Sie sind jetzt bereit, mithilfe des Problemprotokolls zur Problembehebung eine neue Analyse zu erstellen.

Im Folgenden finden Sie eine Beispielanalyse:

Bewährte Methoden in Trusted Remediator

Im Folgenden finden Sie bewährte Methoden, die Ihnen bei der Verwendung von Trusted Remediator helfen sollen:

- Wenn Sie sich über die Ergebnisse der Korrektur nicht sicher sind, beginnen Sie mit dem manuellen Ausführungsmodus. Manchmal kann die automatische Ausführung von Korrekturen von Anfang an zu unerwarteten Ergebnissen führen.
- Führen Sie eine wöchentliche Überprüfung der Abhilfemaßnahmen durch OpsItems , um Einblicke in die Trusted Remediator-Ergebnisse zu erhalten.
- Mitgliedskonten erben die Konfigurationen des delegierten Administratorkontos. Daher ist es wichtig, die Konten so zu strukturieren, dass Sie mehrere Konten mit denselben Konfigurationen verwalten können. Mithilfe von Tags können Sie Ressourcen von der Standardkonfiguration ausnehmen.

Vertrauenswürdiger Remediator FAQs

Im Folgenden finden Sie häufig gestellte Fragen zu Trusted Remediator:

Was ist Trusted Remediator und welche Vorteile habe ich davon?

Wenn Compute Optimizer eine Nichteinhaltung feststellt Trusted Advisor oder eine Empfehlung von Compute Optimizer ausgibt, reagiert Trusted Remediator gemäß Ihren angegebenen Einstellungen, indem es entweder Abhilfemaßnahmen durchführt, die Genehmigung durch manuelle Korrekturen einholt oder die Abhilfemaßnahmen in Ihrem bevorstehenden Monthly Business Review (MBR) meldet. Die Behebung erfolgt zu Ihrem bevorzugten Zeitpunkt oder Zeitplan. Trusted Remediator bietet Ihnen die Möglichkeit, Prüfungen selbst zu verwalten und entsprechend zu reagieren. Sie

haben die Flexibilität, Trusted Advisor Prüfungen einzeln oder in großen Mengen zu konfigurieren und zu korrigieren. Mit einer Bibliothek getesteter Dokumente zur Problembehebung erhöht AMS Ihre Konten ständig, indem es Sicherheitsüberprüfungen durchführt und bewährte Verfahren befolgt. AWS Sie werden nur benachrichtigt, wenn Sie dies in Ihrer Konfiguration angeben. AMS-Benutzer können sich ohne zusätzliche Kosten für Trusted Remediator anmelden.

In welcher Beziehung steht Trusted Remediator zu anderen und wie funktioniert Trusted Remediator mit anderen zusammen? AWS-Services

Im Rahmen Ihres bestehenden Enterprise Support-Plans haben Sie Zugriff auf Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen. Trusted Remediator lässt sich in Trusted Advisor Compute Optimizer integrieren, um bestehende AMS-Automatisierungsfunktionen zu nutzen. Insbesondere verwendet AMS AWS Systems Manager Automatisierungsdokumente (Runbooks) für automatisierte Problembehebungen. AWS AppConfig wird verwendet, um die Behebungsworkflows zu konfigurieren. Sie können alle aktuellen und vergangenen Behebungen über den Systems Manager OpsCenter einsehen. Die Behebungsprotokolle werden in einem Amazon S3 S3-Bucket gespeichert. Sie können die Protokolle verwenden, um benutzerdefinierte Berichts-Dashboards zu importieren und darin zu erstellen. QuickSight

Wer konfiguriert die Abhilfemaßnahmen?

Sie sind der Eigentümer der Konfigurationen in Ihrem Konto. Die Verwaltung Ihrer Konfigurationen liegt in Ihrer Verantwortung. Sie können sich an Ihre CA oder CDSM wenden, um Hilfe bei der Verwaltung Ihrer Konfigurationen zu erhalten. Sie können sich auch über eine Serviceanfrage an AMS wenden, wenn es um Konfigurationsunterstützung, manuelle Korrekturen und die Behebung von Problembehebungsfehlern geht.

Wie installiere ich Dokumente zur SSM-Automatisierung?

Dokumente zur SSM-Automatisierung werden automatisch an integrierte AMS-Konten weitergegeben.

Werden AMS-eigene Ressourcen ebenfalls berichtigt?

AMS-eigene Ressourcen werden von Trusted Remediator nicht gekennzeichnet. Trusted Remediator konzentriert sich nur auf Ihre Ressourcen.

In welcher AWS-Regionen Version ist Trusted Remediator verfügbar und wer kann ihn verwenden?

Trusted Remediator ist für AMS Accelerate-Kunden verfügbar. Eine aktuelle Liste der Support-Regionen finden Sie unter AWS-Services Nach Regionen geordnet.

Wird Trusted Remediator zu einer Verlagerung von Ressourcen führen?

Da SSM-Automatisierungsdokumente Ressourcen direkt über die AWS API aktualisieren, kann es zu einer Verlagerung von Ressourcen kommen. Sie können Tags verwenden, um Ressourcen zu trennen, die mit Ihren vorhandenen Paketen erstellt wurden. CI/CD Sie können Trusted Remediator so konfigurieren, dass die markierten Ressourcen ignoriert werden, während Ihre anderen Ressourcen trotzdem repariert werden.

Wie pausiere oder stoppe ich Trusted Remediator?

Sie können Trusted Remediator über die AWS AppConfig Anwendung ausschalten. Gehen Sie wie folgt vor, um Trusted Remediator anzuhalten oder zu beenden:

1. Öffnen Sie die AWS AppConfig Konsole unter https://console.aws.amazon.com/systems-manager/appconfig.
2. Wählen Sie Trusted Remediator aus.
3. Wählen Sie im Konfigurationsprofil Einstellungen aus.
4. Wählen Sie die Markierung „Trusted Remediator sperren“ aus.
5. Setzen Sie den Wert des Attributs auf`suspended`. `true`

> **Note**
>
> Seien Sie vorsichtig, wenn Sie dieses Verfahren anwenden, da dadurch Trusted Remediator für alle Konten, die mit dem delegierten Administratorkonto verknüpft sind, beendet wird.

Wie kann ich Prüfungen korrigieren, die von Trusted Remediator nicht unterstützt werden?

Sie können AMS weiterhin über Operations On Demand (OOD) kontaktieren, wenn Prüfungen nicht unterstützt werden. AMS unterstützt Sie bei der Behebung dieser Prüfungen. Weitere Informationen finden Sie unter Operations On Demand.

Wie unterscheidet sich Trusted Remediator von AWS Config Remediation?

AWS Config Remediation ist eine weitere Lösung, mit der Sie Cloud-Ressourcen optimieren und die Einhaltung von Best Practices sicherstellen können. Im Folgenden sind einige der betrieblichen Unterschiede zwischen den beiden Lösungen aufgeführt:

- Trusted Remediator verwendet Trusted Advisor Compute Optimizer als Erkennungsmechanismen. AWS Config Remediation verwendet AWS Config Regeln als Erkennungsmechanismus.
- Bei Trusted Remediator erfolgt die Behebung nach Ihrem vordefinierten Behebungszeitplan. In AWS Config, die Behebung erfolgt in Echtzeit.
- Die Parameter für jede Korrektur in Trusted Remediator lassen sich leicht an Ihren Anwendungsfall anpassen. Die Behebung kann automatisiert oder manuell vorgenommen werden, indem Tags zu Ressourcen hinzugefügt werden.
- Trusted Remediator bietet Berichtsfunktionen.
- Trusted Remediator sendet Ihnen eine E-Mail-Benachrichtigung mit der Liste der Abhilfemaßnahmen und dem Behebungsstatus.

Einige Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen enthalten möglicherweise dieselbe Regel. AWS Config Es hat sich bewährt, nur eine Korrektur zu aktivieren, wenn es eine passende AWS Config Regel und Trusted Advisor Prüfung gibt. Informationen zu den AWS Config Regeln für jede Trusted Advisor Prüfung finden Sie unterTrusted Advisor von Trusted Remediator unterstützte Prüfungen.

Welche Ressourcen stellt Trusted Remediator für Ihre Konten bereit?

Trusted Remediator stellt die folgenden Ressourcen im delegierten Administratorkonto von Trusted Remediator bereit:

- Ein Amazon S3 S3-Bucket mit dem Namen`ams-trusted-remediator-{your-account-id}-logs`. Trusted Remediator erstellt den `Remediation item log` im JSON-Format, wenn eine Problembehebung erstellt OpsItem wird, und lädt die Protokolldateien in diesen Bucket hoch.
- Eine AWS AppConfig Anwendung zur Speicherung der Behebungskonfigurationen für unterstützte Trusted Advisor Prüfungen und Compute Optimizer Optimizer-Empfehlungen.

Trusted Remediator stellt keine Ressourcen im Trusted Remediator-Mitgliedskonto bereit.

Überwachung und Vorfallmanagement für Amazon EKS in AMS Accelerate

Monitoring and Incident Management für Amazon EKS überwacht Ihre Amazon EKS-Ressourcen auf Ausfälle, Leistungseinbußen und Sicherheitsprobleme. AMS Accelerate konfiguriert und implementiert die Warnungsmanager-Regeln von Amazon Managed Service for Prometheus, überwacht die Warnmeldungen und führt dann das Incident-Management durch, wenn diese Alerts ausgelöst werden. Die Überwachung und das Incident Management für Amazon EKS basieren auf AMS Alarm Manager und nutzen native AWS Dienste wie Amazon Managed Service for Prometheus, Amazon Managed Grafana, Amazon GuardDuty, und. AWS LambdaAWS Config

> **Note**
>
> Die Überwachung und das Incident Management für Amazon EKS unterstützen AWS GovCloud (US) weder Windows-Knoten noch Windows-Container.

Was ist Überwachung und Vorfallmanagement für Amazon EKS in AMS Accelerate?

Die Überwachung und das Vorfallmanagement für Amazon EKS bieten Folgendes:

- Eine Standardkonfiguration, die Monitore und Richtlinien für Ihr verwaltetes Konto für von Ihnen ausgewählte Amazon EKS-Cluster erstellt, verwaltet und bereitstellt.
- Eine Monitoring-Baseline, die eine erhöhte Verfügbarkeit Ihrer Amazon EKS-Workloads ermöglicht, auch wenn Sie keine andere Überwachung für Ihre Amazon EKS-Cluster konfigurieren. Weitere Informationen finden Sie unter Basiswarnungen bei der Überwachung und dem Incident-Management für Amazon EKS in AMS Accelerate.
- Benachrichtigungen, die durch die für Ihren Amazon EKS-Cluster konfigurierte Basisüberwachung generiert werden. Diese Benachrichtigungen werden als Warnungen bezeichnet. Warnmeldungen werden generiert, wenn drohende, andauernde, sich zurückziehende oder potenzielle Ausfälle, Leistungseinbußen oder Sicherheitsprobleme auftreten. Zu den Warnmeldungen gehören beispielsweise eine Prometheus-Warnung, ein Ereignis oder ein Ergebnis eines AWS Dienstes wie Amazon. GuardDuty

- Untersuchung von Warnmeldungen mit Anleitungen zu geeigneten Abhilfemaßnahmen, die Sie ergreifen können. Weitere Informationen finden Sie unter Vorfallberichte und Serviceanfragen in AMS Accelerate.
- Behebung von Warnmeldungen und Vorfällen durch AMS Operations, sofern möglich und mit Ihrer Zustimmung, um die Auswirkungen auf Ihre Anwendungen zu verhindern oder zu reduzieren. Weitere Informationen finden Sie unter Vorfallberichte und Serviceanfragen in AMS Accelerate.
- Optionale vordefinierte Amazon Managed Grafana-Dashboards, die Einblick in die Ressourcennutzung, Leistung, den Zustand von CoreDNS, aktive Alerts und zuvor behobene Alerts bieten. Wenn Sie Amazon Managed Grafana mithilfe der von AMS bereitgestellten Vorlage konfigurieren, können Sie die Amazon Managed Grafana-Konsole öffnen, um Metriken und Benachrichtigungen für Ihren Amazon EKS-Cluster anzuzeigen.

So funktionieren Überwachung und Vorfallmanagement für Amazon EKS in AMS Accelerate

Generierung: Im Rahmen der Onboarding-Überwachung und des Incident-Managements für EKS konfiguriert AMS die Basisüberwachung für die Amazon EKS-Cluster, die Sie in Ihrem verwalteten Konto ausgewählt haben. AMS verwendet eine Kombination aus Amazon Managed Service for Prometheus Alert Manager-Regeln und CloudWatch Amazon-Event-Regeln, um die Basisüberwachung zu konfigurieren. Ein AMS-konfigurierter Prometheus-Server in Ihrem Cluster scannt Ihre Prometheus-Metriken und schreibt sie remote auf einen Amazon Managed Service for Prometheus-Endpunkt in derselben Region. Die Basisüberwachungskonfiguration generiert eine Warnung, wenn eine Prometheus-Alert-Manager-Regel ausgelöst oder ein CloudWatch Ereignis generiert wird.

Aggregation: AMS sendet alle Benachrichtigungen, die Ihre Ressourcen generieren, an das AMS-Überwachungssystem, indem es sie an ein Amazon Simple Notification Service-Thema weiterleitet, das von AMS verwaltet wird.

Verarbeitung und Auswirkungsanalyse: AMS analysiert die Warnmeldungen und verarbeitet sie dann auf der Grundlage ihres Auswirkungspotenzials. AMS klassifiziert die Warnmeldungen wie folgt:

- Warnmeldungen mit bekannten Auswirkungen auf den Kunden: Für diese Warnmeldungen erstellt AMS mithilfe des Incident-Management-Prozesses einen neuen Vorfallbericht.
- Warnmeldungen mit ungewisser Auswirkung auf den Kunden: Für diese Warnmeldungen sendet AMS einen Vorfallbericht. In vielen Fällen werden Sie in diesen Benachrichtigungen

aufgefordert, die Auswirkungen zu überprüfen, bevor AMS Maßnahmen ergreifen kann. Bei solchen Warnmeldungen sendet AMS eine Warnmeldung mit den Einzelheiten und prüft, ob für die Warnung eine Abhilfemaßnahme erforderlich ist. AMS bietet in der Benachrichtigung Optionen für Abhilfemaßnahmen. Wenn Ihre Antwort bestätigt, dass es sich bei der Warnung um einen Vorfall handelt, veranlasst AMS die Erstellung eines neuen Vorfallberichts und leitet den Vorfallmanagementprozess ein. Jede Servicemeldung, bei der drei Tage lang die Antwort „keine Auswirkungen auf den Kunden“ oder gar keine Antwort eingeht, wird als gelöst markiert. Außerdem wird die entsprechende Warnung als gelöst markiert.

- Benachrichtigungen ohne Auswirkungen auf den Kunden: Wenn AMS nach der Auswertung feststellt, dass die Warnung keine Auswirkungen auf den Kunden hat, wird die Warnung geschlossen.

AMS-Verantwortungsmatrix (RACI)

Die RACI-Matrix „Verantwortlich, Rechenschaftspflichtig, Konsultiert und Informiert“ (AMS) weist entweder dem Kunden oder AMS die Hauptverantwortung für eine Vielzahl von Aktivitäten zu. Die folgende Tabelle bietet einen Überblick über die Verantwortlichkeiten von Kunde und AMS für Aktivitäten in einer Anwendung, die Monitoring and Incident Management für Amazon EKS verwendet.

- R steht für die verantwortliche Partei, die die Arbeit zur Erfüllung der Aufgabe erledigt.
- A steht für die verantwortliche Partei.
- C steht für konsultiert, also für die Partei, deren Meinung eingeholt wird, in der Regel als Fachexperten, und mit der eine bilaterale Kommunikation besteht.
- I steht für informiert, d. h. die Partei, die über den Stand der Dinge informiert wird, oft erst, wenn die Aufgabe oder das Ergebnis abgeschlossen ist.

Aktivität	Customer	AMS
Anforderungen von Discovery für AMS	I	R
Aktivieren Sie AMS-Berechtigungen (RBAC) für den Clusterzugriff	R	C

Aktivität	Customer	AMS
Installieren Sie Amazon EC2 Systems Manager Agent auf Worker-Knoten, falls er noch nicht vorhanden ist	R	C
Stellen Sie AMS-Komponenten im Cluster wie Prometheus, Prometheus Node Exporter und nach Bedarf kube-state-metrics in einem AMS-Namespace bereit.	C	R
Bereitstellen von Amazon Managed Service für Prometheus in der AMS-Steuerebene	I	R
Konfigurieren Sie den Prometheus Alert Manager in der AMS-Steuerebene	I	R
Stellen Sie die Amazon Managed Grafana-Vorlage bereit und helfen Sie bei der Konfiguration	C	R
Aktivieren Sie die GuardDuty EKS-Auditprotokollüberwachung	C	R
Protokollierung der Amazon EKS-Kontrollebene aktivieren	I	R

Aktivität	Customer	AMS
Überwachen Sie den Zustand und die Leistung der Amazon EKS-Steuerebene	I	R
Überwachen Sie den Zustand und die Leistung Ihres Amazon EKS-Clusters (Cluster, Knoten, Workload, Pod, API-Server und CoreDNS)	I	R
Analysieren Sie Warnmeldungen und reagieren Sie auf Vorfälle für Amazon EKS	I	R
Führen Sie bei Vorfällen Diagnosebefehle aus	I	R
Analysieren Sie Protokolle bei Vorfällen (Kontrollebene und Pod-Logs)	I	R
Reaktion auf Vorfälle bei AWS Netzwerkproblemen	I	R
Reagieren Sie auf die Ergebnisse von GuardDuty EKS Audit Log Monitoring	I	R
Bieten Sie Kunden nach Möglichkeit Hinweise zu Maßnahmen zur Behebung von Vorfällen	I	R

Basiswarnungen bei der Überwachung und dem Incident-Management für Amazon EKS in AMS Accelerate

Nach der Überprüfung der Warnungen aktiviert AMS die folgenden Warnmeldungen für Amazon EKS und übernimmt dann die Überwachung und das Incident-Management für Ihre ausgewählten Amazon EKS-Cluster. Die Reaktionszeit, die Service Level Agreements (SLAs) und die Service Level Objectives (SLOs) hängen von der von Ihnen ausgewählten Service-Stufe (Plus, Premium) ab. Weitere Informationen finden Sie unter Vorfallberichte und Serviceanfragen in AMS Accelerate.

Warnmeldungen und Aktionen

In der folgenden Tabelle sind die Amazon EKS-Warnmeldungen und die entsprechenden Maßnahmen aufgeführt, die AMS ergreift:

Warnung	Schwellenwerte	Aktion
Container OOM wurde getötet	Die Gesamtzahl der Container-Neustarts innerhalb der letzten 10 Minuten beträgt mindestens 1 und ein Kubernetes-Container in einem Pod wurde innerhalb der letzten 10 Minuten mit dem Grund „OOMKilled“ beendet.	AMS untersucht, ob der OOM-Kill auf das Erreichen des Container-Limits oder die Überbelegung des Speicherlimits zurückzuführen ist, und berät Sie anschließend über Abhilfemaßnahmen.
Pod-Job ist fehlgeschlagen	Ein Kubernetes-Job kann nicht abgeschlossen werden. Ein Fehler wird dadurch angezeigt, dass mindestens ein fehlgeschlagener Auftragsstatus vorhanden ist.	AMS untersucht, warum der Kubernetes-Job oder der entsprechende Cron-Job fehlschlägt, und berät Sie dann über Abhilfemaßnahmen.
StatefulSet Heruntergefahren	Die Anzahl der Replikate, die bereit sind, Datenverkehr bereitzustellen, entspricht mindestens 1 Minute StatefulS	AMS ermittelt anhand von Fehlermeldungen in Pod-Ereignissen und Fehlerprotokollfragmenten in Pod-Proto

Warnung	Schwellenwerte	Aktion
	et lang nicht der aktuellen Anzahl vorhandener Replikate pro Tag.	kollen, warum Pods nicht bereit sind, und berät Sie dann über Abhilfemaßnahmen.
Fähigkeit zur HPA-Skalierung	Der Horizontal Pod Autoscaler (HPA) kann nicht skaliert werden, da die Statusbedingung „AbleToScale“ mindestens 2 Minuten lang falsch war.	AMS ermittelt, welcher Kubernetes Horizontal Pod Autoscaler (HPA) nicht in der Lage ist, Pods für seine nachfolgende Workload-Ressource zu skalieren, z. B. ein Deployment oder. StatefulSet
Verfügbarkeit von HPA-Metriken	Der Horizontal Pod Autoscaler (HPA) kann keine Messwerte erfassen, da die Statusbedingung „ScalingActive“ mindestens 2 Minuten lang falsch war.	AMS ermittelt, warum HPA keine Messwerte erfassen kann, z. B. Metriken im Zusammenhang mit Serverkonfigurationsproblemen oder RBAC-Autorisierungsprobleme n.
Pod nicht bereit	Ein Kubernetes-Pod bleibt länger als 15 Minuten im Status „Nicht aktiv“ (z. B. „Ausstehend“, „Unbekannt“ oder „Fehlgeschlagen“).	AMS untersucht die betroffenen Pods auf Einzelheiten, überprüft die Pod-Logs auf entsprechende Fehler und Ereignisse und berät Sie anschließend über Abhilfemaßnahmen.

Warnung	Schwellenwerte	Aktion
Pod-Crash-Looping	Ein Pod-Container wird mindestens einmal alle 15 Minuten über einen Zeitraum von 1 Stunde neu gestartet.	AMS untersucht die Gründe dafür, dass der Pod nicht startet, z. B. unzureichende Ressourcen, eine durch einen anderen Container gesperrte Datei, durch einen anderen Container gesperrte Datenbank, fehlgeschlagene Dienstabhängigkeiten, DNS-Probleme für externe Dienste und Fehlkonfigurationen.
Daemonset ist falsch geplant	Mindestens ein Kubernetes-Daemonset-Pod wurde über einen Zeitraum von 10 Minuten verschoben.	AMS ermittelt, warum ein Daemonset auf einem Knoten geplant ist, auf dem sie nicht ausgeführt werden sollen. Dies kann passieren, wenn der falsche Pod auf die Daemonset-Pods angewendet nodeSelector/taints/affinities wurde oder wenn Knoten (Knotenpools) beschädigt waren und die Entfernung vorhandener Pods nicht geplant war.

Warnung	Schwellenwerte	Aktion
Kubernetes-API-Fehler	Die Fehlerrate des Kubernetes-API-Servers liegt über einen Zeitraum von 2 Minuten bei über 3%.	AMS analysiert die Protokolle der Kontrollebene, um das Volumen und die Art der Fehler zu ermitteln, die diese Warnung verursachen, und identifiziert alle Probleme mit Ressourcenkonflikten bei Masterknoten- oder etcd-Autoscaling-Gruppen. Wenn der API-Server nicht wiederhergestellt wird, beauftragt AMS das Amazon EKS-Serviceteam.
Kubernetes-API-Latenz	Die Latenz von Anfragen an den Kubernetes-API-Server beträgt über einen Zeitraum von 2 Minuten mehr als 1 Sekunde.	AMS analysiert die Protokolle der Kontrollebene, um das Volumen und die Art der Fehler zu ermitteln, die zu Latenz führen, und identifiziert alle Probleme mit Ressourcenkonflikten für Masterknoten- oder etcd-Autoscaling-Gruppen. Wenn der API-Server nicht wiederhergestellt wird, beauftragt AMS das Amazon EKS-Serviceteam.
Kubernetes-Client-Zertifikat läuft ab	Das zur Authentifizierung beim Kubernetes-API-Server verwendete Client-Zertifikat läuft in weniger als 24 Stunden ab.	AMS sendet diese Benachrichtigung, um Sie darüber zu informieren, dass Ihr Cluster-Zertifikat in 24 Stunden abläuft.

Warnung	Schwellenwerte	Aktion
Der Knoten ist nicht bereit	Der Status „Bereit“ des Knotens ist mindestens 10 Minuten lang falsch.	AMS untersucht die Bedingungen und Ereignisse des Knotens, z. B. Netzwerkprobleme, die den Kubelet-Zugriff auf den API-Server verhindern.
CPU mit hohem Knotenwert	Die CPU-Last übersteigt über einen Zeitraum von 5 Minuten 80%.	AMS ermittelt, ob ein oder mehrere Pods ungewöhnlich viel CPU verbrauchen. Anschließend überprüft AMS gemeinsam mit Ihnen, ob Ihre Anfragen, Grenzwerte und Pod-Aktivitäten den Erwartungen entsprechen.
Node OOM Kill erkannt	In einem 4-Minuten-Fenster wurde vom Knoten mindestens ein Host-OOM-Kill gemeldet.	AMS ermittelt, ob der OOM-Kill durch das Erreichen des Container-Limits oder durch eine Überbelegung des Knotens verursacht wurde. Wenn die Anwendungsaktivität normal ist, informiert Sie AMS über Anfragen und Beschränkungen für Overcommits und die Änderung der Pod-Limits.

Warnung	Schwellenwerte	Aktion
Contrack-Limit für Knoten	Das Verhältnis zwischen der aktuellen Anzahl von Verbindungsverfolgungseintr ägen und dem Höchstlimit übersteigt über einen Zeitraum von 5 Minuten 80%.	AMS berät Sie über den empfohlenen Conntrack-Wert pro Kern. Kubernetes-Knoten legen den Conntrack -Maximalwert proportional zur Gesamtspeicherkapa zität des Knotens fest. Anwendungen mit hoher Auslastung, insbesondere auf kleineren Knoten, können den Conntrack-Max-Wert leicht überschreiten, was zu Verbindungsresets und Timeouts führt.
Die Knotenuhr ist nicht synchron	Der minimale Synchroni sierungsstatus über einen Zeitraum von 2 Minuten ist 0, und der maximale Fehler in Sekunden ist 16 oder höher.	AMS bestimmt, ob das Network Time Protocol (NTP) installiert ist und ordnungsg emäß funktioniert.
Hohe CPU-Leistung	Die CPU-Auslastung eines Containers liegt über einen Zeitraum von mindestens 2 Minuten bei einer Rate von über 3 Minuten bei über 80%.	AMS untersucht Pod-Logs, um die Pod-Aufgaben zu ermitteln , die viel CPU verbrauchen.
Pod mit hohem Arbeitssp eicher	Die Speicherauslastung eines Containers überschreitet über einen Zeitraum von 2 Minuten 80% des angegeben en Speicherlimits.	AMS untersucht Pod-Logs, um die Pod-Aufgaben zu ermitteln , die viel Speicher verbrauch en.

Warnung	Schwellenwerte	Aktion
CoreDNS ausgefallen	CoreDNS ist seit mehr als 15 Minuten aus der Zielentdeckung von Prometheus verschwunden.	Dies ist eine kritische Warnung, die darauf hinweist, dass die Domainnamenauflösung für interne oder externe Clusterdienste gestoppt wurde. AMS überprüft den Status der CoreDNS-Pods, verifiziert die CoreDNS-Konfiguration, verifiziert DNS-Endpunkte, die auf CoreDNS-Pods verweisen, verifiziert die CoreDNS-Grenzwerte und aktiviert mit Ihrer Zustimmung die CoreDNS-Debug-Protokollierung.
CoreDNS-Fehler	CoreDNS gibt SERVFAIL-Fehler für mehr als 3% der DNS-Anfragen über einen Zeitraum von 10 Minuten zurück.	Diese Warnung kann auf ein Problem mit einer Anwendung oder eine Fehlkonfiguration hinweisen. AMS überprüft den Status der CoreDNS-Pods, verifiziert die CoreDNS-Konfiguration, verifiziert DNS-Endpunkte, die auf CoreDNS-Pods verweisen, verifiziert die CoreDNS-Grenzwerte und aktiviert mit Ihrer Zustimmung die CoreDNS-Debug-Protokollierung.

Warnung	Schwellenwerte	Aktion
CoreDNS-Latenz	Das 99. Perzentil der Dauer von DNS-Anfragen überschreitet 4 Sekunden für 10 Minuten.	Diese Warnung signalisiert, dass CoreDNS möglicherweise überlastet ist. AMS überprüft den Status der CoreDNS-Pods, verifiziert die CoreDNS-Konfiguration, verifiziert DNS-Endpunkte, die auf die CoreDNS-Pods verweisen, verifiziert die CoreDNS-Grenzwerte und aktiviert mit Ihrer Zustimmung die CoreDNS-Debug-Protokollierung.

Warnung	Schwellenwerte	Aktion
CoreDNS-Weiterleitungslatenz	Das 99. Perzentil der Antwortzeit für CoreDNS-Weiterleitungsanfragen an kube-dns überschreitet 4 Sekunden über einen Zeitraum von 10 Minuten.	Wenn CoreDNS nicht der autoritative Server ist oder keinen Cache-Eintrag für einen Domainnamen hat, leitet CoreDNS die DNS-Anfrage an einen Upstream-DNS-Server weiter. Diese Warnung signalisiert, dass CoreDNS möglicherweise überlastet ist oder ein Problem mit einem Upstream-DNS-Server vorliegt. AMS überprüft den Status von CoreDNS-Pods, verifiziert die CoreDNS-Konfiguration, verifiziert DNS-Endpunkte, die auf CoreDNS-Pods verweisen, verifiziert CoreDNS-Grenzwerte und aktiviert mit Ihrer Zustimmung die CoreDNS-Debug-Protokollierung.

Warnung	Schwellenwerte	Aktion
CoreDNS-Weiterleitungsfehler	Mehr als 3% der DNS-Abfragen schlagen innerhalb von 5 Minuten fehl.	Wenn CoreDNS nicht der autoritative Server ist oder keinen Cache-Eintrag für einen Domainnamen hat, leitet CoreDNS die DNS-Anfrage an einen Upstream-DNS-Server weiter. Diese Warnung weist auf eine mögliche Fehlkonfiguration oder ein Problem mit einem Upstream-DNS-Server hin. AMS überprüft den Status von CoreDNS-Pods, verifiziert die CoreDNS-Konfiguration, verifiziert DNS-Endpunkte, die auf CoreDNS-Pods verweisen, verifiziert CoreDNS-Grenzwerte und aktiviert mit Ihrer Zustimmung die CoreDNS-Debug-Protokollierung.

Anforderungen an die Überwachung und das Incident-Management für Amazon EKS in AMS Accelerate

Dies sind die unterstützten and/or erforderlichen Ressourcen für die Überwachung und das Incident-Management für Amazon EKS for AMS Accelerate

- Unterstützte Kubernetes-Versionen: Weitere Informationen zu Amazon EKS Kubernetes-Versionen finden Sie im Amazon EKS-Benutzerhandbuch.
- Knotentypen: Von Amazon EKS verwaltete Knoten werden unterstützt. Windows-Knoten und Container werden nicht unterstützt.
- Kubernetes-Clusterzugriff: AMS benötigt die RBAC-Clusterrolle system:masters und den Cluster-Benutzer.

- SSM Agent auf EC2 Amazon-Knoten: Sowohl Bottle Rocket als auch Amazon EKS AMIs haben SSM Agent vorinstalliert. Stellen Sie sicher, dass SSM Agent auf Ihren benutzerdefinierten Knoten AMIs und EC2 Amazon-Knoten installiert ist.
- Servicekontingente Weitere Informationen finden Sie in den Service Quotas für Amazon Managed Service für Prometheus und Amazon Managed Grafana.
- Unterstützte Regionen: AWS

Name der Region	Region	Metriken, Speicherregion
USA Ost (Ohio)	us-east-2	us-east-2
USA Ost (Nord-Virginia)	us-east-1	us-east-1
USA West (Oregon)	us-west-2	us-west-2
Asien-Pazifik (Tokio)	ap-northeast-1	ap-northeast-1
Asien-Pazifik (Seoul)	ap-northeast-2	ap-northeast-2
Asien-Pazifik (Singapur)	ap-southeast-1	ap-southeast-1
Asien-Pazifik (Sydney)	ap-southeast-2	ap-southeast-2
Europa (Frankfurt)	eu-central-1	eu-central-1
Europa (Irland)	eu-west-1	eu-west-1
Europa (London)	eu-west-2	eu-west-2
Afrika (Kapstadt)	af-south-1	eu-west-1 eu-west-2
Asien-Pazifik (Hongkong)	ap-east-1	ap-northeast-1 ap-northeast-2

> **Note**
>
> Metriken für Amazon EKS-Cluster in af-south-1, Afrika (Kapstadt) und ap-east-1, Asien-Pazifik (Hongkong), werden jeweils im selben Format an den AMS-Überwachungsservice exportiert. AWS-Region Metriken für diese AWS-Regionen werden dann innerhalb des AMS-Überwachungsdienstes in verschiedene Regionen transportiert, wo sie verarbeitet und gespeichert werden. In der obigen Tabelle finden Sie die Regionen, die der AMS-Überwachungsdienst zum Speichern von Metriken verwendet.

Integrieren Sie die Überwachung und das Incident Management für Amazon EKS in AMS Accelerate

Führen Sie die folgenden Schritte aus, um die Überwachung und das Incident-Management für Amazon EKS zu nutzen.

1. Amazon EKS-Kostenoptimierungs-Tags aktivieren: Weitere Informationen finden Sie unter Taggen Ihrer Ressourcen für die Abrechnung im Amazon EKS-Benutzerhandbuch.
2. Initiieren Sie die Einführung von Monitoring und Incident Management für EKS: Wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM) und teilen Sie ihm die Konto IDs - und Clusternamen für das Onboarding mit.
3. Überprüfen Sie die Anforderungen: Ihr Cloud Architect (CA) überprüft, ob alle Anforderungen erfüllt sind, bevor das Onboarding beginnt.
4. Aktualisieren Sie die rollenbasierte Zugriffskontrolle (RBAC) von Kubernetes: AMS teilt die Befehle für die Implementierung dieser Änderungen. `eksctl` Sie können diese Änderungen überprüfen und dann bereitstellen. Sie müssen RBAC-Updates bereitstellen, damit AMS berechtigt ist, Befehle in Ihrem Namen auszuführen. Zu diesen Updates gehören die Zuordnung der AMS-IAM-Rolle zu einem Kubernetes-Benutzer, die Erstellung einer neuen Kubernetes-Clusterrolle für AMS und die Bindung der AMS-Kubernetes-Clusterrolle an den Benutzer.
5. Clusterkomponenten bereitstellen: AMS stellt die folgenden Komponenten in einem AMS-verwalteten Namespace auf Ihrem Cluster bereit:
   - Prometheus-Server
   - Prometheus-Knotenexporteur (gilt nicht für) AWS Fargate
   - kube-state-metrics

6. Führen Sie Prometheus-Konfigurationsupdates durch: AMS konfiguriert Prometheus so, dass Metriken per Fernzugriff geschrieben werden können.
7. (Optional) Dashboards konfigurieren: Ihre CA hilft Ihnen bei der Konfiguration von Amazon Managed Grafana-Dashboards in Ihrem Konto.

> **Note**
>
> Nach dem Onboarding Ihres Amazon EKS-Clusters analysiert AMS Warnsignale und führt eine Basisbewertung durch, um bestehende Probleme in Ihrem Cluster zu identifizieren. Nach Abschluss der Basisbewertung teilt AMS die Ergebnisse und Empfehlungen zur Problembehebung über Trusted Advisor und eine Serviceanfrage mit, mit der Sie Probleme in Ihrem Cluster beheben können. Auf der Grundlage der Bewertung erstellt AMS eine Amazon EKS-Monitoring-Baseline, die speziell auf Ihre EKS-Cluster zugeschnitten ist, indem unsere Alarmschwellenwerte auf Kontoebene angepasst werden. Um doppelte AMS-Antworten auf diese Ergebnisse zu vermeiden, passen wir unsere Überwachung so an, dass diese Warnsignale ausgeschlossen werden. Wir passen unsere Überwachung so an, dass auch die Signale berücksichtigt werden, wenn uns Ihr CSDM darüber informiert, dass die zugrunde liegenden Probleme behoben wurden.

Offboard aus Monitoring und Incident Management für Amazon EKS in AMS Accelerate

Teilen Sie Ihrem Cloud Service Delivery Manager (CSDM) die Konto IDs - und Clusternamen mit, um den Offboarding-Prozess zu starten. Nach dem Offboarding werden die Alert-Verarbeitung, das Speichern von Kennzahlen und das Abfragen von Metriken ausgesetzt und Metriken werden gemäß den standardmäßigen Datenaufbewahrungsrichtlinien von Amazon Managed Service für Prometheus gelöscht.

AMS führt die folgenden Offboarding-Schritte durch:

1. AMS deaktiviert Benachrichtigungen, die an Sie und AMS Operations gesendet werden.
2. AMS entfernt die Prometheus-Instance aus Ihrem Amazon EKS-Cluster.
3. AMS entfernt andere AWS Ressourcen, die in Ihrem Konto installiert sind, wie z. B. IAM-Rollen und -Regeln. AWS Config

Nachdem diese Schritte abgeschlossen sind, müssen Sie die folgenden Offboarding-Schritte ausführen:

1. Wird verwendet`eksctl`, um die Kubernetes-RBAC-Berechtigungen aus dem zu entfernen. `aws-auth` `ConfigMap`
2. Wenn Sie es zuvor installiert haben, entfernen Sie die Amazon Managed Grafana-Instance, die Sie für die Verbindung mit AMS konfiguriert haben.

Kontinuitätsmanagement in AMS Accelerate

AMS nutzt AWS Backup die Möglichkeit, die Sicherung Ihrer Daten dienstübergreifend AWS zu zentralisieren und zu automatisieren. AMS-Backup-Pläne bieten bewährte Methoden für verschiedene Anwendungsfälle. Sie können Ihre bestehenden Backup-Pläne jedoch gerne weiterhin verwenden. Nach der Einführung in das AMS-Backup-Management erstellt AMS Backup-Berichte, und AMS-Experten überwachen Ihre Backup-Aufgaben kontinuierlich, um sicherzustellen, dass Sie über eine zuverlässige Backup-Lösung verfügen.

Weitere Informationen finden Sie unter AWS Backup: So funktioniert es und unterstützte AWS Ressourcen und Anwendungen von Drittanbietern.

AMS Accelerate bietet eine Reihe von Betriebsdienstleistungen, die Sie dabei unterstützen, betriebliche Exzellenz zu erreichen AWS. Einen schnellen Überblick darüber, wie AMS Ihren Teams dabei hilft, AWS Cloud mit einigen unserer wichtigsten betrieblichen Funktionen, darunter Helpdesk rund um die Uhr, proaktive Überwachung, Sicherheit, Patching, Protokollierung und Backup, zu operativer Exzellenz zu gelangen, finden Sie in den AMS-Referenzarchitekturdiagrammen.

Sehen Sie sich Carls Video an, um mehr zu erfahren (9:29)

Themen

So funktioniert das Kontinuitätsmanagement in AMS

Die AMS-Backup-Pläne definieren, wie häufig Ihre Daten gesichert werden und welche Aufbewahrungsrichtlinien für Ihre Backups gelten. AMS-Backup-Tresore sorgen dafür, dass Ihre Backup-Daten organisiert sind. Sobald eine Ressource einem Backup-Plan zugeordnet ist, werden kompatible Ressourcen inkrementell gesichert. Das erste Backup ist eine vollständige Kopie, und nachfolgende Backups erfassen inkrementelle Änderungen. Abhängig von der ausgewählten Ressource und dem ausgewählten AMS-Backup-Plan können Sie mit Point-in-time Restore (PITR)

Ihre Ressourcen zurückspulen, indem Sie einen Zeitpunkt für Ihre Wiederherstellung auswählen. Um mit AMS Backup Management zu beginnen, wählen Sie einfach einen AMS-Backup-Plan aus und markieren Sie Ihre Ressourcen.

> **Note**
>
> Stellen Sie sicher, dass dieser für jedes Konto und jeden Ressourcentyp aktiviert AWS Backup ist AWS-Region, indem Sie die folgenden Schritte ausführen: Erste Schritte 1: Service-Opt-In.
> Sie müssen nicht mit Erste Schritte 2: On-Demand-Backup erstellen fortfahren.

Verwandte Themen von AWS Backup

- Arbeiten mit Backups (Erstellen, Bearbeiten, Kopieren, Wiederherstellen, Löschen)
- Erstellen eines On-Demand-Backups
- Erstellen von Sicherungskopien auf AWS-Regionen
- AWS Backup Unterstützte Services
- Point-in-time wiederherstellen
- AWS Backup Funktionen

Wählen Sie einen AMS-Backup-Plan

AMS bietet drei verschiedene Backup-Pläne mit einem vierten Backup-Plan, um die Kosten beim Onboarding zu minimieren. Um für jede unterstützte Ressource einen AMS-Backup-Plan auszuwählen, kennzeichnen Sie die Ressource mit dem zugehörigen Tag des Plans. Bei der Einführung von Accelerate arbeitet AMS mit Ihnen zusammen, um den Backup-Plan zu finden, der Ihren Anforderungen am besten entspricht.

> **Important**
>
> Bearbeiten Sie Ihre AMS-Standard-Backup-Pläne nicht, da Ihre Änderungen verloren gehen könnten. Erstellen Sie stattdessen neue Pläne für Ihre benutzerdefinierten Konfigurationen. Weitere Informationen finden Sie unter Erstellen eines Backup-Plans.

Standard-AMS-Backup-Plan

AWS Backup Die kontinuierliche Sicherung ist für diesen Backup-Plan nicht aktiviert. Einzelheiten finden Sie unter Wiederherstellung zu einem bestimmten Zeitpunkt mithilfe von point-in-time Restore (PITR) wiederherstellen.

TAG-Schlüssel: `ams:rt:backup-orchestrator`

TAG-Wert: `true`

Standard-AMS-Backup-Plan	Start Time	Aufbewahrung
stündliches Backup	N/A	N/A
tägliches Backup	täglich 4:00 UTC	7 Tage
wöchentliches Backup	Samstag, 2:00 Uhr UTC	4 Wochen
monatliches Backup	1. des Monats, 2:00 UTC	26 Wochen
jährliches Backup	1. Januar, 2:00 Uhr UTC	2 Jahre

Verbesserter Backup-Plan

AWS Backup Kontinuierliches Backup ist mit maximaler Aufbewahrung (31 Tage) auf unterstützten Ressourcen aktiviert. Weitere Informationen finden Sie unter Wiederherstellung zu einem bestimmten Zeitpunkt mithilfe von point-in-time Wiederherstellung (PITR) und Unterstützte Dienste und Anwendungen für die point-in-time Wiederherstellung (PITR).

TAG-Schlüssel: `ams:rt:backup-orchestrator-enhanced`

TAG-Wert: `true`

Verbesserter Backup-Plan	Start Time	Aufbewahrung
stündliches Backup	N/A	N/A
tägliches Backup	täglich 4:00 UTC	31 Tage

Verbesserter Backup-Plan	Start Time	Aufbewahrung
wöchentliches Backup	Samstag, 2:00 Uhr UTC	6 Wochen
monatliches Backup	1. des Monats, 2:00 UTC	26 Wochen
jährliches Backup	1. Januar, 2:00 Uhr UTC	2 Jahre

Backup-Plan für sensible Daten

AWS Backup Kontinuierliches Backup ist mit maximaler Aufbewahrung (31 Tage) auf unterstützten Ressourcen aktiviert. Einzelheiten finden Sie unter Wiederherstellung zu einem bestimmten Zeitpunkt mithilfe von point-in-time Wiederherstellung (PITR) und Unterstützte Dienste und Anwendungen für die point-in-time Wiederherstellung (PITR).

TAG-Schlüssel: `ams:rt:backup-orchestrator-data-sensitive`

TAG-Wert: `true`

Backup-Plan für sensible Daten	Start Time	Aufbewahrung
stündliches Backup	jede Stunde	7 Tage
tägliches Backup	täglich 4:00 UTC	31 Tage
wöchentliches Backup	Samstag, 2:00 Uhr UTC	6 Wochen
monatliches Backup	1. des Monats, 2:00 UTC	26 Wochen
jährliches Backup	1. Januar, 2:00 Uhr UTC	2 Jahre

Backup-Plan für AMS Accelerate Onboarding

AWS Backup Kontinuierliches Backup ist für diesen Backup-Plan nicht aktiviert. Einzelheiten finden Sie unter Wiederherstellung zu einem bestimmten Zeitpunkt mithilfe von point-in-time Restore (PITR) wiederherstellen.

TAG-Schlüssel: `ams:rt:backup-orchestrator-onboarding`

TAG-Wert: `true`

Backup-Plan für das Accelerate Onboarding von AMS	Start Time	Aufbewahrung
stündliches Backup	jede Stunde	2 Wochen
tägliches Backup	N/A	N/A
wöchentliches Backup	N/A	N/A
monatliches Backup	N/A	N/A
jährliches Backup	N/A	N/A

Verwandte AWS Backup Themen

- Einen Backup-Plan erstellen
- Point-in-time restore (PITR) ermöglicht kontinuierliche Backups der unterstützten Ressourcen und ermöglicht es Ihnen, einen bestimmten Zeitpunkt für Ihre Wiederherstellung auszuwählen. Eine Liste der unterstützten Ressourcen finden Sie unter Verfügbarkeit von Funktionen nach Ressourcen.

Kennzeichnen Sie Ihre Ressourcen, um AMS-Backup-Pläne anzuwenden

Um einem AMS-Backup-Plan Ressourcen zuzuweisen, kennzeichnen Sie die Ressource mit dem Tag-Schlüssel-Wert-Paar des Plans. Sie können AMS Resource Tagger verwenden, um die AMS-Backup-Pläne auf eine Teilmenge Ihrer Ressourcen oder auf alle unterstützten Ressourcen in Ihrem Konto anzuwenden. Wenn Sie eine alternative Methode verwenden möchten, um Tags auf Ihre Ressourcen anzuwenden, z. B. AWS CloudFormation oder Terraform, dann schalten Sie Resource Tagger aus, damit es nicht mit der von Ihnen gewählten Tagging-Methode konkurriert. Weitere Informationen finden Sie unter Verhindern, dass Resource Tagger Ressourcen verändert.

Das folgende Beispiel zeigt, wie Sie Resource Tagger verwenden können, um den standardmäßigen AMS-Backup-Plan auf Amazon Elastic Compute Cloud-Instances in Ihrem Konto anzuwenden. Wenden Sie für diesen Backup-Plan den Tag-Schlüssel `ams:rt:backup-orchestrator` und

den Tag-Wert `true` an. Um einen anderen Backup-Plan zu verwenden, ändern Sie den Schlüssel so, dass er dem Tag-Schlüssel Ihres gewünschten Backup-Plans entspricht. Weitere Informationen zu AMS Resource Tagger und zur Integration des folgenden referenzierten Profils in das aktuelle (bereits konfigurierte) Profil in Ihrem Accelerate-Konto finden Sie unterBeschleunigen Sie Resource Tagger.

1. Öffnen Sie die AWS AppConfig Konsole unter https://console.aws.amazon.com/systems-manager/appconfig.
2. Wählen Sie die ResourceTagger-Anwendung.
3. Wählen Sie die Registerkarte Konfigurationsprofile und wählen Sie dann CustomerManagedTags
4. Wählen Sie Erstellen, um eine neue Version zu erstellen.
5. Wählen Sie JSON und kopieren Sie dann das folgende JSON-Objekt und fügen Sie es ein:

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. Wählen Sie Gehostete Konfigurationsversion erstellen aus.
7. Klicken Sie auf Start deployment (Bereitstellung starten).
8. Definieren Sie die folgenden Bereitstellungsdetails:

```
Environment: AMSInfrastructure
```

```
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. Klicken Sie auf Start deployment (Bereitstellung starten). Resource Tagger kennzeichnet Ihre Instances `ams:rt:backup-orchestrator: true` und stellt so sicher, dass Ihre Instances gemäß dem standardmäßigen AMS-Backup-Plan gesichert werden.

Backups in AMS-Tresoren anzeigen

Mithilfe von Tags können Sie die Benachrichtigungen für den Backup-Tresor auf individueller Tresorebene steuern. Sie können Benachrichtigungen für einen bestimmten Tresor deaktivieren, indem Sie das Tag hinzufügen `AMSNotificationOptOut` und den Wert für einen bestimmten Tresor `True` auf setzen. Um weiterhin Benachrichtigungen aus dem Tresor zu erhalten, entfernen Sie das Tag.

Um eine Liste Ihrer AMS-Backups anzuzeigen, öffnen Sie die AWS Backup Konsole. Wählen Sie im Navigationsbereich Backup-Tresore und wählen Sie einen der AMS-Backup-Tresore aus den folgenden Tabellen aus. Sehen Sie sich im Abschnitt Backups die Liste aller Backups im Backup-Tresor an. Wählen Sie ein Backup aus, das bearbeitet, gelöscht oder wiederhergestellt werden soll.

Tresore für AMS-Backup-Pläne

Name des AMS-Tresors	AMS-Backup-Plan-Tag-Schlüssel
ams-automated-backups	ams:rt:backup-orchestrator
ams-automated-enhanced-backups	ams: rt: backup-orchestrator-enhanced
ams-automated-data-sensitive-Backups	ams: rt: backup-orchestrator-data-sensitive
ams-onboarding-backups	ams:rt: backup-orchestrator-onboarding

Andere AMS-Tresore

Name des AMS-Tresors	Beschreibung
ams-manual-backups	Dieser Tresor enthält manuell gestartete Backups, die mit dem `AWSManagedServices`

Name des AMS-Tresors	Beschreibung
	`-StartBackupJob` SSM Automation-Dokument erstellt wurden, und Pre-Patch-Backups, die vor dem Patchen von AMS-Patch-Automatisierungen erstellt wurden.
ams-custom-backups	Dies ist der empfohlene Tresor für Backups, die außerhalb von AMS-Backup-Plänen erstellt wurden.

Verwandte AWS Backup Themen

- Backups nach Ressource anzeigen
- Mit Backups arbeiten

Überwachung und Berichterstattung von AMS-Backups

> **Important**
>
> Die Überwachung und Berichterstattung von AMS-Backups sind nur in Regionen verfügbar, die von AMS unterstützt werden. Dies sind USA Ost (Virginia), USA West (Nordkalifornien), USA West (Oregon), USA Ost (Ohio), Kanada (Zentral), Südamerika (São Paulo), EU (Irland), EU (Frankfurt), EU (London), EU (Paris), Asien-Pazifik (Mumbai), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio).

AMS generiert tägliche Self-Service-Berichte sowie monatliche Berichte zur Ressourcenabdeckung und zum Status der Backup-Jobs. Die monatlichen Berichte werden in Monthly Business Reviews (MBRs) veröffentlicht. Weitere Informationen zu täglichen Backup-Berichten finden Sie unter Täglicher Backup-Bericht .

AMS-Experten überwachen alle Ihre Backup-Aufgaben, die mit konfiguriert sind AWS Backup. Im Falle von Backup-Ausfällen untersucht AMS den Fehler und informiert Sie über die Ursache und die Behebungsoptionen, sofern verfügbar. Um Warnmeldungen zu vermeiden, gibt AMS bei Ereignissen, die zu einer hohen Anzahl von Backup-Ausfällen in Ihren Konten führen, über Ihr CSDM eine kollektive Empfehlung ab, anstatt Sie bei jedem einzelnen Fehler zu benachrichtigen.

Beachten Sie, dass AMS keine Backups überwacht, die mithilfe der eigenständigen AWS Backup-Funktion eines Dienstes konfiguriert wurden.

Patch-Management in AMS Accelerate verstehen

Important

Accelerate Patch Reporting implementiert in regelmäßigen Abständen eine AWS Glue ressourcenbasierte Richtlinie. Beachten Sie, dass AMS-Updates für das Patching-System bestehende ressourcenbasierte Richtlinien überschreiben. AWS Glue

Important

Sie können alternative Patch-Repositorys für verwaltete Knoten angeben. AMS implementiert zwar Ihre angeforderten Patch-Konfigurationen, Sie sind jedoch dafür verantwortlich, die Sicherheit Ihrer ausgewählten Repositorys auszuwählen und zu überprüfen. Sie müssen auch alle Risiken akzeptieren, die sich aus der Nutzung dieser Repositorien ergeben, wie z. B. Risiken in der Lieferkette.
Im Folgenden finden Sie bewährte Methoden für die Sicherheit Ihres Patch-Management-Prozesses:

- Verwenden Sie nur vertrauenswürdige, verifizierte Repository-Quellen
- Verwenden Sie nach Möglichkeit standardmäßig standardmäßige Repositorys von Betriebssystemanbietern
- Prüfen Sie regelmäßig benutzerdefinierte Repository-Konfigurationen

Sie können das AMS Accelerate-Patch-System Patch Add-On verwenden, um Ihre Instances mit sicherheitsrelevanten und anderen Updates zu patchen. Accelerate Patch Add-On ist eine Funktion, die tagbasiertes Patching für AMS-Instances ermöglicht. Es nutzt die AWS Systems Manager (SSM) - Funktionalität, sodass Sie Instances taggen und diese Instances mithilfe einer Baseline und eines von Ihnen konfigurierten Fensters patchen lassen können. Das AMS Accelerate Patch Add-On ist eine Onboarding-Option. Wenn Sie es beim Onboarding Ihres Accelerate-Kontos nicht erhalten haben, wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM), um es zu erhalten.

AMS Accelerate Patch Management verwendet die Patch-Baseline-Funktionalität von Systems Manager, um die Definition der Patches zu steuern, die auf eine Instanz angewendet werden.
Die Patch-Baseline enthält die Liste der Patches, die vorab genehmigt wurden, z. B. alle

Sicherheitspatches. Die Konformität der Instanz wird anhand der ihr zugewiesenen Patch-Baseline gemessen. AMS Accelerate installiert standardmäßig alle verfügbaren Patches, um die Instance auf dem neuesten Stand zu halten.

> **Note**
>
> AMS Accelerate wendet nur Betriebssystem-Patches (OS) an. Beispielsweise werden für Windows nur Windows-Updates angewendet, keine Microsoft-Updates.

Informationen zu Berichten finden Sie unterAMS-Host-Management-Berichte.

AMS Accelerate bietet eine Reihe von Betriebsdienstleistungen, die Sie dabei unterstützen, betriebliche Exzellenz zu erreichen AWS. Einen schnellen Überblick darüber, wie AMS Ihren Teams dabei hilft, AWS Cloud mit einigen unserer wichtigsten betrieblichen Funktionen, darunter Helpdesk rund um die Uhr, proaktive Überwachung, Sicherheit, Patching, Protokollierung und Backup, zu operativer Exzellenz zu gelangen, finden Sie in den AMS-Referenzarchitekturdiagrammen.

Themen

Empfehlungen zum Patchen

Wenn Sie im Anwendungs- oder Infrastrukturbetrieb tätig sind, wissen Sie, wie wichtig eine Patch-Lösung für das Betriebssystem (OS) ist, die flexibel und skalierbar genug ist, um den unterschiedlichen Anforderungen Ihrer Anwendungsteams gerecht zu werden. In einer typischen Organisation verwenden einige Anwendungsteams eine Architektur, die unveränderliche Instanzen beinhaltet, während andere ihre Anwendungen auf veränderbaren Instanzen bereitstellen.

Weitere Informationen zu AWS präskriptiven Anleitungen zum Patchen finden Sie unter Automatisiertes Patchen für veränderliche Instanzen in der Hybrid Cloud unter Verwendung von. AWS Systems Manager

> **Note**
>
> Accelerate Patch Add-On ist eine Funktion, die tagbasiertes Patching für AMS-Instanzen ermöglicht. Es nutzt die AWS Systems Manager (SSM) -Funktionalität, sodass Sie Instances taggen und diese Instances mithilfe einer Baseline und eines von Ihnen konfigurierten Fensters patchen lassen können. Das AMS Accelerate Patch Add-On ist eine Onboarding-Option. Wenn Sie es beim Onboarding Ihres Accelerate-Kontos nicht erhalten haben, wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM), um es zu erhalten.

Empfehlungen zur Patch-Verantwortung

Der Patch-Prozess für persistente Instanzen sollte die folgenden Teams und Aktionen einbeziehen:

- Die Application (DevOps) -Teams definieren die Patchgruppen für ihre Server auf der Grundlage der Anwendungsumgebung, des Betriebssystemtyps oder anderer Kriterien. Sie definieren auch die Wartungsfenster, die für jede Patchgruppe spezifisch sind. Diese Informationen sollten auf Tags gespeichert werden, die an die Instanzen angehängt sind. Die empfohlenen Tag-Namen sind „Patch Group“ und „Maintenance Window“. Während jedes Patch-Zyklus bereiten sich die Anwendungsteams auf das Patchen vor, testen die Anwendung nach dem Patchen und beheben alle Probleme mit ihren Anwendungen und dem Betriebssystem während des Patchens.
- Das Security Operations Team definiert die Patch-Baselines für verschiedene Betriebssystemtypen, die von den Anwendungsteams verwendet werden, und stellt die Patches über Systems Manager Patch Manager zur Verfügung.
- Die automatisierte Patching-Lösung wird regelmäßig ausgeführt und stellt die in den Patch-Baselines definierten Patches auf der Grundlage der benutzerdefinierten Patch-Gruppen und Wartungsfenster bereit.
- Die Governance- und Compliance-Teams definieren Patching-Richtlinien sowie Ausnahmeverfahren und -mechanismen.

Weitere Informationen finden Sie unter Lösungsdesign für Patches für EC2 veränderbare Instanzen.

Anleitung für Anwendungsteams

- Machen Sie sich mit der Erstellung und Verwaltung von Wartungsfenstern vertraut. Weitere Informationen finden Sie unter AWS Systems Manager Wartungsfenster und SSM-Wartungsfenster für Patches erstellen. Wenn Sie die allgemeine Struktur und Verwendung von Wartungsfenstern

verstehen, können Sie besser verstehen, welche Informationen Sie bereitstellen müssen, wenn Sie nicht selbst die Person sind, die sie erstellt.

- Planen Sie für Hochverfügbarkeits-Setups (HA) ein Wartungsfenster pro Availability Zone und pro Umgebung ein (Dev/Test/Prod). Dadurch wird die kontinuierliche Verfügbarkeit während des Patchens gewährleistet.
- Die empfohlene Dauer des Wartungsfensters beträgt 4 Stunden mit einer Frist von 1 Stunde plus 1 zusätzliche Stunde pro 50 Instanzen
- Patchen Sie Entwicklungs- und Testversionen mit ausreichend Abstand zwischen den Versionen, damit Sie potenzielle Probleme vor dem Patchen in der Produktionsumgebung erkennen können.
- Automatisieren Sie allgemeine Aufgaben vor und nach dem Patchen mithilfe von SSM-Automatisierung und führen Sie sie als Aufgaben im Wartungsfenster aus. Beachten Sie, dass Sie für Aufgaben nach dem Patchen sicherstellen müssen, dass genügend Zeit zur Verfügung steht, da Aufgaben nicht gestartet werden, sobald der Grenzwert erreicht ist.
- Machen Sie sich mit Patch-Baselines und ihren Funktionen vertraut, insbesondere mit Verzögerungen bei der automatischen Genehmigung von Patch-Schweregradtypen, mit denen sichergestellt werden kann, dass nur die Patches, die in installiert wurden, zu einem späteren Zeitpunkt in der Dev/Test Produktion angewendet werden. Weitere Informationen finden Sie unter Über Patch-Baselines.

Hinweise für Teams für Sicherheitsoperationen

- Lesen Sie die Patch-Baselines und machen Sie sich mit ihnen vertraut. Die Patch-Genehmigung erfolgt automatisiert und verfügt über verschiedene Regeloptionen. Weitere Informationen finden Sie unter Über Patch-Baselines.
- Besprechen Sie die Anforderungen rund um das Patchen Dev/Test/Prod mit den Anwendungsteams und entwickeln Sie mehrere Baselines, um diesen Anforderungen gerecht zu werden.

Leitlinien für Governance- und Compliance-Teams

- Beim Patchen sollte es sich um eine Abmeldefunktion handeln. Ein standardmäßiges Wartungsfenster und automatisches Tagging sollten vorhanden sein, um sicherzustellen, dass nichts ungepatcht bleibt. AMS Resource Tagger kann Ihnen dabei helfen. Besprechen Sie diese Option mit Ihrem Cloud-Architekten (CA) oder Cloud Service Delivery Manager (CSDM), um sich bei der Implementierung beraten zu lassen.

- Anträge auf Befreiung vom Patching sollten Unterlagen enthalten, die die Ausnahme begründen. Ein Chief Information Security Officer (CISO) oder ein anderer Genehmigungsbeauftragter sollte den Antrag genehmigen oder ablehnen.
- Die Einhaltung der Patches sollte regelmäßig über die Patch Manager-Konsole, den Security Hub oder einen Schwachstellenscanner überprüft werden.

Beispieldesign für eine Windows-Anwendung mit hoher Verfügbarkeit

Überblick:

- Ein Wartungsfenster pro AZ.
- Ein Satz von Wartungsfenstern pro Umgebung.
- Eine Patch-Baseline pro Umgebung:
  - Entwickler: Genehmigen Sie alle Schweregrade und Klassifizierungen nach 0 Tagen.
  - Test: Genehmigen Sie kritische Sicherheitsupdates nach 0 Tagen und alle anderen Schweregrade und Klassifizierungen nach 7 Tagen.
  - Prod: Genehmigen Sie kritische Sicherheitsupdate-Patches nach 0 Tagen und alle anderen Schweregrade und Klassifizierungen nach 14 Tagen.

CloudFormation Skripte:

Diese Skripts werden eingerichtet, um die Wartungsfenster, Baselines und Patching-Aufgaben für eine Windows EC2 HA-Anwendung mit zwei Verfügbarkeitszonen unter Verwendung der oben beschriebenen Basisgenehmigungseinstellungen zu erstellen.

- Beispiel für einen CFN-Stack für Windows Dev: HA-Patching-dev-stack.json
- Beispiel für einen CFN-Stack für Windows-Tests: HA-Patching-Test-Stack.json
- Beispiel für einen Windows Prod-CFN-Stack: HA-Patching-Prod-Stack.json

Patch-Empfehlungen FAQs

F: Wie gehe ich mit ungeplanten Patches für Exploits am Tag 0 um?

A: SSM unterstützt eine Patch-Now-Funktion, die die aktuelle Standard-Baseline für das Betriebssystem der Instanz verwendet. AMS stellt einen Standardsatz von Patch-Baselines bereit, der alle Patches nach 0 Tagen genehmigt. Bei Verwendung der Funktion „Jetzt patchen“ wird jedoch kein Snapshot vor dem Patch erstellt, da mit diesem Befehl das RunPatchBaseline AWS-SSM-Dokument ausgeführt wird. Wir empfehlen, vor dem Patchen ein manuelles Backup zu erstellen.

F: Unterstützt AMS das Patchen für Instances in Auto-Scaling-Gruppen ()? ASGs

A: Nein. Derzeit wird ASG-Patching für Accelerate-Kunden nicht unterstützt.

F: Gibt es Einschränkungen für Maintenance Windows, die Sie beachten sollten?

A: Ja, es gibt einige Einschränkungen, die Sie beachten sollten.

- Wartungsfenster pro Konto: 50
- Aufgaben pro Wartungsfenster: 20
- Maximale Anzahl gleichzeitiger Automatisierungen pro Wartungsfenster: 20
- Maximale Anzahl gleichzeitiger Wartungsfenster: 5

Eine vollständige Liste der SSM-Standardgrenzwerte finden Sie unter AWS Systems Manager Endpunkte und Kontingente.

Erstellen Sie ein Patch-Wartungsfenster in AMS

In einem Patch-Wartungsfenster werden AMS-Patch-Automatisierungen nach einem festgelegten Zeitplan für bestimmte EC2 Amazon-Instances ausgeführt. Ziele werden durch ein oder mehrere Tags für eine Gruppe von Instances definiert. Sie können Zeitpläne festlegen, die auf Tagen und Uhrzeiten rund um den Patch Tuesday basieren, oder Sie können einen Zeitplan mithilfe eines Cron-Ausdrucks definieren. Weitere Informationen finden Sie im Benutzerhandbuch unter Referenz: Cron- und Rate-Ausdrücke für Systems Manager.AWS Systems Manager Vor dem Patchen erstellt AMS einen Snapshot des Root-Volumes jeder Instanz. Wenn AMS feststellt, dass sich das Patchen auf den Zustand der Instance auswirkt, oder wenn Sie AMS über die Auswirkungen des Patchens auf die Anwendung informieren, verwendet AMS diesen Snapshot, um das Root-Volume auf den Zustand vor dem Patch zurückzusetzen.

Zeitlimits für die Wartung von AMS Accelerate Patches

AMS-Patching-Anwendungen AWS Systems Manager (Systems Manager). Zusätzlich zu den Systems Manager Manager-Servicebeschränkungen gilt für AMS-Patching ein Limit von 300

Zielinstanzen pro Patch-Wartungsfenster. Bei einer allgemeinen Patch-Abschlusszeit von 30 Minuten pro Instanz enthält die folgende Tabelle Beispiele für die Anzahl und Dauer der Wartungsfenster.

Zu patchende Instanzen	Dauer der Wartungsfenster (Stunden)	Gleichzeitige Wartungsfenster erforderlich
100	1	1
200	1	1
300	2	1
600	3	2
800	4	3
1200	6	4
1500	8	5

> **Important**
>
> Bei diesen Beispielen wird davon ausgegangen, dass keine anderen Systems Manager Manager-Wartungsfenster aktiv sind und keine anderen Automatisierungen ausgeführt werden.

Weitere Informationen zu Grenzwerten finden Sie unter AWS Systems Manager Endpunkte und Kontingente.

Themen

- Ein wiederkehrendes „Patch Tuesday“ -Wartungsfenster von der AMS-Konsole aus erstellen (empfohlen)
- Erstellen Sie ein Patch-Wartungsfenster mit CloudFormation AMS Accelerate
- Erstellen Sie von der Systems Manager Manager-Konsole aus ein Wartungsfenster für AMS Accelerate

- Erstellen Sie ein Wartungsfenster mit der Systems Manager Manager-Befehlszeilenschnittstelle (CLI) für AMS Accelerate

Ein wiederkehrendes „Patch Tuesday“ -Wartungsfenster von der AMS-Konsole aus erstellen (empfohlen)

Microsoft veröffentlicht jeden zweiten Dienstag im Monat Patches für seine Betriebssysteme, auch bekannt als Patch Tuesday. Es ist üblich, Patches sowohl für Windows- als auch für Linux-Instanzen relativ zum Patch Tuesday zu planen. Um wiederkehrende Patch-Wartungsfenster für das erste oder zweite Wochenende nach dem Patch Tuesday zu planen, besuchen Sie die AMS-Konsole und gehen Sie wie folgt vor:

1. Geben Sie einen Namen für Ihr Patch-Wartungsfenster ein.
2. [optional] Geben Sie eine Beschreibung für das Patch-Wartungsfenster ein.
3. Wählen Sie einen Tag aus, der sich auf den Patch Tuesday bezieht.
4. Geben Sie im Format hh:mm eine Uhrzeit ein, zu der das Patch-Wartungsfenster beginnen soll. Beispiel: Mitternacht ist 00:00 Uhr und 23:00 Uhr ist 23:00 Uhr. Wählen Sie dann eine Zeitzone aus.
5. [optional] Passen Sie die Dauer an Ihre Bedürfnisse an. AMS empfiehlt eine Mindestdauer von vier Stunden.
6. Geben Sie einen Patch-Tag-Schlüssel und einen Wert für das Ziel ein. Weitere Informationen finden Sie unter Was sind Tags? .
7. [optional] Erweitern Sie die optionalen Parameter, um Parallelität, Fehlerrate und Wartungsfensterbegrenzung anzupassen.

    1. Durch Parallelität wird gesteuert, wie viele Ziel-Instances gleichzeitig gepatcht werden. Bei einer Parallelität von 50% für 10 Ziel-Instances werden beispielsweise nicht mehr als 5 Instances gleichzeitig gepatcht, während bei einer Parallelität von 100% alle 10 gleichzeitig gepatcht werden.
    2. Die Fehlerrate bestimmt die Toleranz für Fehler, bevor das Patchen unterbrochen wird. Bei einer Fehlerquote von 100% für 10 Ziel-Instances werden beispielsweise alle Instances gepatcht, unabhängig davon, wie viele ausfallen, während bei einer Fehlerquote von 50% das Patchen unterbrochen wird, sobald das Patchen bei 5 Instances fehlgeschlagen ist. AMS empfiehlt eine Fehlerquote von 100%.

3. Durch das Abschalten des Patch-Wartungsfensters wird eine Überschreitung des Patch-Wartungsfensters verhindert, indem der Start neuer Patching-Aktivitäten die angegebenen Stunden vor dem Ende des Patch-Wartungsfensters unterbrochen wird. Beispielsweise werden neue Patch-Aktivitäten eine Stunde vor dem Ende des Patch-Wartungsfensters eingestellt, wenn der Zeitraum für die Patch-Wartung auf 1 Stunde festgelegt wird (empfohlen).

> ⚠ Important
>
> Überprüfen Sie den Zeitpunkt der nächsten Ausführung.
> Rufen Sie die SSM-Wartungsfenster-Konsole auf, suchen Sie nach Ihrem neu erstellten Patch-Wartungsfenster und überprüfen Sie den Zeitpunkt der nächsten Ausführung. Wenn Sie Fragen haben oder Ihr Patch-Wartungsfenster bearbeiten möchten, erstellen Sie eine Serviceanfrage, um mit einem AMS-Patch-Experten zu sprechen

Informationen zur Planung eines CRON-basierten Patch-Wartungsfensters mithilfe von finden Sie unter CloudFormation. Erstellen Sie ein Patch-Wartungsfenster mit CloudFormation AMS Accelerate

Erstellen Sie ein Patch-Wartungsfenster mit CloudFormation AMS Accelerate

Um ein Wartungsfenster für AMS Accelerate-Patches mithilfe von zu erstellen AWS CloudFormation, melden Sie sich zunächst bei Ihrem Accelerate-Konto an und wählen Sie aus AWS-Region , wo sich Ihre Ziel-Instances befinden. Folgen Sie dann diesen Schritten auf der https://console.aws.amazon.com/cloudformation:

1. Wählen Sie eine von zwei benutzerdefinierten CloudFormation Accelerate-Patching-Vorlagen aus.

   - Planung von Patch Tuesday: Microsoft veröffentlicht Patches für seine Betriebssysteme am zweiten Dienstag im Monat, auch bekannt als Patch Tuesday, um Patch-Wartungsfenster am ersten oder zweiten Wochenende nach dem Patch Tuesday zu planen: Sobald Sie bei der Accelerate-Konsole angemeldet sind, verwenden Sie diese PatchTuesdayScheduling CloudFormation Linkvorlage.
   - CRON-Planung: Verwenden Sie diese CRONScheduling CloudFormation Linkvorlage, um Patch-Wartungsfenster mithilfe von CRON zu erstellen, um den Starttag zu definieren. Denken

Sie daran, dass Systems Manager CRON die Tage 1—7 nummeriert (Einzelheiten zu Systems Manager CRON finden Sie unter Referenz: Cron und Preisausdrücke für Systems Manager).

Wenn Sie einen dieser Links wählen, wird die Vorlage automatisch auf die Konsole geladen. CloudFormation Klicken Sie dann auf Next (Weiter).

2. Geben Sie auf der Seite „Stack-Details angeben“ (Schritt 2 der Seiten „Stack erstellen“) einen Stack-Namen und Vorlagenparameter ein (die angezeigten Standardparameter sind von AMS empfohlene Standardwerte. Wählen Sie Tag und Uhrzeit für Ihren Anwendungsfall aus). Klicken Sie auf Next, wenn Sie fertig sind.
3. Konfigurieren Sie die Stack-Optionen (optional). Informationen zu den Optionen finden Sie unter CloudFormation AWS-Stack-Optionen einrichten. Klicken Sie auf Next, wenn Sie fertig sind.
4. Überprüfen Sie Ihre Stack-Werte (optional). Informationen zur Überprüfung der Stack-Details zur Schätzung der Kosten finden Sie unter Überprüfung Ihres Stacks und Schätzung der Stack-Kosten. Wenn Sie fertig sind, klicken Sie auf Stack erstellen.

   Die Erstellung des Stacks kann bis zu einer Minute dauern. Sobald der Stack erfolgreich erstellt wurde, wird Ihr Patch-Wartungsfenster zur angegebenen Zeit ausgeführt. Sie können Änderungen an Ihrem Patch-Wartungsfenster vornehmen, indem Sie einen CloudFormation Änderungssatz erstellen und ausführen (empfohlen) (Einzelheiten dazu finden Sie unter Erstellen von Stacks mithilfe von Changesets) oder indem Sie das Patch-Wartungsfenster in der Konsole des Systems Manager Manager-Wartungsfensters aktualisieren (). https://console.aws.amazon.com/systems-manager/maintenance-windows

Sehen Sie sich das Video von Namrata an, um mehr zu erfahren (5:41)

Erstellen Sie von der Systems Manager Manager-Konsole aus ein Wartungsfenster für AMS Accelerate

Gehen Sie wie folgt vor, um von der Systems Manager Manager-Konsole aus ein AMS Accelerate-Wartungsfenster zu erstellen:

1. Klicken Sie in der linken Navigationsleiste im Bereich Änderungsmanagement auf Wartungsfenster und dann oben rechts auf dem Bildschirm auf Wartungsfenster erstellen. Füllen Sie das Formular aus. Einzelheiten zu den Optionen finden Sie unter Wartungsfenster (Konsole) erstellen. Wenn Sie fertig sind, klicken Sie auf Wartungsfenster erstellen.

Die Listenseite mit den Wartungsfenstern wird geöffnet.

2. Wählen Sie das neu erstellte Wartungsfenster aus.

   Die Detailseite des Wartungsfensters wird geöffnet.

3. Gehen Sie zur Registerkarte Ziele und wählen Sie Ziel registrieren.

   Die Seite Ziel registrieren wird geöffnet.

4. Fügen Sie Ihr Accelerate-Ziel hinzu. Informationen zu Zielen finden Sie unter Zuweisen von Zielen zu einem Wartungsfenster (Konsole). Wenn Sie fertig sind, klicken Sie auf Ziel registrieren. Notieren Sie sich das Ziel, wenn Sie es später benötigen.

   Die Detailseite des Wartungsfensters wird auf der Registerkarte Ziele erneut geöffnet. Sie enthält eine Liste, die das neue Ziel enthält.

5. Wählen Sie auf der Registerkarte Aufgaben der Detailseite des Wartungsfensters die Option Aufgabe registrieren und wählen Sie dann in der Dropdownliste die Option Automatisierungsaufgabe registrieren aus. Füllen Sie das Formular aus. Beschleunigen Sie Ihre Notizen:

   - Geben Sie einen aussagekräftigen Namen für die Aufgabe ein. Zum Beispiel: AcceleratePatch.
   - Klicken Sie im Bereich Automation-Dokumente in das Suchfeld, wählen Sie Eigentümer und dann Geteilte Dokumente aus.
   - Wählen Sie das Automatisierungsdokument aus, indem Sie in das Suchfeld klicken und das Präfix für den Dokumentnamen --> Gleich wählen und dann Folgendes eingeben: AWSManagedServices-PatchInstance. Wählen Sie dann das AWSManagedServices-PatchInstanceDokument aus, indem Sie das entsprechende Optionsfeld auswählen.
   - Wählen Sie unter Dokumentversion die Option Standardversion zur Laufzeit aus.
   - Gehen Sie im Abschnitt Ziele wie folgt vor:
     - Setzen Sie Ziel durch: auf Auswahl registrierter Zielgruppen.
     - Wählen Sie in der Liste der Ziele das Ziel aus, das Sie auf der Registerkarte Ziele registriert haben.
   - Füllen Sie im Abschnitt Eingabeparameter das Formular aus.
     - InstanceId: `{{TARGET_ID}}`
     - StartInactiveInstances: `True` um die Instanzen zu starten, wenn sie während des Patch-Wartungsfensters gestoppt werden.

> **Note**
>
> Beim InstanceIdParameterwert wird zwischen Groß- und Kleinschreibung unterschieden, und der StartInactiveInstancesParameterwert kann entweder True oder False sein.
> Gestoppte Instanzen können nicht gestartet werden, wenn sie von Tags als Ziel ausgewählt wurden. Weitere Informationen finden Sie unter Keine Aufrufe zur Ausführung.

- Wählen Sie im Bereich Ratensteuerung die Option Prozentsätze aus. AMS Accelerate empfiehlt 100% für Parallelität und 100% für den Schwellenwert für Fehler, um zu versuchen, alle Instanzen gleichzeitig zu patchen, unabhängig von Automatisierungsfehlern. Wenn Sie die Hälfte Ihrer Ziele gleichzeitig patchen möchten, um beispielsweise die Hälfte der Ziel-Instances hinter einem Load-Balancing laufen zu lassen, legen Sie Parallelität auf 50% fest.
- Wählen Sie im Abschnitt IAM-Servicerolle die Option Benutzerdefinierte Servicerolle verwenden und anschließend ams_ssm_automation_role aus.

Klicken Sie auf Automatisierungsaufgabe registrieren.

Das Wartungsfenster für das Patchen wird erstellt. Auf der Registerkarte Beschreibung können Sie den Zeitpunkt der nächsten Ausführung sehen.

Erstellen Sie ein Wartungsfenster mit der Systems Manager Manager-Befehlszeilenschnittstelle (CLI) für AMS Accelerate

Um ein AMS Accelerate-Wartungsfenster mit der Befehlszeilenschnittstelle zu erstellen:

1. Folgen Sie dem SSM-Tutorial: Ein Wartungsfenster erstellen und konfigurieren (AWS CLI). Für jeden Schritt des Tutorials finden Sie hier Beispiele für CLI-Befehle zum Patchen.

> **Note**
>
> Diese Beispiele sind spezifisch für Linux oder macOS. Die Befehle können auch ausgeführt werden AWS CloudShell , was möglicherweise einfacher ist als die

Konfiguration `awscli` auf einem lokalen Computer. Einzelheiten finden Sie unter Arbeiten mit AWS CloudShell.

a. Gehen Sie in Schritt 1 des Tutorials wie folgt vor, um ein Wartungsfenster zu erstellen:

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

Bei erfolgreichem Abschluss `window-id` wird zurückgegeben.

b. Gehen Sie in Schritt 2 des Tutorials wie folgt vor, um einen Zielknoten zu registrieren:

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

Bei erfolgreichem Abschluss werden `WindowTargetID` s zurückgegeben.

c. Gehen Sie in Schritt 3 des Tutorials wie folgt vor, um eine Aufgabe zu registrieren:

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

Aufnäher mit Haken

Mithilfe von AMS-Patch-Hooks können Sie AMS-Patching so konfigurieren, dass Befehle auf Betriebssystemebene (OS) vor und nach dem Patchen ausgeführt werden. Verwenden Sie AMS-Patch-Hooks, um SSM-Befehlsdokumente auszuführen, um einen Dienst vor dem Patchen zu beenden und dann den Dienst nach dem Patchen zu starten, oder um Befehle auszuführen, um zu überprüfen, ob Ihre Anwendung nach dem Patchen fehlerfrei ist.

Um AMS-Patch-Hooks zu verwenden, müssen Sie wie folgt vorgehen:

1. Erstellen Sie SSM-Befehlsdokumente, die als Patch-Hooks verwendet werden sollen.
2. Erstellen Sie ein AMS-Patch-Wartungsfenster oder verwenden Sie ein vorhandenes AMS-Patch-Wartungsfenster. Einzelheiten finden Sie unter AMS-Patch-Wartungsfenster.
3. Konfigurieren Sie ein AMS-Patch-Wartungsfenster, um Ihre SSM-Befehlsdokumente für AMS-Patch-Hooks zu verwenden.

AMS-Patch-Hooks (RACI)

In der Matrix „Verantwortliche, Rechenschaftspflichtige, Konsultierte und Informierte“ (RACI) wird entweder dem Kunden oder AMS die Hauptverantwortung für eine Vielzahl von Aktivitäten zugewiesen. Die folgende Tabelle bietet einen Überblick über die Zuständigkeiten von Kunde und AMS für Aktivitäten in einer Anwendung, die AMS-Patchhooks verwendet.

- R steht für die verantwortliche Partei, die die Arbeit zur Erfüllung der Aufgabe erledigt
- A steht für die verantwortliche Partei
- C steht für konsultiert, also für die Partei, deren Meinung eingeholt wird, in der Regel als Fachexperten, und mit der ein bilateraler Austausch besteht
- I steht für informiert, d. h. die Partei, die über den Fortschritt informiert wird, oft erst nach Abschluss der Aufgabe oder des Liefergegenstands

Aktivität	Customer	AMS
Erstellen Sie das pre/post Patch-SSM-Befehlsdokument und den Dokumentinhalt	R	C

Aktivität	Customer	AMS
Konfigurieren Sie Patch-Hook-Parameter für AMS-Patching	R	C
Führen Sie das SSM-Befehlsdokument „ pre/post Patch“ aus	I	R
Suchen Sie nach Patch-Hook-Fehlern und reagieren Sie darauf	I	R
Informieren Sie den Kunden über den Ausfall eines Patch-Hooks	I	R
Rollback zu einem Status vor dem Patch, falls vom Kunden gewünscht	C	R

Erstellen Sie SSM-Dokumente für Patch-Hooks

AMS-Patch-Hooks verwenden beim Patchen Amazon EC2 Systems Manager (SSM) -Dokumente. Erstellen Sie ein SSM-Befehlsdokument oder geben Sie ein vorhandenes SSM-Befehlsdokument für das Konto frei, in dem das Patchen ausgeführt wird. Informationen zu SSM-Dokumenten, einschließlich Einschränkungen, finden Sie unter SSM-Dokumente teilen.

Gehen Sie folgendermaßen vor, um ein SSM-Befehlsdokument zu erstellen:

1. Erstellen Sie ein SSM-Dokument mit Document Type = „Command“.
2. Geben Sie Ihre Befehle im Bereich Inhalt ein. Weitere Informationen finden Sie unter SSM-Dokumentinhalte erstellen.

> **Note**
>
> SSM-Dokumente für AMS-Patch-Hooks können auch mit AWS CLI oder erstellt werden. CloudFormation Wenn Sie Unterstützung bei der Erstellung von SSM-Dokumenten für Ihre AMS-Patch-Hooks benötigen, wenden Sie sich an Ihren Cloud-Architekten.

Konfigurieren Sie das AMS-Patch-Wartungsfenster so, dass Ihre SSM-Befehlsdokumente als AMS-Patch-Hooks verwendet werden

Ein AMS-Patch-Wartungsfenster ist ein Systems Manager Manager-Wartungsfenster, das Ihre konfigurierte AMS-Patch-Automatisierung ausführt.

Gehen Sie folgendermaßen vor, um ein AMS-Patch-Wartungsfenster so zu bearbeiten, dass Patch-Hooks verwendet werden:

1. Wählen Sie im linken Navigationsbereich unter Change Management Tools die Option Maintenance Windows aus. https://console.aws.amazon.com/systems-manager/

   Eine Seite mit den vorhandenen Wartungsfenstern wird geöffnet.
2. Wählen Sie eine Fenster-ID, die mit mw- beginnt.

   Die Detailseite für dieses Wartungsfenster wird geöffnet.
3. Wählen Sie die Registerkarte Aufgaben und das Fenster Task-ID mit dem Task-ARN von AMS-PatchInstance und klicken Sie auf Bearbeiten.

4. Scrollen Sie nach unten zum Abschnitt Parameter und aktualisieren Sie die folgenden Parameter.

AMS-Patch-Hook-Parameter:

- PrePatchHook: Der Name des SSM-Dokuments vom Typ „Command“, das Sie vor dem Patchen ausführen möchten. Lassen Sie dieses Feld leer oder geben Sie „AWS-noop“ (Groß- und Kleinschreibung beachten) ein, wenn Sie vor dem Patchen keinen Befehl ausführen.
- PostPatchHook: Der Name des SSM-Dokuments vom Typ „Command“, das Sie nach dem Patchen ausführen möchten. Lassen Sie dieses Feld leer oder geben Sie „AWS-noop“ (Groß- und Kleinschreibung beachten) ein, wenn Sie nach dem Patchen keinen Befehl ausführen.

- ExecutePatchBasedOnPreHookStatus: Führen Sie das Patchen je nach Erfolg oder Misserfolg des Laufs aus. Wählen Sie eine Option aus: PrePatchHook
  - OnPreHookSuccess: Führen Sie die AMS-Patch-Automatisierung nur aus, wenn der erfolgreich PrePatchHook ist.
  - Immer: Führen Sie die AMS-Patch-Automatisierung aus, wenn die erfolgreich PrePatchHook ist und wenn sie fehlschlägt.
  - OnPreHookFailure- Führen Sie die AMS-Patch-Automatisierung nur aus, wenn sie PrePatchHook fehlschlägt.
  - Niemals: Führen Sie die AMS-Patch-Automatisierung nicht aus. Dies kann nützlich sein, wenn Sie Ihre testen PrePatchHook.
- ExecutePostHookBasedOnPatchStatus: Führen Sie den Post-Patch-Hook je nach Erfolg oder Misserfolg der AMS-Patch-Automatisierung aus. Wählen Sie einen aus:
  - OnPatchSuccess: Führen Sie den nur aus PostPatchHook , wenn die AMS-Patch-Automatisierung erfolgreich ausgeführt wurde.
  - Immer: Führen Sie den aus PostPatchHook , wenn die AMS-Patch-Automatisierung erfolgreich ist und wenn sie fehlschlägt.
  - OnPatchFailure- PostPatchHook Nur ausführen, wenn die AMS-Patch-Automatisierung fehlschlägt.

> **Note**
>
> Wenn bei einer dieser Variablen das Textfeld fehlt, beheben Sie das Problem, indem Sie auf derselben Seite zum Abschnitt mit dem Automatisierungsdokument blättern, ein anderes Dokument auswählen und dann das Originaldokument erneut auswählen. Dadurch werden die Eingabeparameter aktualisiert, sodass Sie sie bearbeiten können.

AMS Accelerate-Patch-Baseline

Eine Patch-Baseline definiert, welche Patches für die Installation in Ihren Instances genehmigt sind. Sie können für Patches einzeln angeben, ob sie genehmigt oder abgelehnt werden. Sie können auch automatische Genehmigungsregeln erstellen, um festzulegen, dass bestimmte Arten von Updates (z. B. wichtige Updates), automatisch genehmigt werden. Die Liste mit den Ablehnungen setzt sowohl die Regeln als auch die Liste mit Genehmigungen außer Kraft.

Standard-Patch-Baseline

Wenn Sie das AMS Accelerate-Patching verwenden, werden die Standard-Patch-Baselines von den AMS Accelerate-Standard-Patch-Baselines für die folgenden Betriebssysteme außer Kraft gesetzt.

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

> **Important**
>
> Standard-Patch-Baselines werden von AMS verwaltet. Bearbeiten Sie keine Standard-Patch-Baselines, da Ihre Änderungen möglicherweise verloren gehen. Erstellen Sie stattdessen eine benutzerdefinierte Patch-Baseline. Siehe Benutzerdefinierte Patch-Baseline mit AMS Accelerate

> **Note**
>
> Die als Produkt = * definierten AMS Accelerate-Patch-Baselines bedeuten, dass alle Patches auf die Instance aller Sicherheits- und Klassifizierungen angewendet werden.

Benutzerdefinierte Patch-Baseline mit AMS Accelerate

Um eine benutzerdefinierte Patch-Baseline mit AMS Accelerate zu verwenden, stellen Sie zunächst sicher, dass Sie über eine Patchgruppe verfügen, und erstellen Sie dann die benutzerdefinierte Baseline.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Mit Patchgruppen arbeiten

- Erstellen einer benutzerdefinierten Patch-Baseline (Windows)
- Erstellen einer benutzerdefinierten Patch-Baseline (Linux)
- Aktualisieren oder Löschen einer benutzerdefinierten Patch-Baseline (Konsole)

Erstellen einer IAM-Rolle für On-Demand-Patching von AMS Accelerate

Nachdem Ihr Konto in AMS Accelerate-Patching integriert wurde, stellt AMS Accelerate eine verwaltete Richtlinie, amspatchmanagedpolicy, bereit. Diese Richtlinie enthält die erforderlichen Berechtigungen für On-Demand-Patching mithilfe des AMS-Automatisierungsdokuments. `AWSManagedServices-PatchInstance` Um dieses Automatisierungsdokument verwenden zu können, erstellt der Kontoadministrator eine IAM-Rolle für Benutzer. Dazu gehen Sie wie folgt vor:

Erstellen Sie eine Rolle mit dem AWS-Managementkonsole:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich der Konsole Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie den AWS-Konto Rollentyp „Anderer“.
4. Geben Sie unter Konto-ID die AWS Konto-ID ein, der Sie Zugriff auf Ihre Ressourcen gewähren möchten.

   Der Administrator des angegebenen Kontos kann die Berechtigung erteilen, diese Rolle für alle IAM-Benutzer in diesem Konto zu übernehmen. Zu diesem Zweck fügt der Administrator dem Benutzer oder einer Gruppe eine Richtlinie zu, die die Berechtigung für die sts: AssumeRole -Aktion erteilt. In dieser Richtlinie muss der Amazon-Ressourcenname (ARN) der Rolle als Ressource angegeben werden. Beachten Sie Folgendes:

   - Wenn Sie Benutzern über ein Konto, das Sie nicht kontrollieren, Berechtigungen gewähren und die Benutzer diese Rolle programmgesteuert übernehmen, wählen Sie „Externe ID erforderlich“. Die externe ID kann ein beliebiges Wort oder eine beliebige Zahl sein, das bzw. die zwischen Ihnen und dem Administrator des Drittanbieter-Kontos vereinbart wurde. Diese Option fügt der Vertrauensrichtlinie automatisch eine Bedingung hinzu, die es dem Benutzer ermöglicht, die Rolle nur dann anzunehmen, wenn die Anfrage die richtige sts:ExternalID enthält. Weitere Informationen finden Sie unter So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren.

- Wenn Sie die Rolle auf Benutzer beschränken möchten, die sich mit Multi-Factor Authentication (MFA) anmelden, wählen Sie Require MFA. Dadurch wird eine Bedingung zur Vertrauensrichtlinie der Rolle hinzugefügt, mit der geprüft wird, ob eine MFA-Anmeldung vorliegt. Ein Benutzer, der die Rolle übernehmen möchte, muss sich über ein konfiguriertes MFA-Gerät mit einem temporären einmaligen Passwort anmelden. Benutzer ohne MFA-Authentifizierung können die Rolle nicht übernehmen. Weitere Informationen zu MFA finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in. AWS

5. Wählen Sie Weiter: Berechtigungen aus.

   IAM enthält eine Liste von Richtlinien im Konto. Geben Sie unter Berechtigungen hinzufügen den Text amspatchmanagedpolicy in das Filterfeld ein und aktivieren Sie das Kontrollkästchen für diese Berechtigungsrichtlinie. Klicken Sie auf Weiter.

6. Geben Sie unter Rollendetails einen Rollennamen ein, z. B. PatchRole fügen Sie eine Beschreibung für die Rolle hinzu (empfohlen) und fügen Sie auch Tags hinzu, mit denen Sie diese Rolle leichter identifizieren können. Bei Rollennamen wird nicht zwischen Groß- und Kleinschreibung unterschieden, sie müssen jedoch innerhalb von eindeutig sein AWS-Konto. Wenn Sie fertig sind, klicken Sie auf Rolle erstellen.

   > **Note**
   >
   > Rollennamen können nicht bearbeitet werden, nachdem sie erstellt wurden.

Verstehen Sie Patch-Benachrichtigungen und Patch-Fehler in AMS Accelerate

> **Important**
>
> Ab dem 1. Februar 2025 erhalten AMS-Kunden in ihren verwalteten Konten keine Benachrichtigungen mehr, wenn das Fenster zur Patch-Wartung leer ist.

Patch-Serviceanfragen und E-Mail-Benachrichtigungen

AMS erstellt vier Tage vor dem nächsten Patch-Wartungsfenster eine neue Serviceanfrage. Vier Tage vor der Ausführung eines Patch-Wartungsfensters mit dem Namen App1 PROD erstellt AMS

beispielsweise eine Serviceanfrage mit dem Titel April Patch Maintenance Window for App1 Prod for Account [Account-ID]. Verwenden Sie die Patch-Serviceanfrage, um mit AMS zu kommunizieren, falls Sie Anpassungen an Ihrem geplanten Patch benötigen, oder um einen bevorstehenden Patch zu überspringen. Wenn eine Serviceanfrage erstellt wird, wird eine E-Mail mit einem Link zur Serviceanfrage an Ihre Patch-Benachrichtigungsadresse gesendet. Sie erhalten jedes Mal, wenn AMS die Serviceanfrage aktualisiert, eine zusätzliche E-Mail.

> **Note**
>
> AMS erstellt eine neue Serviceanfrage, auch wenn das Patch-Wartungsfenster weniger als vier Tage vor der geplanten Ausführung erstellt wird.
> Das Patch-Wartungsfenster muss den Status „Aktiviert“ haben, um Benachrichtigungen über Serviceanfragen empfangen zu können.

Eine Stunde vor Beginn des Patches benachrichtigt AMS Sie über die Patch-Serviceanfrage. Nach Abschluss des Patches aktualisiert AMS die Patchdienstanforderung mit einem Link zur Patch Manager-Konsole. Verwenden Sie den Link, um die Patch-Konformität für die Instanzen einzusehen, auf die das Patch-Wartungsfenster abzielt.

> **Note**
>
> Die Links in der Patch Manager-Konsole zeigen die aktuelle Konformität der Instanzen. Patch Manager zeigt eine Instanz als nicht konform an, wenn zwischen dem Abschluss des Patches durch AMS und dem Zugriff auf den Link neue Patches veröffentlicht werden.

Patch-Benachrichtigungen über Ereignisse CloudWatch

AMS sendet während des Patch-Vorgangs dreimal CloudWatch Ereignisse, darunter die folgenden:

- Vier Tage, bevor das Patch-Wartungsfenster läuft.
- Eine Stunde, bevor das Patch-Wartungsfenster läuft.
- Wenn das Patch-Wartungsfenster abgeschlossen ist.

Im Folgenden finden Sie das Ereignisschema für erweiterte Benachrichtigungen im Patch-Wartungsfenster:

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

In der folgenden Tabelle wird das Ereignisschema für die Vorankündigung im Fenster „Patch Maintenance“ beschrieben:

Einzelheiten der Patch-Benachrichtigung

Name der Eigenschaft	Beschreibung	Beispielwerte
Zustand	Der Status des Wartungsfensters für das Patchen	PRÄVENTIV — Das Patch-Zeitfenster soll in Kürze beginnen
Status	Der Status des Wartungsfensters für das Patchen	ERFOLGREICH — Alle Instanzen wurden ohne Fehler gepatcht FEHLGESCHLAGEN — Mindestens eine Instanz konnte nicht gepatcht werden

Name der Eigenschaft	Beschreibung	Beispielwerte
StartTime	Die Startzeit des Wartungsfensters für das Patchen im ISO-Format	2021-02-03T 22:14:05.814 308
WindowArn	Die eindeutige Kennung des Patching-Wartungsfensters	arn:aws:ssm:us-east-1:12345 6789012:maintenancewindow/ mw-00000001235
Ergebnisse	Die Liste der Instanzen, auf die das Patch-Fenster abzielt	InstanceId — die Instanz-ID der Zielinstanz

Im Folgenden finden Sie das Endereignisschema für das Patch-Wartungsfenster:

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

In der folgenden Tabelle wird das Endereignisschema des Patch-Wartungsfensters beschrieben:

Einzelheiten zum Ende des Patchfensters

Name der Eigenschaft	Beschreibung	Beispielwerte
Zustand	Der Status des Wartungsfensters für das Patchen	ABGESCHLOSSEN — Das Patch-Fenster ist beendet
Status	Der Status des Wartungsfensters für das Patchen	ERFOLGREICH — Alle Instanzen wurden ohne Fehler gepatcht FEHLGESCHLAGEN — Mindestens eine Instanz konnte nicht gepatcht werden
StartTime	Die Startzeit des Wartungsfensters für das Patchen im ISO-Format	2021-02-03T 22:14:05.814 308
EndTime	Die Endzeit des Wartungsfensters für das Patchen im ISO-Format	2021-02-03T 23:14:05.814 308
WindowArn	Die eindeutige Kennung des Wartungsfensters für das Patchen.	arn:aws:ssm:us-east-1:12345 6789012:maintenancewindow/ mw-00000001235
WindowExecutionId	Die Ausführungs-ID des Fensters, die in der SSM Maintenance Window Console eingesehen werden kann	e32088eb-c05f-4c63- b766-6866e163c818
Ergebnisse	Die Liste der Instances, auf die das Patch-Fenster abzielt	InstanceId — die Zielinstanz-ID Status — der Patch-Status der Instanz

Name der Eigenschaft	Beschreibung	Beispielwerte
		missing_critical_patch_count — die Anzahl der fehlenden kritischen Patches auf der Instanz missing_total_patch_count — die Anzahl der gesamten fehlenden Patches auf der Instanz

Sie können das Ereignis CloudWatch Ereignisse verwenden, um eine CloudWatch Regel auszulösen, die Sie benachrichtigt, wenn eine Vorankündigung für das Patching Maintenance Window gesendet wird. Konfigurieren Sie dazu die CloudWatch Regel mit der folgenden Konfiguration:

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **Note**
>
> Patch-Fehlerwarnungen werden nicht für Instanzen erstellt, deren Betriebssysteme nicht unterstützt werden oder die während des Wartungsfensters gestoppt werden.

Untersuchung von Patch-Fehlern in AMS

AWS Managed Services (AMS) verwaltet das Patchen und umfasst die Behebung von Patch-Fehlern. Schlägt das Patchen fehl, wird AMS Operations benachrichtigt und versucht, das Problem mithilfe der folgenden AWS und bewährten AMS-Methoden zu beheben.

<instance-id>Wenn ein Patch fehlschlägt, erstellt AMS OpsItem im Konto ein SSM mit dem folgenden Titel: AWS Managed Services — Patch Instance failure zum Beispiel.

AMS untersucht dann das. OpsItem Wenn AMS den Fehler ohne Ihr Zutun beheben kann, behebt AMS das Problem. OpsItem Wenn Ihr Eingreifen erforderlich ist, benachrichtigt AMS Sie in einer Serviceanfrage, die die Untersuchungsergebnisse und die empfohlenen Schritte zur Behebung enthält. Wenn Sie keine Maßnahmen zur Behebung des Problems ergreifen, versucht AMS, die Instance während des nächsten geplanten Patch-Wartungsfensters zu patchen.

> **Note**
>
> Patch-Fehler OpsItems werden nicht für Instances verursacht, deren Betriebssysteme nicht unterstützt werden oder die sich während des Patch-Wartungsfensters im Status Gestoppt befinden.

Kostenoptimierung mit AMS Resource Scheduler

Die AMS Resource Scheduler AWS on-Lösung hilft Ihnen dabei, Ihre AWS und AMS-Kosten zu senken, indem Ressourcen, die nicht genutzt werden, gestoppt und Ressourcen gestartet werden, wenn Kapazität benötigt wird. Sie können AMS Resource Scheduler beispielsweise AWS in einer Entwicklungsumgebung verwenden, um täglich automatisch Instanzen außerhalb der Geschäftszeiten zu stoppen. Wenn Sie alle Ihre Instances mit voller Auslastung laufen lassen, kann diese Lösung zu einer Verringerung der Instanzauslastung führen, was die Gesamtkosten auf der Grundlage der von Ihnen konfigurierten Zeitpläne senkt.

Verwenden Sie den AWS Managed Services (AMS) Resource Scheduler, um den automatischen Start und Stopp von Auto Scaling Scaling-Gruppen, EC2 Amazon-Instances und Amazon RDS-Instances in Ihrem Konto zu planen. Dies trägt dazu bei, die Infrastrukturkosten dort zu senken, wo die Ressourcen nicht rund um die Uhr laufen sollen. Die Lösung basiert auf AWS Instance Scheduler, enthält jedoch zusätzliche Funktionen und Anpassungen, die speziell auf die Bedürfnisse von AMS-Kunden zugeschnitten sind. Die Anpassung umfasst Unterstützung für die Planung von Auto Scaling Scaling-Gruppen, CloudWatch Alarmunterdrücker für Elastic Load Balancing Balancing-Alarme, Unterstützung für mehrere AWS Systems Manager Wartungsfenster für Amazon EC2, eine Kosteneinsparungsschätzung und Betriebsunterstützung durch AMS.

AMS Resource Scheduler verwendet Perioden und Zeitpläne. Perioden definieren die Zeiten, zu denen die Ressource ausgeführt werden soll, z. B. Startzeit, Endzeit und Tage des Monats. Zeitpläne enthalten Ihre definierten Zeiträume zusammen mit zusätzlichen Konfigurationen (SSM-Wartungsfenster, Zeitzone, Ruhezustand usw.) und geben an, wann Ressourcen ausgeführt werden sollen. Sie können diese Zeiträume und Zeitpläne mithilfe von von AMS bereitgestellter Automatisierungs-Runbooks konfigurieren. AWS Systems Manager Jeder Zeitplan muss mindestens einen Zeitraum enthalten, der die Zeit (en) definiert, zu der die Instance ausgeführt werden soll. Ein Zeitplan kann mehr als einen Zeitraum enthalten. Wenn mehr als ein Zeitraum in einem Zeitplan verwendet wird, wendet der Instance Scheduler die entsprechende Startaktion an, wenn mindestens eine der Periodenregeln zutrifft. Weitere Informationen zu Zeitplan und Zeiträumen finden Sie unter Lösungskomponenten von AWS Instance Scheduler.

AMS Resource Scheduler verwendet AWS Ressourcen-Tags, um einer oder mehreren Ressourcen einen Zeitplan zuzuordnen, um sie gezielt für geplante Start- und Stoppaktionen zu verwenden. Sie taggen Ihre Ressourcen mit dem Tag-Schlüssel (Standard ist`Schedule`), der im Scheduler konfiguriert ist und den Namen des Zeitplans als Wert hat. Sie konfigurieren denselben Tag-Schlüssel

wie das Tag AWS Cost Explorer für die Kostenzuweisung in der Kostenkalkulationsfunktion von Scheduler, um Kosteneinsparungen nachzuverfolgen und Berichte darüber zu erstellen.

AMS Resource Scheduler ist eine Opt-in-Funktion, die Sie pro Konto aktivieren können.

Ressourcen mit AMS Resource Scheduler verwenden

Amazon EC2

- EC2 Amazon-Instances, die Teil einer Auto Scaling Scaling-Gruppe sind, werden nicht einzeln verarbeitet und vom AMS Resource Scheduler übersprungen, auch wenn sie markiert sind.
- Wenn das Root-Volume der Ziel-Instance mit einem AWS KMS Customer Master Key (CMK) verschlüsselt ist, muss Ihrer Resource Scheduler IAM-Rolle eine zusätzliche `kms:CreateGrant` Berechtigung hinzugefügt werden, damit der Scheduler solche Instances starten kann. Diese Berechtigung wird der Rolle standardmäßig nicht hinzugefügt, um die Sicherheit zu erhöhen. Wenn Sie diese Berechtigung benötigen, können Sie die Berechtigung hinzufügen, `ams-resource-scheduler` indem Sie den CloudFormation Stack mit einer Liste von CMK als Wert für den `UseCMK` Parameter aktualisieren (verwenden Sie einen oder mehrere CMK-Schlüssel ARNs im Format `arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`* anstelle eines KMS-Alias).
- Wenn Ihre EC2 Amazon-Instances mit einer bestimmten Software konfiguriert sind oder Herstellerlizenzen von verwaltet werden AWS License Manager, benötigt Resource Scheduler Berechtigungen für die jeweiligen AWS License Manager Lizenzen, um die Instance starten zu können. Sie können Resource Scheduler die erforderlichen Berechtigungen gewähren, indem Sie die Liste der ARN (s) der AWS License Manager Lizenzen zur License Manager-Lizenz für den EC2 Instanzparameter des CloudFormation Stacks hinzufügen (`ams-resource-scheduler`).

Amazon EC2 Auto Scaling

- AMS Resource Scheduler startet oder stoppt die Auto Scaling von Auto Scaling-Gruppen, nicht von einzelnen Instances in der Gruppe. Das heißt, der Scheduler stellt die Größe der Auto Scaling Scaling-Gruppe wieder her (Start) oder setzt die Größe auf 0 (Stopp).
- Kennzeichnen Sie die Auto Scaling Scaling-Gruppe mit dem angegebenen Tag und nicht die Instances innerhalb der Gruppe.
- Während des Stopps speichert AMS Resource Scheduler die minimalen, gewünschten und maximalen Kapazitätswerte der Auto Scaling Scaling-Gruppe und setzt die Minimal- und Gewünschte Kapazität auf 0. Während des Starts stellt der Scheduler die Auto Scaling Scaling-

Gruppengröße wieder her, wie sie beim Stopp war. Daher müssen Auto Scaling Scaling-Gruppeninstanzen eine geeignete Kapazitätskonfiguration verwenden, damit die Beendigung und der Neustart der Instances keine Auswirkungen auf Anwendungen haben, die in der Auto Scaling Scaling-Gruppe ausgeführt werden.

- Wenn die Auto Scaling Scaling-Gruppe während einer Laufzeit geändert wird (die minimale oder maximale Kapazität), speichert der Scheduler die neue Auto Scaling Scaling-Gruppengröße und verwendet sie, wenn die Gruppe am Ende eines Stopp-Zeitplans wiederhergestellt wird.

Amazon RDS

- Der Scheduler kann vor dem Stoppen der RDS-Instances einen Snapshot erstellen (gilt nicht für den Aurora-DB-Cluster). Diese Funktion ist standardmäßig aktiviert, wobei der CloudFormation AWS-Vorlagenparameter Create RDS Instance Snapshot auf true gesetzt ist. Der Snapshot wird aufbewahrt, bis die Amazon RDS-Instance das nächste Mal gestoppt und ein neuer Snapshot erstellt wird.
- Scheduler kann start/stop Amazon RDS-Instances verwenden, die Teil eines Clusters oder einer Amazon RDS Aurora-Datenbank sind oder sich in einer Multi-AZone-Konfiguration (Multi-AZ) befinden. Überprüfen Sie jedoch die Amazon RDS-Beschränkung, wenn der Scheduler die Amazon RDS-Instance, insbesondere Multi-AZ-Instances, nicht stoppen kann.
- Verwenden Sie den Vorlagenparameter Schedule Aurora Clusters, um Aurora Cluster für den Start oder Stopp zu planen (der Standardwert ist true). Der Aurora-Cluster (nicht die einzelnen Instances innerhalb des Clusters) muss mit dem Tag-Schlüssel, der bei der Erstkonfiguration definiert wurde, und dem Zeitplannamen als Tag-Wert für die Planung dieses Clusters gekennzeichnet werden.

> **Note**
>
> Der Resource Scheduler überprüft nicht, ob eine Ressource gestartet oder gestoppt wurde. Er ruft die API für den entsprechenden Dienst auf und fährt fort. Wenn der API-Aufruf fehlschlägt, wird der Fehler zur Untersuchung protokolliert.
> AMS Resource Scheduler unterstützt AWS Backup Windows nicht. Wenn Sie eine RDS-Instance mit AWS Backup aktiviertem Resource Scheduler-Zeitplan zuordnen, muss das Backup-Fenster innerhalb des laufenden Zeitplans liegen, damit das Backup erwartungsgemäß funktioniert.

Einführung in AMS Resource Scheduler

Ihr Konto wird nicht automatisch in AMS Resource Scheduler integriert, wenn Ihr Konto in den AMS Accelerate-Betriebsplan aufgenommen wird. Im Rahmen der Kontoeinbindung in den AMS Accelerate-Betriebsplan oder jederzeit danach können Sie Ihren Cloud Service Delivery Manager (CSDM) jedoch bitten, das Konto in AMS Resource Scheduler zu integrieren. Sobald Ihr CSDM das Konto eingerichtet hat, wird Ihrem Konto automatisch ein CloudFormation Stapel mit AMS Resource Scheduler-Ressourcen mit Standardkonfiguration zugewiesen.

Nachdem der AMS Resource Scheduler in Ihrem Konto bereitgestellt wurde, empfehlen wir Ihnen, die Standardkonfiguration zu überprüfen und bei Bedarf Konfigurationen wie Tag-Schlüssel, Zeitzone, geplante Dienste usw. an Ihre Präferenzen anzupassen. Einzelheiten zu den empfohlenen Anpassungen finden Sie unter Weiter. AMS Resource Scheduler anpassen

AMS Resource Scheduler anpassen

Nach dem Onboarding wird AMS Resource Scheduler als CloudFormation Stack mit Namen `ams-resource-scheduler` in der primären AWS-Region für Ihr AMS Accelerate-Konto bereitgestellt. Sie können die Eigenschaften von AMS Resource Scheduler anhand Ihrer Präferenzen mithilfe von CloudFormation Stack-Parametern konfigurieren und ein Stack-Update durchführen. Informationen zum Aktualisieren von CloudFormation Stacks finden Sie unter Direktes Aktualisieren von Stacks.

Wir empfehlen Ihnen, die folgenden Eigenschaften anzupassen und den Rest auf den Standardeinstellungen zu belassen, um eine optimale Funktionalität zu gewährleisten.

- Tagname: Der Name des Tags, das Resource Scheduler verwendet, um Instanzpläne mit Ressourcen zu verknüpfen. Der Standardwert ist `Schedule`.
- Zu planende Dienste: Eine durch Kommas getrennte Liste von Diensten, die Resource Scheduler verwalten kann. Der Standardwert lautet "`ec2,rds,autoscaling`". Gültige Werte sind „ec2", „rds“ und „autoscaling“.
- Standardzeitzone:Geben Sie die Standardzeitzone an, die der Resource Scheduler verwenden soll. Der Standardwert ist `UTC`.
- CMK für verschlüsselte EBS-Volumes: Eine durch Kommas getrennte Liste von Amazon KMS Customer Managed Key (CMK) ARNs , für die Resource Scheduler Berechtigungen erteilt werden können.
- EC2 Beispiel Lizenzmanager-Lizenz: Eine durch Kommas getrennte Liste von AWS-Lizenzmanagern, für ARNs die Resource Scheduler Berechtigungen erteilt werden können.

> **Note**
>
> AMS veröffentlicht gelegentlich Funktionen und Korrekturen, um AMS Resource Scheduler in Ihrem Konto auf dem neuesten Stand zu halten. In diesem Fall bleiben alle Anpassungen, die Sie über Stack-Parameter am AMS Resource Scheduler-Stack vornehmen, erhalten.
> Wir raten dringend davon ab, Anpassungen direkt an einer der Komponentenressourcen von AMS Resource Scheduler vorzunehmen. Dies beeinträchtigt die Funktionalität von Resource Scheduler und die Fähigkeit von AMS, ihn auf dem neuesten Stand zu halten.

AMS Resource Scheduler verwenden

So verwenden Sie AMS Resource Scheduler-Perioden in AMS Accelerate-Konten.

Verwenden Sie die folgenden AWS Systems Manager Automatisierungs-Runbooks, um den erforderlichen Zeitplan und Zeitraum in AMS Resource Scheduler zu verwalten.

> **Note**
>
> Diese SSM-Automatisierungs-Runbooks sind in der primären AWS-Region Ihres Kontos verfügbar.

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

Darüber hinaus stellt AMS eine AWS Identity and Access Management Rolle bereit`ams_resource_scheduler_ssm_automation_role`, die für die Verwendung der Runbooks AWS Systems Manager erforderlich ist und die diese übernimmt. Für die IAM-Rolle gilt eine Inline-Richtlinie mit den geringsten Rechten, die SSM-Berechtigungen gewährt, die für die Funktionalität der Runbooks erforderlich sind.

Voraussetzungen

Führen Sie die folgenden Schritte aus, bevor Sie das SSM-Automatisierungsrunbook und den AMS Resource Scheduler verwenden.

Fügen Sie die folgende Richtlinie der entsprechenden IAM-Entität (Benutzer, Gruppe oder Rolle) hinzu, der Sie die Nutzung der Automatisierungs-Runbooks zur Verwaltung des Zeitplans und der Periode im AMS Resource Scheduler ermöglichen möchten. Die Richtlinie ist nicht erforderlich, wenn Ihre IAM-Entität über einen Administrator oder PowerUser eine entsprechende Berechtigung für Ihr Konto verfügt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
```

```
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdatePeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdateSchedule:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DeleteScheduleOrPeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DescribeScheduleOrPeriods:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
EnableOrDisableAMSResourceScheduler:*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

Sie können die Automatisierung entweder über die AWS Systems Manager Konsole oder über die AWS CLI ausführen. Wenn Sie die AWS CLI verwenden, müssen Sie sie oder die AWS Tools dafür möglicherweise installieren und konfigurieren PowerShell, falls Sie dies noch nicht getan haben. Informationen finden Sie unter AWS Befehlszeilentools installieren oder aktualisieren.

Sehen Sie sich das Video von Navish an, um mehr zu erfahren (4:52)

Arbeiten mit Zeiträumen und Zeitplänen in AWS Managed Services Resource Scheduler

Sie können AMS Resource Scheduler verwenden, um Zeitpläne oder Perioden in AMS Accelerate-Konten hinzuzufügen, zu aktualisieren oder zu löschen.

Perioden in AMS Resource Scheduler hinzufügen oder aktualisieren

Fügen Sie einen Resource Scheduler-Zeitraum in Ihren AMS-Konten hinzu oder aktualisieren Sie ihn.

Daten, die Sie benötigen:

- Aktion: Die Art des auszuführenden Vorgangs. Verwenden Sie „Hinzufügen“, wenn Sie einen Zeitraum hinzufügen möchten, oder „Aktualisieren“, wenn Sie einen vorhandenen Zeitraum aktualisieren möchten.
- Name: Der Name des Zeitraums. Sie müssen einen eindeutigen Wert angeben, wenn Sie einen neuen Zeitraum hinzufügen.
- AutomationAssumeRole: Der ARN der AWS Identity and Access Management (IAM) -Rolle, die es dem Runbook ermöglicht, den Zeitraum in Ihrem Namen hinzuzufügen oder zu aktualisieren. Geben Sie die Rolle als an. `ams_resource_scheduler_ssm_automation_role`

- Beschreibung (optional): Eine aussagekräftige Beschreibung für den Zeitraum.
- BeginTime(Optional): Die Uhrzeit im Format HH:MM, zu der Sie die Ressourcen starten möchten.
- EndTime(Optional): Die Uhrzeit im Format HH:MM, zu der Sie die Ressourcen beenden möchten.
- Monate (optional): Eine durch Kommas getrennte Liste von Monaten oder ein Bereich von Monaten mit Bindestrich, in denen die Ressourcen laufen sollen.
- MonthDays(Optional): Eine durch Kommas getrennte Liste von Tagen im Monat oder ein Bereich von Tagen mit Bindestrich, an denen die Ressourcen laufen sollen.
- WeekDays(Optional): Eine durch Kommas getrennte Liste der Wochentage oder einer Reihe von Wochentagen, an denen die Ressourcen laufen sollen.

Wie geht das:

- Sehen Sie sich das Dokument an unter AWSManagedServices-AddOrUpdatePeriod(möglicherweise müssen Sie Ihre Onboarding-Region auswählen).

  Geben Sie die Anforderungen im Abschnitt Eingabeparameter an und wählen Sie dann Ausführen. Nachdem der Vorgang abgeschlossen ist, können Sie die Ergebnisse auf der Registerkarte „Ausgabe“ anzeigen.
- AWS CLI:

  Führen Sie den folgenden Befehl aus, um eine Automatisierung zu starten. *placeholders*Ersetzen Sie es durch Ihre eigenen Informationen.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Beispiel:

Das folgende Beispiel zeigt, wie Sie mithilfe der AWS Systems Manager Konsole einen neuen Zeitraum hinzufügen können. Wir haben den Zeitraum Periodenname benannt und ihn so konfiguriert, dass er die ersten 15 Tage eines jeden Monats von Montag bis Freitag von 9.00 bis 18.00 Uhr abdeckt.

1. Das AWS Systems Manager Automatisierungsdokument finden Sie unter AWSManagedServices-AddOrUpdatePeriod(möglicherweise müssen Sie Ihre Onboarding-Region auswählen).

2. Geben Sie Werte für die Parameter an.

3. Klicken Sie auf Ausführen und warten Sie, bis die Automatisierung abgeschlossen ist.

Hinzufügen oder Aktualisieren von Zeitplänen im AMS Resource Scheduler

Fügen Sie einen Resource Scheduler-Zeitplan in AMS Accelerate-Konten hinzu oder aktualisieren Sie ihn.

Daten, die Sie benötigen:

- Aktion: Die Art des auszuführenden Vorgangs. Verwenden Sie „Hinzufügen“, wenn Sie einen Zeitplan hinzufügen möchten, oder „Aktualisieren“, wenn Sie einen vorhandenen Zeitplan aktualisieren möchten.
- Name: Der Name des Zeitplans. Sie müssen einen eindeutigen Wert angeben, wenn Sie einen neuen Zeitplan hinzufügen.
- AutomationAssumeRole: Der ARN der AWS Identity and Access Management (IAM) -Rolle, die es dem Runbook ermöglicht, den Zeitplan in Ihrem Namen hinzuzufügen oder zu aktualisieren. Geben Sie die Rolle an. `ams_resource_scheduler_ssm_automation_role`
- Beschreibung (optional): Eine aussagekräftige Beschreibung für den Zeitplan.
- Zeitpläne (optional): Geben Sie eine durch Kommas getrennte Liste von Perioden an, die mit diesem Zeitplan verwendet werden sollen. Jeder Zeitraum muss bereits erstellt worden sein.
- RetainRunning(Optional): Geben Sie „true“ an, um zu verhindern, dass Resource Scheduler eine laufende Ressource am Ende einer Laufzeit stoppt, wenn die Ressource vor Beginn der laufenden Periode manuell gestartet wurde. Standardmäßig stoppt Resource Scheduler die Ressource.
- StopNewInstances(Optional): Geben Sie „false“ an, um zu verhindern, dass Resource Scheduler eine Ressource stoppt, wenn sie das erste Mal markiert wird, wenn sie außerhalb der Laufzeit ausgeführt wird. Standardmäßig stoppt Resource Scheduler die Ressource.
- SSMMaintenanceFenster (optional): Geben Sie eine durch Kommas getrennte Liste von AWS Systems Manager (SSM) -Wartungsfenstern an, die Sie als Laufzeiten für den Zeitplan hinzufügen möchten. Außerdem müssen Sie für die Eigenschaft "UseMaintenanceWindow" den Wert „true“ angeben.

- TimeZone(Optional): Geben Sie die Zeitzone an, die Resource Scheduler verwenden soll. Standardmäßig verwendet Resource Scheduler UTC.
- UseMaintenanceWindow(Optional): Geben Sie „true“ an, wenn Resource Scheduler das Wartungsfenster von Amazon Relational Database Service (RDS) als Laufzeit für einen Amazon RDS-Instance-Zeitplan betrachten soll, oder wenn Sie einem EC2 Amazon-Instance-Zeitplan die Wartungsfenster von AWS Systems Manager (SSM) als Laufzeit hinzufügen möchten.
- UseMetrics(Optional): Geben Sie „true“ an, um CloudWatch Metriken auf Zeitplanebene zu aktivieren, und „false“, um Metriken zu deaktivieren. CloudWatch Die Angabe dieser Eigenschaft überschreibt die auf Stack-Ebene festgelegte CloudWatch Metrikeinstellung.

Wie geht das:

- Sehen Sie sich das Dokument an unter AWSManagedServices-AddOrUpdateSchedule(möglicherweise müssen Sie Ihre Onboarding-Region auswählen).

  Geben Sie die Anforderungen im Abschnitt Eingabeparameter an und wählen Sie dann Ausführen. Zeigen Sie nach Abschluss des Vorgangs die Ergebnisse auf der Registerkarte Ausgabe an.
- AWS CLI:

  Führen Sie den folgenden Befehl aus, um eine Automatisierung zu starten. *placeholders*Ersetzen Sie es durch Ihre eigenen Informationen.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Beispiel:

Das folgende Beispiel zeigt, wie Sie einen Zeitplan für AMS Resource Scheduler hinzufügen. In diesem Beispiel fügen Sie einen Zeitplan mit dem Namen using hinzu. CustomSchedule CustomPeriod

1. Sehen Sie sich das AWS Systems Manager Automatisierungsdokument unter an AWSManagedServices-AddOrUpdateSchedule(möglicherweise müssen Sie Ihre Onboarding-Region auswählen).

2. Geben Sie Werte für die Parameter an.

3. Klicken Sie auf Ausführen und warten Sie, bis die Automatisierung abgeschlossen ist.

Löschen von Perioden oder Zeitplänen in AMS Resource Scheduler

Um Resource Scheduler-Perioden oder -Zeitpläne in AMS Accelerate-Konten zu löschen, benötigen Sie die folgenden Daten:

- ConfigurationType: Der Konfigurationstyp, den Sie löschen möchten. Verwenden Sie „Zeitraum“, wenn Sie Perioden löschen möchten, oder „Zeitplan“, wenn Sie Zeitpläne löschen möchten.
- Name: Der Name des Zeitplans oder der Periode, den Sie löschen möchten.
- AutomationAssumeRole: Der ARN der AWS Identity and Access Management (IAM) -Rolle, die es dem Runbook ermöglicht, Zeitpläne oder Perioden in Ihrem Namen zu löschen. Geben Sie die Rolle an. `ams_resource_scheduler_ssm_automation_role`

Wie geht das:

- Sehen Sie sich das Dokument an unter AWSManagedServices-DeleteScheduleOrPeriod(möglicherweise müssen Sie Ihre Onboarding-Region auswählen).

  Geben Sie die Anforderungen im Abschnitt Eingabeparameter an und wählen Sie dann Ausführen. Nachdem der Vorgang abgeschlossen ist, können Sie die Ergebnisse auf der Registerkarte „Ausgabe“ anzeigen.

- AWS CLI:

  Führen Sie den folgenden Befehl aus, um eine Automatisierung zu starten. *`placeholders`*Ersetzen Sie es durch Ihre eigenen Informationen.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

Beispiel:

Das folgende Beispiel zeigt, wie Sie einen Zeitraum mithilfe der AWS Systems Manager Konsole löschen können.

1. Sehen Sie sich das AWS Systems Manager Automatisierungsdokument unter an AWSManagedServices-DeleteScheduleOrPeriod(möglicherweise müssen Sie Ihre Onboarding-Region auswählen).

2. Geben Sie Werte für die Parameter an.

3. Klicken Sie auf Ausführen und warten Sie, bis die Automatisierung abgeschlossen ist.

Beschreibung von Zeiträumen oder Zeitplänen im AMS Resource Scheduler

Um einen Resource Scheduler-Periode oder einen Zeitplan in AMS Accelerate-Konten zu beschreiben (Details dazu einzusehen), benötigen Sie die folgenden Daten:

- ConfigurationType: Der Konfigurationstyp, den Sie beschreiben möchten. Verwenden Sie „Perioden“, wenn Sie alle Perioden beschreiben möchten, oder „Zeitpläne“, wenn Sie alle Zeitpläne beschreiben möchten.
- AutomationAssumeRole: Der ARN der Rolle AWS Identity and Access Management (IAM), der es dem Runbook ermöglicht, Zeitpläne oder Zeiträume in Ihrem Namen zu beschreiben. Geben Sie die Rolle an. `ams_resource_scheduler_ssm_automation_role`

Wie geht das:

- Sehen Sie sich das Dokument an unter AWSManagedServices-DescribeScheduleOrPeriods(möglicherweise müssen Sie Ihre Onboarding-Region auswählen):

1. Geben Sie die Anforderungen im Abschnitt Eingabeparameter an und wählen Sie dann Ausführen.
2. Nachdem der Vorgang abgeschlossen ist, können Sie die Ergebnisse auf der Registerkarte Ausgabe anzeigen.

- AWS CLI:

1. Führen Sie den folgenden Befehl aus, um eine Automatisierung zu starten. *placeholders*Ersetzen Sie es durch Ihre eigenen Informationen.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

Beispiel:

Das folgende Beispiel zeigt, wie Sie mithilfe der AWS Systems Manager Konsole einen Zeitraum beschreiben können.

1. Sehen Sie sich das AWS Systems Manager Automatisierungsdokument unter an AWSManagedServices-DescribeScheduleOrPeriods(möglicherweise müssen Sie Ihre Onboarding-Region auswählen).

2. Geben Sie Werte für die Parameter an.

3. Klicken Sie auf Ausführen und warten Sie, bis die Automatisierung abgeschlossen ist.

Tagging-Ressourcen für AMS Resource Scheduler

Taggen von Ressourcen für AMS Resource Scheduler.

Sobald Sie Zeitpläne und Perioden zu AMS Resource Schedule hinzugefügt haben, müssen Sie Ihre Ressourcen mit dem Resource Scheduler-Tagnamen als Tag-Schlüssel oder dem benutzerdefinierten Tag-Namen und dem Namen des Zeitplans als Tag-Wert taggen. Einzelheiten dazu, wie Sie Ihre Ressourcen in Ihrem AMS Accelerate-Konto taggen können, finden Sie unterTaggen in AMS Accelerate.

> **Note**
>
> Wenn Resource Tagger verwendet wird, um die Ressourcen zu taggen, muss der Standard-Tag-Schlüssel für Resource Scheduler so angepasst werden, dass er das Präfix '`ams:rt:`' hat, da alle vom Resource Tagger angewendeten Tags das key prefix '' haben. `ams:rt:` Andernfalls werden die mit Resource Tagger markierten Ressourcen nicht von Resource Scheduler verwaltet. Weitere Informationen zum Anpassen des Standard-Tag-Schlüssels für Resource Scheduler finden Sie unter. AMS Resource Scheduler anpassen

Kostenschätzer im AMS Resource Scheduler

Um Kosteneinsparungen nachzuverfolgen, bietet AMS Resource Scheduler eine Komponente, die stündlich die geschätzten Kosteneinsparungen für Amazon EC2 - und Amazon RDS-Ressourcen berechnet, die vom Scheduler verwaltet werden. Diese Daten zu den Kosteneinsparungen werden dann als CloudWatch Metrik (`AMS/ResourceScheduler`) veröffentlicht, um Ihnen zu helfen, sie nachzuverfolgen. Der Kosteneinsparungsschätzer schätzt nur die Einsparungen bei den Betriebsstunden der Instance. Andere Kosten, wie z. B. die mit einer Ressource verbundenen Datenübertragungskosten, werden nicht berücksichtigt.

Der Kosteneinsparungsrechner ist mit Resource Scheduler aktiviert. Er läuft stündlich und ruft Kosten- und Nutzungsdaten von ab. AWS Cost Explorer Aus diesen Daten berechnet es die durchschnittlichen Kosten pro Stunde für jeden Instance-Typ und prognostiziert dann die Kosten für einen ganzen Tag, wenn die Instanz ohne Zeitplan ausgeführt wurde. Die Kosteneinsparungen sind die Differenz zwischen den prognostizierten Kosten und den tatsächlich gemeldeten Kosten aus dem Cost Explorer für einen bestimmten Tag.

Wenn Instanz A beispielsweise so konfiguriert ist, dass Resource Scheduler von 9.00 Uhr bis 17.00 Uhr ausgeführt wird, sind das acht Stunden an einem bestimmten Tag. Cost Explorer meldet die Kosten mit 1$ und die Nutzung mit 8. Die durchschnittlichen Kosten pro Stunde belaufen sich daher auf 0,125$. Wenn die Instanz nicht mit Resource Scheduler geplant wurde, würde die Instanz an diesem Tag rund um die Uhr laufen. In diesem Fall hätten die Kosten 24x0,125 = 3$ betragen. Resource Scheduler hat Ihnen dabei geholfen, Kosten in Höhe von 2$ einzusparen.

Damit der Kosteneinsparungsschätzer Kosten und Nutzung nur für Ressourcen abrufen kann, die von Resource Scheduler aus dem Cost Explorer verwaltet werden, muss der Tag-Schlüssel, den Resource Scheduler für die Ausrichtung von Ressourcen verwendet, als Kostenzuordnungs-Tag im Fakturierungs-Dashboard aktiviert werden. Wenn das Konto zu einer Organisation gehört, muss der

Tag-Schlüssel im Verwaltungskonto der Organisation aktiviert werden. Informationen dazu finden Sie unter Benutzerdefinierte Kostenverrechnungs-Tags und Benutzerdefinierte Kostenverrechnungs-Tags aktivieren

Nachdem der Tag-Schlüssel als Cost Allocation Tag aktiviert wurde, beginnt die AWS-Abrechnung mit der Erfassung der Kosten und der Nutzung für Ressourcen, die von Resource Scheduler verwaltet werden. Sobald diese Daten verfügbar sind, beginnt der Kosteneinsparungsschätzer mit der Berechnung der Kosteneinsparungen und veröffentlicht die Daten unter dem `AMS/ResourceScheduler` Metrik-Namespace in. CloudWatch

Wenn das Kostenzuweisungs-Tag nicht aktiviert ist, kann der Kalkulator die Einsparungen nicht berechnen und die Metrik nicht veröffentlichen, selbst wenn er aktiviert ist.

> **Note**
>
> Der Kosteneinsparungsschätzer berücksichtigt keine Rabatte wie Reserved Instances, Sparpläne usw. bei der Berechnung. Der Estimator verwendet die Nutzungskosten aus dem Cost Explorer und berechnet die durchschnittlichen Kosten pro Stunde für die Ressourcen. Weitere Informationen finden Sie unter Grundlegendes zu Ihren AWS Kostendatensätzen: Ein Spickzettel.

Alarmunterdrücker im AMS Resource Scheduler

AMS Resource Scheduler verfügt über einen CloudWatch Alarmsuppressor, der als separate Lambda-Funktion mit dem Namen bereitgestellt wird und Alarme für Instances unterdrücktAMSAlarmSuppressor, die sich hinter einem Elastic Load Balancing, Application Load Balancer oder Network Load Balancer befinden. Die Funktion wird alle 5 Minuten ausgeführt, ruft alle im Konto vorhandenen Alarme ab und gruppiert sie nach Namespace, z. B.,,. `AWS/ELB` `AWS/ApplicationELB` `AWS/NetworkELB` Für jede Gruppe von Alarmen findet der Suppressor den Namen des Load Balancers (and/or Zielgruppe) und überprüft den Instanzstatus, um festzustellen, ob die Instances vom AMS Resource Scheduler geplant wurden. ALB/NLB) from alarm dimensions, finds the instances that are registered with the load balancer and/or Wenn Instances vom Resource Scheduler geplant und vom Resource Scheduler gestoppt werden, markiert der Suppressor dann die Alarme, um sie zu deaktivieren. Wenn mindestens eine Instanz in der Liste der registrierten Instanzen läuft, markiert der Suppressor die entsprechenden Alarme, um die Alarme zu aktivieren, und deaktiviert Alarme, die für die Deaktivierung markiert sind. Protokolle hierfür werden in der `/aws/lambda/AMSAlarmSuppressor` Protokollgruppe gespeichert.

Protokollverwaltung in AMS Accelerate

AMS Accelerate konfiguriert unterstützte AWS Dienste für die Erfassung von Protokollen. Diese Protokolle werden von AMS Accelerate verwendet, um die Einhaltung der Vorschriften und die Prüfung der Ressourcen in Ihrem Konto sicherzustellen.

AMS Accelerate bietet eine Reihe von Betriebsservices, die Ihnen helfen, betriebliche Exzellenz auf AWS zu erreichen. Um schnell zu verstehen, wie AMS Ihren Teams hilft, mit einigen unserer wichtigsten operativen Funktionen, darunter Helpdesk rund um die Uhr, proaktive Überwachung, Sicherheit, Patching, Protokollierung und Sicherung, allgemeine betriebliche Exzellenz in der AWS-Cloud zu erreichen, sehen Sie sich die AMS-Referenzarchitekturdiagramme an.

Themen

Protokollverwaltung — AWS CloudTrail

AWS CloudTrailist ein Service, der für die Kontoverwaltung verwendet wird: Einhaltung von Vorschriften, betriebliche Prüfungen und Risikoprüfungen. Damit können Sie Kontoaktivitäten im Zusammenhang mit CloudTrail Aktionen in Ihrer gesamten AWS Infrastruktur protokollieren, kontinuierlich überwachen und speichern.

AMS Accelerate erfordert eine AWS CloudTrail Protokollierung, um Audits und die Einhaltung von Vorschriften für alle Ressourcen in Ihrem Konto zu verwalten. Beim Onboarding können Sie eine der folgenden Optionen wählen:

- Von AMS bereitgestellter Trail: Wenn Sie sich für diese Option entscheiden, erstellt, implementiert und verwaltet AMS einen Trail mit CloudTrail mehreren Regionen in Ihrer AWS Hauptregion, unabhängig von den vorhandenen Trails in Ihrem Konto.
- Bringen Sie Ihren eigenen Trail mit: Wenn Sie sich dafür entscheiden, Ihr eigenes Konto oder Ihren eigenen CloudTrail Organisations-Trail bereitzustellen, müssen Sie mit Ihrem Cloud Architect (CA) zusammenarbeiten, um sicherzustellen, dass dieser die erforderlichen Konfigurationen für Accelerate erfüllt. Wenn Sie sich für diese Option entscheiden, aber keinen eigenen Trail bereitstellen, stellt Accelerate automatisch einen eigenen CloudTrail Trail bereit, um kontinuierliche

Sicherheit und Audit-Abdeckung zu gewährleisten. Wenn Sie später Ihren eigenen Trail bereitstellen, entfernt AMS den bereitgestellten Trail, um Redundanz und zusätzliche Kosten zu vermeiden. Dieser Ansatz trägt dazu bei, einen einzigen aktiven CloudTrail Trail in Ihrem Konto zu verwalten und verhindert doppelte Logging-Kosten.

> **Note**
>
> Wenn Ihr Konto über einen bestehenden CloudTrail Trail verfügt und Sie beim Onboarding keinen von AMS verwalteten Trail speziell konfiguriert oder angefordert haben, entfernt AMS Accelerate den von AMS bereitgestellten Trail automatisch aus Ihrem Konto. Dies verhindert doppelte Protokollierung, optimiert die Ressourcennutzung und spart zusätzliche Kosten.

AMS Accelerate erstellt einen Amazon S3 S3-Bucket für einen von Accelerate bereitgestellten CloudTrail Trail als Ziel für die Ereigniszustellung und verwendet AWS Key Management Service (AWS KMS) -Verschlüsselung. Die Mitarbeiter von AMS Accelerate greifen zu Untersuchungs- und Diagnosezwecken auf Ihre Trail-Ereignisse zu. Wenn für das Konto bereits ein vorhandener CloudTrail Trail aktiviert ist, wird dieser Trail zusätzlich zu dem Trail hinzugefügt, falls Sie sich beim Onboarding dafür entschieden haben, dass Accelerate einen von Accelerate verwalteten Trail bereitstellen soll.

AMS Accelerate stellt mithilfe von AWS Config Regeln sicher, dass Ihre CloudTrail Konto-Trails, einschließlich eines von Accelerate bereitgestellten CloudTrail Trails, korrekt eingerichtet und verschlüsselt sind. Weitere Informationen hierzu finden Sie unter AWS Config. Dies sind die verwendeten Regeln, die als Links zu der AWS Dokumentation dargestellt werden, in der sie beschrieben werden:

- multi-region-cloudtrail-enabled. Überprüft, ob AMS Accelerate ordnungsgemäß mit den richtigen Konfigurationen eingerichtet CloudTrail ist.
- cloud-trail-encryption-enabled. AWS CloudTrail Überprüft, ob die serverseitige Verschlüsselung (SSE) mit CMK-Verschlüsselung (AWS KMS Customer Master Key) konfiguriert ist.
- cloud-trail-log-file-Validierung aktiviert. Wenn diese Option aktiviert ist, wird überprüft, ob eine signierte Digest-Datei mit Protokollen AWS CloudTrail erstellt wird. Wir empfehlen dringend, die Dateiüberprüfung auf allen Pfaden zu aktivieren.
- s-3 bucket-default-lock-enabled. Wenn diese Option aktiviert ist, wird überprüft, ob für den Amazon S3 S3-Bucket die Sperre aktiviert ist.

- s-3 bucket-logging-enabled. Wenn diese Option aktiviert ist, wird geprüft, ob die Protokollierung für Amazon S3 S3-Buckets aktiviert ist.

AMS Accelerate verwendet AWS KMS , um die protokollierten Ereignisse für einen von Accelerate bereitgestellten CloudTrail Trail in Ihrem Konto zu verschlüsseln. Dieser Schlüssel wird von den Kontoadministratoren, AMS Accelerate-Betreibern und gesteuert und CloudTrail ist für diese zugänglich. Weitere Informationen AWS KMS finden Sie in der Produktdokumentation zu den AWS Key Management Service Funktionen.

Zugriff auf und Prüfung von CloudTrail Protokollen

CloudTrail Protokolle für einen von AMS Accelerate bereitgestellten CloudTrail Trail werden in einem Amazon S3 S3-Bucket in Ihrem Konto gespeichert. Im Amazon S3 S3-Bucket gespeicherte Trail-Daten werden mit einem AWS-KMS-Schlüssel verschlüsselt, der bei der Bereitstellung von CloudTrail Ressourcen erstellt wird.

Amazon S3 S3-Buckets nutzen das Benennungsmuster ams-a ***aws account id*** -cloudtrail- (Beispiel: ams-a123456789- ***AWS Region*** cloudtrail-us-east -1a) und alle Ereignisse werden mit dem Präfix AWS/ gespeichert. CloudTrail Jeder Zugriff auf den primären Bucket wird protokolliert und die Protokollobjekte werden zu Prüfungszwecken verschlüsselt und versioniert.

Weitere Informationen zum Nachverfolgen von Änderungen und zum Abfragen der Protokolle finden Sie unter. Änderungen in Ihren AMS Accelerate-Konten verfolgen

Protokolle schützen und aufbewahren CloudTrail

AMS Accelerate ermöglicht das Sperren von Amazon S3 S3-Objekten mit dem Governance-Modus für einen von Accelerate bereitgestellten CloudTrail Trail, um sicherzustellen, dass Benutzer eine Objektversion nicht ohne besondere Berechtigungen überschreiben oder löschen oder deren Sperreinstellungen ändern können. Weitere Informationen finden Sie unter Amazon S3 S3-Objektsperre.

Standardmäßig werden alle Protokolle in diesem Bucket auf unbestimmte Zeit aufbewahrt. Wenn Sie den Aufbewahrungszeitraum ändern möchten, können Sie über das AWS Support Center eine Serviceanfrage einreichen, um eine andere Aufbewahrungsrichtlinie einzurichten.

Zugreifen auf EC2 Amazon-Logs

Sie können auf EC2 Amazon-Instance-Logs zugreifen, indem Sie den verwenden AWS-Managementkonsole. Von Instances und AWS Services erstellte CloudWatch Protokolle sind in Logs verfügbar, das in jedem von AMS Accelerate verwalteten Konto verfügbar ist. Informationen zum Zugriff auf Ihre Logs finden Sie in der CloudWatch Logs-Dokumentation.

Aufbewahrung von EC2 Amazon-Protokollen

EC2 Amazon-Instance-Logs werden standardmäßig auf unbestimmte Zeit aufbewahrt. Wenn Sie den Aufbewahrungszeitraum ändern möchten, können Sie über das AWS Support Center eine Serviceanfrage stellen, um eine andere Aufbewahrungsrichtlinie einzurichten.

Protokollverwaltung — Amazon EC2

AMS Accelerate installiert den CloudWatch Agenten auf allen EC2 Amazon-Instances, die Sie als von AMS Accelerate verwaltet identifiziert haben. Dieser Agent sendet Protokolle auf Systemebene an Amazon CloudWatch Logs. Weitere Informationen finden Sie unter Was sind CloudWatch Amazon-Logs?

Die folgenden Protokolldateien werden an CloudWatch Logs in eine Protokollgruppe mit demselben Namen wie das Protokoll gesendet. Innerhalb jeder Protokollgruppe wird für jede EC2 Amazon-Instance ein Log-Stream erstellt, der nach der EC2 Amazon-Instance-ID benannt ist.

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log
- /.log var/log/audit/audit
- /.log var/log/auth
- /-init-output.log var/log/cloud
- /var/log/cron
- /var/log/dnf.log
- /.log var/log/dpkg
- /var/log/maillog
- /var/log/messages

- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /.log var/log/yum
- /.log var/log/zypper

Weitere Informationen finden Sie unter Manuelles Erstellen oder Bearbeiten der CloudWatch Agent-Konfigurationsdatei.

Windows

- SSMAgentAmazon-Protokoll
- AmazonCloudWatchAgentLog
- SSMErrorAmazon-Protokoll
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventLoggen
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

Weitere Informationen finden Sie unter Schnellstart: Aktivieren Sie Ihre EC2 Amazon-Instances, auf denen Windows Server 2016 ausgeführt wird, um mithilfe des Logs-Agenten CloudWatch Logs an CloudWatch Logs zu senden.

Protokollverwaltung — Amazon VPC Flow Logs

VPC Flow Logs ist eine Funktion, die Informationen über den IP-Verkehr erfasst, der zu und von Netzwerkschnittstellen in Ihrer VPC fließt. Flow-Protokolldaten können in Amazon CloudWatch Logs oder Amazon S3 veröffentlicht werden. Die Erfassung von Flow-Protokolldaten hat keinen Einfluss auf den Netzwerkdurchsatz oder die Latenz. Sie können Flow-Protokolle erstellen oder löschen, ohne die Netzwerkleistung zu beeinträchtigen.

Mit Flow-Protokollen können Sie eine Reihe von Aufgaben ausführen, z. B.:

- Diagnose zu restriktiver Sicherheitsgruppenregeln
- Überwachung des Datenverkehrs, der Ihre Instance erreicht
- Ermitteln der Richtung des Datenverkehrs zu und von den Netzwerkschnittstellen

Sie müssen die VPC-Flow-Logs nicht für jede neu erstellte VPC in Accelerate-Konten aktivieren. AMS erkennt anhand der Regel ams-nist-cis-vpc- flow-logs-enabled Config automatisch, ob eine VPC über ein Flow-Log verfügt. Wenn VPC-Flow-Logs nicht aktiviert sind, behebt AMS das Problem automatisch, indem es ein VPC-Flow-Protokoll mit benutzerdefinierten Feldern erstellt. Mit diesen zusätzlichen Feldern können AMS und Kunden den VPC-Verkehr besser überwachen, Netzwerkabhängigkeiten verstehen, Netzwerkverbindungsprobleme beheben und Netzwerkbedrohungen identifizieren.

Informationen zum Anzeigen und Durchsuchen von Flow-Logs finden Sie unter Arbeiten mit Flow-Logs.

Änderungen in Ihren AMS Accelerate-Konten verfolgen

Important

Der Change Record-Service ist seit dem 1. Juli 2025 veraltet.
Neue Konten können nicht in den Change Record-Service integriert werden.
Um CloudTrail Daten in Ihren AMS Accelerate-Konten abzufragen, können Sie diese Dienste verwenden:

- Wählen Sie AWS CloudTrail unter Eventverlauf und filtern Sie Ereignisse mithilfe von Lookup-Attributen. Sie können den Zeitbereichsfilter verwenden und wählen, ob der Ereignisverlauf nach der `s3.amazon.aws.com` angegebenen Ereignisquelle gefiltert werden soll, oder ob der Ereignisverlauf nach dem Benutzernamen gefiltert werden soll. Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Ereignisverlauf.
- Verwenden Sie AWS CloudTrail Lake, um Daten mithilfe von Abfragen zu sammeln. AWS CloudTrail Wählen Sie in Lake und dann Query aus. Sie können Ihre eigenen Abfragen erstellen, den Abfragegenerator verwenden oder Beispielabfragen verwenden, um ereignisbasierte Daten zu sammeln. Sie können beispielsweise fragen, wer in der vergangenen Woche eine EC2 Amazon-Instance gelöscht hat. Weitere Informationen finden Sie unter Einen Data Lake aus einer AWS CloudTrail Quelle und CloudTrailLake Abfragen erstellen.
- Erstellen Sie eine Amazon Athena Athena-Tabelle in AWS CloudTrail und legen Sie den Speicherort als den Amazon S3 S3-Bucket fest, der Ihrem Trail zugeordnet ist. Vergewissern Sie sich, dass die Heimatregion für Ihren Trail und Ihren Amazon S3 S3-Bucket identisch ist. Verwenden Sie in Amazon Athena den Abfrage-Editor, um die Standardabfragen auszuführen, die Accelerate für die Verwendung mit der Athena-Konsole bereitstellt. Weitere Informationen zum Erstellen einer Athena-Tabelle zum Abfragen von Logs finden Sie unter CloudTrail Logs abfragen AWS CloudTrail.

Themen

AWS Managed Services hilft Ihnen dabei, Änderungen nachzuverfolgen, die vom AMS Accelerate Operations Team und AMS Accelerate Automation vorgenommen wurden, indem es eine abfragbare Schnittstelle über die Amazon Athena (Athena) -Konsole und das AMS Accelerate-Protokollmanagement bereitstellt.

Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten in Amazon S3 mithilfe der standardmäßigen Structured Query Language (SQL) analysieren können (siehe SQL-Referenz für Amazon Athena). Athena ist Serverless, weshalb auch keine Infrastruktur eingerichtet oder verwaltet werden muss – und Sie zahlen nur für tatsächlich ausgeführte Abfragen. AMS Accelerate erstellt Athena-Tabellen mit täglichen Partitionen über CloudTrail Logs und stellt Abfragen in Ihrer primären AWS Region und innerhalb der ams-change-recordArbeitsgruppe bereit. Sie können eine der Standardabfragen wählen und sie nach Bedarf ausführen. Weitere Informationen zu Athena-Arbeitsgruppen finden Sie unter So funktionieren Arbeitsgruppen.

> **Note**
>
> Nur Accelerate kann CloudTrail Ereignisse für Ihr Accelerate-Konto mit Athena abfragen, wenn Accelerate in Ihren CloudTrail Organization-Trail integriert ist, es sei denn, Ihr Organisationsadministrator hat während des Onboardings eine IAM-Rolle für die Nutzung von Athena zur Abfrage und Analyse von CloudTrail Ereignissen in Ihrem Konto bereitgestellt.

Mithilfe von Change Record können Sie ganz einfach Fragen wie die folgenden beantworten:

- Wer (AMS Accelerate Systems oder AMS Accelerate Operators) hat auf Ihr Konto zugegriffen
- Welche Änderungen wurden von AMS Accelerate an Ihrem Konto vorgenommen
- Wann hat AMS Accelerate Änderungen an Ihrem Konto vorgenommen
- Wo können Sie die an Ihrem Konto vorgenommenen Änderungen einsehen
- Warum musste AMS Accelerate die Änderungen an Ihrem Konto vornehmen
- So ändern Sie Abfragen, um Antworten auf all diese Fragen zu erhalten, auch für Änderungen, die nicht von AMS stammen

Ihre Änderungsdatensätze anzeigen

Um Athena-Abfragen zu verwenden, melden Sie sich bei der AWS Management Console an und navigieren Sie zur Athena-Konsole in Ihrer primären AWS Region.

> **Note**
>
> Wenn Sie während der Ausführung eines der Schritte die Seite Erste Schritte von Amazon Athena sehen, klicken Sie auf Erste Schritte. Dies kann Ihnen auch dann angezeigt werden, wenn Ihre Change Record-Infrastruktur bereits vorhanden ist.

1. Wählen Sie im oberen Navigationsbereich der Athena-Konsole Workgroup aus.
2. Wählen Sie die ams-change-recordArbeitsgruppe aus und klicken Sie dann auf Arbeitsgruppe wechseln.
3. Wählen Sie ams-change-record-databaseaus dem Kombinationsfeld Datenbank aus. Das ams-change-record-databasebeinhaltet die ams-change-record-tableTabelle.
4. Wählen Sie im oberen Navigationsbereich die Option Gespeicherte Abfragen aus.
5. Das Fenster Gespeicherte Abfragen zeigt eine Liste von Abfragen, die AMS Accelerate bereitstellt und die Sie ausführen können. Wählen Sie die Abfrage, die Sie ausführen möchten, aus der Liste der gespeicherten Abfragen aus. Zum Beispiel die Abfrage ams_session_accesses_v1.

   Die vollständige Liste der voreingestellten AMS Accelerate-Abfragen finden Sie unter. Standardabfragen
6. Passen Sie den Datetime-Filter im Abfrage-Editor-Feld nach Bedarf an. Standardmäßig überprüft die Abfrage nur Änderungen vom letzten Tag.
7. Wählen Sie Abfrage ausführen.

Standardabfragen

AMS Accelerate bietet mehrere Standardabfragen, die Sie in der Athena-Konsole verwenden können. Die Standardabfragen sind in den folgenden Tabellen aufgeführt.

> **Note**
>
> - Alle Abfragen akzeptieren den Datums-/Uhrzeitbereich als optionalen Filter. Alle Abfragen werden standardmäßig über die letzten 24 Stunden ausgeführt. Informationen zu den erwarteten Eingaben finden Sie im folgenden Unterabschnitt:. Ändern des Datetime-Filters in Abfragen

- Parametereingaben, die Sie ändern können oder müssen, werden in der Abfrage wie *<PARAMETER_NAME>* eckige Klammern angezeigt. Ersetzen Sie den Platzhalter und die eckigen Klammern durch Ihren Parameterwert.
- Alle Filter sind optional. In den Abfragen werden einige optionale Filter mit einem doppelten Gedankenstrich (--) am Anfang der Zeile auskommentiert. Alle Abfragen werden ohne sie mit Standardparametern ausgeführt. Wenn Sie Parameterwerte für diese optionalen Filter angeben möchten, entfernen Sie den doppelten Gedankenstrich (--) am Anfang der Zeile und ersetzen Sie den Parameter wie gewünscht.
- Alle Abfragen geben zurück `IAM PincipalId` und `IAM SessionId` in den Ausgaben
- Die berechneten Kosten für die Ausführung einer Abfrage hängen davon ab, wie viele CloudTrail Protokolle für das Konto generiert werden. Verwenden Sie zur Berechnung der Kosten den AWS Athena Pricing Calculator.

Vorgefertigte Abfragen

Zweck/Beschreibung	Eingaben	Ausgaben
Name der Abfrage: `ams_access_session_query_v1`		
Verfolgung von AMS Accelerate-Zugriff ssitzungen Stellt Informationen zu einer bestimmten AMS Accelerate-Zugriffssitzung bereit. Die Abfrage akzeptiert die IAM-Prinz ipal-ID als optionalen Filter und gibt die Uhrzeit des Ereignisses, die Geschäftsanforderungen für den Zugriff auf das Konto, den Anforderer usw. zurück.	(Optional)`IAM PrincipalId` : Die IAM-Prinzipal-ID der Ressource , auf die zugegriff en werden soll. Das Format ist*UNIQUE_ID ENTIFIER* :*RESOURCE_ NAME* . Einzelheiten finden Sie unter eindeutig e Identifikatoren. Sie können die Abfrage auch ohne diesen Filter ausführen, um den genauen IAM zu ermitteln , mit PrincipalId dem Sie filtern möchten.	• EventTime: Uhrzeit des Zugriffs • EventName: AWS-Ereignisname (AssumeRole) • EventRegion: AWS-Region, die die Anfrage erhält • EventId: CloudTrail Ereignis-ID • BusinessNeed Typ: Art des geschäftl ichen Grundes für den Zugriff auf das Konto. Zulässige Werte sind: SupportCase, OpsItem, Issue, Text. • BusinessNeed: Unternehmen müssen auf das Konto zugreifen. Zum Beispiel Support Case ID, Ops-Item ID usw. • Anforderer: Bediener-ID, die auf das Konto zugreift, oder Automatis

Zweck/Beschreibung	Eingaben	Ausgaben
Sie können nach einer bestimmten IAM-Prinzipal-ID filtern, indem Sie die Zeile auskommentieren und den Platzhalter `IAM PrincipalId` im Abfrage-Editor durch eine bestimmte ID ersetzen. Sie können auch Sitzungen auflisten, bei denen es sich nicht um AMS-Zugriffe handelt, indem Sie die Useragent-Filterzeile in der WHERE-Klausel der Abfrage entfernen.		ierungssystem, das auf das Konto zugreift. • RequestAccessType: Typ des Anforderers (System, OpsAPI OpsConsole, Unset)
Name der Abfrage: `ams_events_query_v1`		

Zweck/Beschreibung	Eingaben	Ausgaben
Verfolgen Sie alle Mutationsaktionen, die von AMS Accelerate durchgeführt wurden Gibt alle Schreibaktionen zurück, die auf dem Konto mithilfe dieses AMS Accelerate-Rollenf ilters ausgeführt wurden. Sie können auch Mutationsaktionen nachverfolgen, die von Nicht-AMS-Rollen ausgeführt wurden, indem Sie die Filterzei len useridentity.arn aus der WHERE-Klausel der Abfrage entfernen.	(Optional) Nur Datums-/Uhrzeitber eich. Siehe Ändern des Datetime-Filters in Abfragen.	• AccountId: AWS-Konto-ID • RoleArn: RoleArn für den Anforderer • EventTime: Zeitpunkt der Erlangung des Zugriffs • EventName: AWS-Ereignisname (AssumeRole) • EventRegion: AWS-Region, die die Anfrage erhält • EventId: CloudTrail Ereignis-ID • RequestParameters : Anforderu ngsparameter für die Anfrage • ResponseElements: Antwortelemente für die Antwort. • UserAgent: CloudTrail AWS-Benut zeragent
Name der Abfrage: `ams_instance_access_sessions_query_v1`		

Zweck/Beschreibung	Eingaben	Ausgaben
Verfolgen Sie Instanzzugriffe mit AMS Accelerate Gibt eine Liste der AMS Accelerate-Instance-Zugriffe zurück. Jeder Datensatz enthält die Ereigniszeit, die Region des Ereignisses, die Instanz-ID, die IAM-Prinzipal-ID, die IAM-Sitzungs-ID und die SSM-Sitzungs-ID. Sie können die IAM-Prinzipal-ID verwenden, um mithilfe der `ams_access_sessions_query_v1` Athena-Abfrage weitere Informationen zu den geschäftlichen Anforderungen für den Zugriff auf die Instance zu erhalten. Sie können die SSM-Sitzungs-ID verwenden, um weitere Informationen zur Instanzzugriffssitzung zu erhalten, einschließlich der Start- und Endzeit der Sitzung, Protokolldetails und der Verwendung der AWS Session Manager-Konsole in der Region der Instanz. AWS	Nur `datetime range`. Siehe Ändern des Datetime-Filters in Abfragen.	• InstanceId: Instanz-ID • SSMSession ID: SSM-Sitzungs-ID • RoleArn: RoleArn für den Anforderer • EventTime: Zeitpunkt der Erlangung des Zugriffs • EventName: AWS-Ereignisname (AssumeRole) • EventRegion: AWS-Region, die die Anfrage erhält • EventId: CloudTrail Ereignis-ID

Zweck/Beschreibung	Eingaben	Ausgaben
Benutzer können auch Instanzzugriffe auflisten , die nicht von AMS stammen, indem sie die Zeile für den Benutzeri dentitätsfilter in der WHERE-Klausel der Abfrage entfernen.		
Name der Abfrage: ams_privilege_escalation_events_query_v1		

Zweck/Beschreibung	Eingaben	Ausgaben
Verfolgen Sie Genehmigungsereignisse (Eskalation) für AMS- und Nicht-AMS-Benutzer Stellt eine Liste von Ereignissen bereit, die direkt oder potenziell zu einer Rechteeskalation führen können. Die Abfrage akzeptiert ActionedBy als optionalen Filter und gibt EventName, EventId EventTime, usw. zurück. Alle mit dem Ereignis verknüpften Felder werden ebenfalls zurückgegeben. Felder sind leer, wenn sie für dieses Ereignis nicht relevant sind. Der ActionedBy Filter ist standardmäßig deaktiviert. Um ihn zu aktivieren, entfernen Sie „--“ aus dieser Zeile. Standardmäßig ist der ActionedBy Filter deaktiviert (er zeigt Ereignisse zur Rechteeskalation von allen Benutzern an). Um Ereignisse für einen bestimmten Benutzer	(Optional)`ACTIONEDBY_PUT_USER_NAME` : Benutzername für den ActionedBy-Benutzer. Dabei kann es sich um einen IAM-Benutzer oder -Rolle handeln. Zum Beispiel. ams-access-admin (Fakultativ)`datetime range`. Siehe Ändern des Datetime-Filters in Abfragen.	• AccountId: Konto-ID • ActionedBy: ActionedBy Nutzername • EventTime: Uhrzeit des Zugriffs • EventName: AWS-Ereignisname (AssumeRole). • EventRegion: AWS-Region, die die Anfrage erhält • EventId: CloudTrail Ereignis-ID

Zweck/Beschreibung	Eingaben	Ausgaben
oder eine bestimmte Rolle anzuzeigen, entfernen Sie den doppelten Gedankens trich (--) aus der Zeile des Benutzeridentitäts filters in der WHERE-Klausel und ersetzen Sie den Platzhalter *ACTIONEDBY_PUT_USER_NAME_HERE* durch einen IAM-Benutzer- oder Rollennamen. Sie können die Abfrage auch ohne den Filter ausführen, um genau den Benutzer zu ermitteln, nach dem Sie filtern möchten.		
Name der Abfrage: ams_resource_events_query_v1		

Zweck/Beschreibung	Eingaben	Ausgaben
Verfolgen Sie Schreiberignisse für bestimmte Ressourcen (AMS oder Nicht-AMS) Stellt eine Liste der Ereignisse bereit, die auf einer bestimmten Ressource ausgeführt wurden. Die Abfrage akzeptiert die Ressource n-ID als Teil der Filter (ersetzen Sie den Platzhalter *RESOURCE_INFO* in der WHERE-Klausel der Abfrage) und gibt alle Schreibaktionen zurück, die für diese Ressource ausgeführt wurden.	(Erforderlich)`RESOURCE_INFO` : Die Ressource n-ID kann eine ID für jede AWS-Ressource im Konto sein. Verwechseln Sie dies nicht mit einer Ressource ARNs. Zum Beispiel eine Instanz-ID für eine EC2 Instanz, ein Tabellenname für eine DynamoDB-Tabelle, logGroupName für ein CloudWatch Protokoll usw. (Optional). `datetime range` Siehe Ändern des Datetime-Filters in Abfragen.	• AccountId: Konto-ID • ActionedBy: ActionedBy Nutzername • EventTime: Uhrzeit des Zugriffs • EventName: AWS-Ereignisname (AssumeRole). • EventRegion: AWS-Region, die die Anfrage erhält • EventId: CloudTrail Ereignis-ID
Name der Abfrage: `ams_session_events_query_v1`		

Zweck/Beschreibung	Eingaben	Ausgaben
Verfolgen Sie Schreibaktionen, die von AMS Accelerate während einer bestimmten Sitzung ausgeführt wurden Stellt eine Liste der Ereignisse bereit, die in einer bestimmten Sitzung ausgeführt wurden. Die Abfrage akzeptiert die IAM-Prinzipal-ID als Teil der Filter (ersetzen Sie den Platzhalter *PRINCIPAL_ID* in der WHERE-Klausel der Abfrage) und gibt alle Schreibaktionen zurück, die für diese Ressource ausgeführt wurden.	(Erforderlich)`PRINCIPAL_ID` : Prinzipal-ID für die Sitzung. Das Format ist*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Einzelheiten finden Sie unter eindeutige Identifikatoren. Sie können die Abfrage „ams_session_ids_by_requester_v1" ausführen, um eine Liste der IAM-Principale für einen Anforderer abzurufen. IDs Sie können die Abfrage auch ohne diesen Filter ausführen, um den genauen IAM zu ermitteln, mit dem Sie filtern möchten. PrincipalId (Optional). `datetime range` Siehe Ändern des Datetime-Filters in Abfragen.	• AccountId: Konto-ID • ActionedBy: ActionedBy Nutzername • EventTime: Uhrzeit des Zugriffs • EventName: AWS-Ereignisname (AssumeRole) • EventRegion: AWS-Region, die die Anfrage erhält • EventId: CloudTrail Ereignis-ID
Name der Abfrage: `ams_session_ids_by_requester_v1`		

Zweck/Beschreibung	Eingaben	Ausgaben
Verfolgen Sie IAM Principal/Session IDs für einen bestimmten Anforderer. Die Abfrage akzeptiert den Begriff „Anforderer“ (ersetzen Sie den Platzhalter *Requester* in der WHERE-Klausel der Abfrage) und gibt alle IAM-Prinzipal-IDs dieses Anforderers im angegebenen Zeitraum zurück.	(Erforderlich)`Requester` : Operator-ID, die auf das Konto zugreift (z. B.: Alias eines Operators), oder Automatisierungssystem, das auf das Konto zugreift (z. B.: OsConfiguration, AlarmManager usw.). (Fakultativ). `datetime range` Siehe Ändern des Datetime-Filters in Abfragen.	• IAM PrincipalId — IAM-Principal-ID der Sitzung. Das Format ist*UNIQUE_IDENTIFIER* :. *RESOURCE_NAME* Einzelheiten finden Sie unter eindeutige Identifikatoren. Sie können die Abfrage auch ohne diesen Filter ausführen, um den genauen IAM zu ermitteln, mit dem PrincipalId Sie filtern möchten. • IAM SessionId — IAM-Sitzungs-ID für die Zugriffssitzung • EventTime: Uhrzeit des Zugriffs

Ändern des Datetime-Filters in Abfragen

Alle Abfragen akzeptieren den Datums-/Uhrzeitbereich als optionalen Filter. Alle Abfragen werden standardmäßig am letzten Tag ausgeführt.

Das für das Datetime-Feld verwendete Format ist yyyy/MM/dd (zum Beispiel: 2021/01/01). Denken Sie daran, dass nur das Datum und nicht der gesamte Zeitstempel gespeichert wird. Verwenden Sie für den gesamten Zeitstempel das Feld eventime, das den Zeitstempel im ISO 8601-Format yyyy-MM-dd T HH:mm:ss Z speichert (zum Beispiel: 2021-01-01T 23:59:59 Z). Da die Tabelle jedoch nach dem Datetime-Feld partitioniert ist, müssen Sie sowohl den Datetime- als auch den Eventtime-Filter an die Abfrage übergeben. Sehen Sie sich die folgenden Beispiele an.

> **Note**
>
> Alle akzeptierten Möglichkeiten zur Änderung des Bereichs finden Sie in der neuesten Presto-Funktionsdokumentation, die auf der Athena-Engine-Version basiert, die derzeit für die Datums- und Uhrzeitfunktionen und -Operatoren verwendet wird. Dort finden Sie alle akzeptierten Möglichkeiten, den Bereich zu ändern.

Datumsebene: Letzter Tag oder letzte 24 Stunden (Standard) Beispiel: Wenn CURRENT_DATE='2021/01/01' ist, subtrahiert der Filter einen Tag vom aktuellen Datum und formatiert es als Datetime > '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

Datumsebene: Beispiel für die letzten 2 Monate:

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

Datumsebene: Beispiel zwischen 2 Daten:

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

Zeitstempelebene: Beispiel für die letzten 12 Stunden:

Partitionieren Sie die Daten, die bis zum letzten Tag gescannt wurden, und filtern Sie dann alle Ereignisse der letzten 12 Stunden

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

Zeitstempelebene: Beispiel zwischen zwei Zeitstempeln:

Holen Sie sich Ereignisse zwischen dem 1. Januar 2021, 12:00 Uhr und dem 10. Januar 2021, 15:00 Uhr.

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

Beispiele für Standardabfragen

ams_access_session_query_v1

```
Name: ams_access_session_query_v1
```

```
Description: >-
   The query provides more information on specific AMS access session.
   The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   By default; the query filter last day events only, the user can change the datetime
 filter to search for more wide time range.
   By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
 that line.

AthenaQueryString: |-
   /*
     The query provides list of AMS access sessions during specific time range.
     The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
     If you want to only show access sessions for a particular IAM principal ID, remove
 the double-dash (--) from
     the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
 the placeholder "<IAM PrincipalId>" with the specific ID that you want.
     You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.

     By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
     remove the "useragent" filter in the WHERE clause of the query.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionId",
      eventtime AS "EventTime",
      eventname AS "EventName",
      awsregion AS "EventRegion",
```

```
      eventid AS "EventId",
      json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
      json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
      json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
      json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND eventname = 'AssumeRole'
      AND useragent = 'access.managedservices.amazonaws.com'
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
```

```
      awsRegion as EventRegion,
      eventID as EventId,
      requestParameters.tags.0.value as BusinessNeed,
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
```

```
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
```

```
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
```

```
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
```

```
    eventname = 'SetDefaultPolicyVersion'
  )
  AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
  The query provides list of events done on specific resource.
  The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
  By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
  /*
    The query provides list of events done on specific resource.

    The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
    and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
    Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

    By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
  */

  SELECT
     useridentity.principalId AS "IAM PrincipalId",
     useridentity.accesskeyid AS "IAM SessionId",
     useridentity.accountid AS "AccountId",
     reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
     eventname AS "EventName",
     awsregion AS "EventRegion",
     eventid AS "EventId",
     eventsource AS "EventService",
```

```
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
```

```
   | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
```

```
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.
```

```
    The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
    and returns all IAM Principal IDs by that requester during a specific time range.

    By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
  */

  SELECT
     json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
     json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
     eventtime AS "EventTime"
  FROM
      "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
  WHERE
     datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
     AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
  ORDER BY eventtime

InsightsQueryString: |-
  # The query provides list of IAM Principal IDs for a specific requester.
  #
  # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
  # and returns all IAM Principal IDs by that requester during a specific time range.
  #
  # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
  filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
  | sort eventTime desc
  | fields
     responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
     responseElements.credentials.accessKeyId as IAMSessionId,
     eventTime as EventTime
```

Datensatzberechtigungen ändern

Die folgenden Berechtigungen sind erforderlich, um Abfragen zum Ändern von Datensätzen auszuführen:

- Athena
  - Athene: GetWorkGroup
  - Athene: StartQueryExecution
  - Athene: ListDataCatalogs
  - Athene: GetQueryExecution
  - Athene: GetQueryResults
  - Athene: BatchGetNamedQuery
  - Athene: ListWorkGroups
  - Athene: UpdateWorkGroup
  - Athene: GetNamedQuery
  - Athene: ListQueryExecutions
  - Athene: ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS Schlüssel-ID von AMSCloud TrailLogManagement oder Ihre AWS KMS Schlüssel-ID (en), wenn Accelerate Ihren Amazon S3 S3-Bucket-Datenspeicher für CloudTrail Trail-Ereignisse mit SSE-KMS-Verschlüsselung verwendet.
- AWS Glue
  - Klebstoff: GetDatabase
  - kleben: GetTables
  - kleben: GetDatabases
  - kleben: GetTable
- Amazon S3 S3-Lesezugriff
  - Amazon S3 CloudTrail S3-Bucket-Datenspeicher: ams-a *`AccountId`* -cloudtrail- oder Ihr Amazon S3 S3-Bucket-Name*`primary region`*, CloudTrail Trail-Ereignisse Amazon S3 S3-Bucket-Datenspeicher.
- Amazon S3 S3-Schreibzugriff

- Ergebnisse der Athena-Ereignisabfrage Amazon S3 S3-Bucket: *AccountId* ams-a athena-results- *primary region*

AWS Systems Manager in Accelerate

Ein AWS Systems Manager Dokument (SSM-Dokument) definiert die Aktionen, die Systems Manager mit Ihren AWS Ressourcen durchführt. Systems Manager enthält mehr als ein Dutzend vorkonfigurierte Dokumente, die Sie verwenden können, indem Sie zur Laufzeit Parameter angeben. Dokumente verwenden JavaScript Object Notation (JSON) oder YAML und enthalten Schritte und Parameter, die Sie angeben.

AWS Managed Services (AMS) ist ein vertrauenswürdiger Herausgeber für SSM-Dokumente. SSM-Dokumente, die sich im Besitz von AMS befinden, werden nur mit integrierten AMS-Konten geteilt, beginnen immer mit einem reservierten Präfix (AWSManagedServices-*) und werden in der Systems Manager Manager-Konsole als Eigentum von Amazon angezeigt. Der AMS-Prozess für die Entwicklung und Veröffentlichung von SSM-Dokumenten folgt den bewährten AWS-Methoden und erfordert mehrere Peer-Reviews während des gesamten Dokumentenlebenszyklus. Weitere Informationen zu bewährten AWS-Methoden für die gemeinsame Nutzung von SSM-Dokumenten finden Sie unter Bewährte Methoden für gemeinsam genutzte SSM-Dokumente.

Verfügbare AMS Accelerate SSM-Dokumente

AMS Accelerate SSM-Dokumente stehen ausschließlich AMS Accelerate-Kunden zur Verfügung und werden verwendet, um den betrieblichen Arbeitsablauf zur Verwaltung Ihres Kontos zu automatisieren.

Die verfügbaren AMS Accelerate SSM-Dokumente finden Sie unter: AWS-Managementkonsole

1. Öffnen Sie die Systems Manager-Konsole an der Konsole.AWS Systems Manager
2. Wählen Sie Mit mir geteilt.
3. Filtern Sie in der Suchleiste nach dem Präfix für den Dokumentnamen und anschließend nach „Gleich“ und setzen Sie den Wert auf AWSManagedDienste-.

   AWS CLI Anweisungen finden Sie unter Geteilte SSM-Dokumente verwenden.

AMS Accelerate SSM-Dokumentversionen

SSM-Dokumente unterstützen die Versionierung. AMS Accelerate SSM-Dokumente können nicht vom Kundenkonto aus geändert und nicht erneut geteilt werden. Sie werden zentral von AMS Accelerate verwaltet und verwaltet, um das Konto zu verwalten.

Die Versionsnummern werden mit jeder Aktualisierung des Dokuments in einer bestimmten AWS-Region erhöht. Wenn neue Regionen verfügbar werden, kann derselbe Dokumentinhalt in zwei Regionen unterschiedliche Versionsnummern haben. Dies ist typisch und bedeutet nicht, dass sich ihr Verhalten unterscheidet. Wenn Sie zwei AMS Accelerate SSM-Dokumente vergleichen möchten, empfehlen wir, ihre Hashes mit den folgenden zu vergleichen: AWS CLI

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Zwei SSM-Dokumente sind identisch, wenn ihre Hashes übereinstimmen.

Systems Manager-Preise

Für den Zugriff auf AMS Accelerate SSM-Dokumente fallen keine Kosten an. Die Laufzeitkosten variieren je nach Art des SSM-Dokuments, seinen Schritten und der Laufzeitdauer. Weitere Informationen finden Sie unter AWS Systems Manager Preise.

Dokumentenverlauf für AMS Accelerate User Guide

In der folgenden Tabelle werden die wichtigen Änderungen in den einzelnen Versionen des AMS Accelerate-Benutzerhandbuchs beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Der AWS CloudTrail Abschnitt „Protokollverwaltung“ wurde aktualisiert	Neue Informationen und Hinweise zur AWS CloudTrail Protokollierung.	25. September 2025
Es wurden 4 neue Trusted Advisor Kostenoptimierungsprüfungen hinzugefügt, die von Trusted Remediator unterstützt werden	Die folgenden Kostenoptimierungsprüfungen wurden hinzugefügt: • c1z7kmr00n — Amazon-Empfehlungen zur Kostenoptimierung für Instances EC2 • c1z7kmr02n — Empfehlungen zur Amazon EBS-Kostenoptimierung für Volumen • c1z7kmr03n — Empfehlungen zur Amazon RDS-Kostenoptimierung für DB-Instances • c1z7kmr05n — Empfehlungen zur Kostenoptimierung für Funktionen AWS Lambda	22. September 2025
Der Veraltungshinweis für den Change Record-Service wurde aktualisiert	Der Veraltungshinweis für den Change Record-Service wurde mit alternativen Lösungen aktualisiert.	11. September 2025

Aktualisierte Trusted Advisor Sicherheitsüberprüfungen, die von Trusted Remediator unterstützt werden	Die unterstützten vorkonfig urierten Parameter und Einschränkungen für die Prüfung Hs4Ma3G108 aktualisiert — CloudTrail Trails sollten in Amazon Logs integriert werden CloudWatch	5. September 2025
Aktualisierte Trusted Advisor Sicherheitsüberprüfungen, die von Trusted Remediator unterstützt werden	Die Trusted Advisor Sicherhei tsüberprüfung wurde aktualisi ert, sodass Version 2 von Hs4Ma3G184 hinzugefügt wurde. Die Protokollierung von Application Load Balancers und Classic Load Balancers sollte aktiviert sein	5. September 2025
Aktualisierte Prüfungen der Trusted Advisor betriebli chen Exzellenz, unterstützt durch den Bereich Trusted Remediator	Die von Trusted Remediator unterstützten Prüfungen zur Trusted Advisor betrieblichen Exzellenz wurden aktualisiert und um die neue unterstützte Prüfung c1fd6b96l4 Amazon S3 Access Logs Enabled hinzugefügt.	28. August 2025
Der Bereich Trusted Remediator wurde aktualisiert und enthält nun neue Inhalte für Compute Optimizer	Der Abschnitt Trusted Remediator wurde aktualisiert und enthält nun neue Inhalte für unterstützte Empfehlungen. AWS Compute Optimizer	18. August 2025
Link zum TOC-Glossar wurde entfernt	AWS Glossar.	8. August 2025
Link zum TOC-Glossar wurde entfernt	AWS Glossar.	8. August 2025

Neues Feld im Patch Daily-Bericht	Instance-Tags: Die mit der EC2 Amazon-Instance-ID verknüpften Tags.	8. August 2025
Neue Trusted Remediator-Prüfungen	Trusted Advisor Kostenoptimierungsprüfungen werden durch Trusted Trusted Advisor Remediator-Sicherheitsprüfungen unterstützt, die von Trusted Remediator AWSManagedServices-TerminateEC Hs4Ma3G120—2, Hs4Ma3G230—2 und c18d2gz150—2 InstanceStoppedForPeriodOfTime unterstützt werden. AWSManagedServices-TrustedRemediator EnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	8. August 2025
Aktualisierung des IAM-Standards in Punkt 3.2	Der Wortlaut wurde geklärt und die Erwähnung von Tagging gestrichen.	25 Juli 2025
Die Resource Tagger-Konfigurationsprofile wurden in Accelerate aktualisiert	Ein neuer AvailabilityZone Filter wurde in den Resource Tagger-Konfigurationsprofilen in Accelerate hinzugefügt.	25 Juli 2025
Aktualisierte Vorfallberichte, Serviceanfragen und Abrechnungsfragen in Accelerate.	Die Verweise auf die Servicestufen Plus und Premium wurden durch einen Link zur Service-SLA ersetzt.	25 Juli 2025

Das Incident-Management in Accelerate wurde aktualisiert.	Aktualisierte Informationen zu Operations Centern.	25 Juli 2025
Die Seite mit AMS-Mustern wurde mit den richtigen Links aktualisiert.	Die SLA- und SLO-Links wurden behoben.	25 Juli 2025
Aktualisierung der Optionen zur Deaktivierung von Alarmen	Wenn Sie ein Tag hinzufüge n, können Sie sich von zwei weiteren Benachrichtigungen abmelden.	25 Juli 2025
Neue Funktion für Backups	Passen Sie Benachric htigungen in Backup-Tresoren mit einem neuen Tag an.	25 Juli 2025
Der Abschnitt für unterstützte Konfigurationen in Accelerate wurde aktualisiert	Die unterstützten Konfigura tionen für unterstützte Betriebssysteme und unterstüt zte Betriebssysteme mit dem Ende des Support (EOS) wurden in Accelerate aktualisi ert.	26. Juni 2025
Die Seite „Tags verwalten“ für das Patch-Management in Accelerate wurde entfernt	Die Seite Tags für das Patch-Management in Accelerate verwalten wurde entfernt, da diese Funktion veraltet ist.	19. Juni 2025
Wichtiger Sicherheitshinweis zur Patchverwaltung für alternative Patch-Repositorys.	Wichtiger Sicherheitshinweis und bewährte Methoden für die Verwendung alternativer Patch-Repositorys in AMS Accelerate.	10. Juni 2025
AMS Accelerate Change Record ist veraltet.	Der AMS Accelerate Change Record-Service ist mit Wirkung zum 1. Juli 2025 veraltet.	27. Mai 2025

Unterstützte Betriebssystem-Updates.	Von AMS Accelerate unterstützte Betriebssysteme wurden aktualisiert, einige hinzugefügt, andere entfernt.	22. Mai 2025
Hinweis für unterstützte Dienste in der Region Naher Osten (VAE).	Eingeschränkte Unterstützung für einige Dienste in der Region Naher Osten (VAE).	22. Mai 2025
Nur intern. APIs	Nur intern, die in einigen APIs Protokollen vorkommen. CloudWatch	22. Mai 2025
Fehlende Protokollspeicherorte hinzugefügt.	Einige fehlende Windows-Protokollspeicherorte wurden hinzugefügt.	22. Mai 2025
AMS Accelerate Trusted Remediator-Aktualisierungen.	So verwenden Sie einen neuen Parameter`preconfigured-parameters` , um Trusted Advisor Prüfungen in Trusted Remediator anzupassen.	22. Mai 2025
Häufig gestellte Fragen und Updates zu AMS Accelerate Trusted Remediator.	Verschiedene Aktualisierungen der unterstützten Trusted Advisor Prüfungen , häufig gestellte Fragen zu Trusted Remediator (hinzugefügt „Welche Ressourcen stellt Trusted Remediator für Ihre Konten bereit?“) und mehr. Siehe auch Trusted Advisor Prüfungen, die von Trusted Remediator unterstützt werden.	8. Mai 2025

Aktualisierung der Sicherheitskontrollen für AMS Accelerate Standard.	Steuerelemente für die gemeinsame Nutzung von Sicherheitsgruppen wurden hinzugefügt.	8. Mai 2025
Beschleunigen Sie die Aktualisierung der Überwachungswarnungen.	Zusätzliche Benachrichtigungen wurden hinzugefügt und der Name der Warnung wurde zur Spalte „Notizen“ hinzugefügt.	28. April 2025
Beschleunigen Sie die Ressourceninventur.	Die Tabellendatei für das Ressourceninventar (komprimiert) wurde aktualisiert.	24. April 2025
Beschleunigen Sie die Protokollspeicherorte.	Zusätzliche Protokollspeicherorte wurden hinzugefügt.	24. April 2025
Beschleunigen Sie die Einführung neuer Rollen und Verantwortlichkeiten (RACI) für die Reaktion auf Sicherheitsvorfälle.	RACI für die Reaktion auf Sicherheitsvorfälle.	27. März 2025
Beschleunigen Sie die neue automatische Problembehebungswarnung von Amazon RDS.	Alert-ID: - 0224, wird ausgelöst, wenn der angeforderte zugewiesene Speicherplatz den konfigurierten maximalen Speicherschwellenwert erreicht oder überschreitet.	27. März 2025
Beschleunigen Sie die Aktualisierung der Onboarding-Rollenvorlage.	Die Rollenvorlage für AMS Accelerate Onboarding wurde aktualisiert, um GovCloud AWS-Regionen zu unterstützen.	25. März 2025

Beschleunigen Sie die RDS-Warnung für neue automatische Korrekturen.	RDS-EVENT-0224 hinzugefügt.	17. März 2025
Accelerate Neue Funktion: Benachrichtigungen bei Vorfällen.	Sie können AppRegistry damit Anwendungen erstellen und die Benachrichtigungen zu Vorfällen für diese Anwendungen anpassen.	13. März 2025
Beschleunigen Sie die Aktualisierung auf den Schwellenwert für die RDS-Alarmüberwachung.	Der Alarmschwellenwert für die durchschnittliche RDS-CPU-Auslastung wurde von 75 auf 90% geändert.	20. Februar 2025
Beschleunigen Sie das Update auf die Tabelle mit der automatischen AMS-Problembehebung.	Die Tabelle zur Behebung von Warnmeldungen wurde um neue Inhalte erweitert.	20. Februar 2025
Accelerate Neue Funktion: Alarme speichern.	Sie können den Alarm Manager so konfigurieren, dass Alarme gespeichert werden, CloudWatch anstatt sie automatisch zu löschen.	20. Februar 2025

Aktualisierte Self-Service-Berichte mit neuen Datenoptionen für die Anzeige aggregierter Berichte	`Trusted AWS Organization account enabled by the customer`Für die folgenden Self-Service-Berichte wurden die neuen Datenoptionen „Feldname :“`Admin Account ID`, „Datensatz-Feldname: **`aws_admin_account_id`** “ und „Definition:“ hinzugefügt: • Patch-Bericht (täglich) • Backup-Bericht (täglich) • Vorfallbericht (wöchentlich) • Resource Tagger-Dashboard • Dashboard „Regeln für Sicherheitskonfigurationen“	28. Januar 2025

Zusätzliche AWS Trusted Advisor Prüfungen wurden hinzugefügt, die von Trusted Remediator unterstützt werden	Die folgenden Trusted Advisor Prüfungen werden jetzt von Trusted Remediator unterstützt:
	• Kostenoptimierung
	  • c1cj39rr6v — Konfiguration zum Abbruch eines unvollständigen mehrteiligen Uploads in Amazon S3
	• Sicherheit
	  • Hs4Ma3G199 — RDS-DB-Instances sollten Protokolle in Logs veröffentlichen CloudWatch
	  • Hs4Ma3G326 — Die Amazon EMR-Einstellung zum Blockieren des öffentlichen Zugriffs sollte aktiviert sein
	  • Hs4Ma3G272 — Benutzer sollten keinen Root-Zugriff auf KI-Notebook-Instances haben SageMaker
	  • Hs4Ma3G325 — Bei EKS-Clustern sollte die Auditprotokollierung aktiviert sein
	  • HHs4Ma3G118 - VPC-Standardsicherheitsgruppen sollten keinen eingehenden oder
		28. Januar 2025

ausgehenden Datenverkehr zulassen

- Hs4Ma3G127 - API-Gateway-REST- und WebSocket API-Ausführungsprotokollierung sollten aktiviert sein
- Hs4Ma3G124 — EC2 Amazon-Instances sollten Instance Metadata Service Version 2 () verwenden IMDSv2

- Fehlertoleranz
  - c1qf5bt013 — Bei Amazon RDS-DB-Instances ist die auto Speicherskalierung deaktiviert
  - 7q GXs KIUw — Classic Load Balancer Balancer-Verbindungsabbau
  - c18d2gz106 — Amazon EBS nicht im Plan enthalten AWS Backup
  - c18d2gz107 — Amazon DynamoDB-Tabelle nicht im Plan enthalten AWS Backup
  - cc18d2gz117 — Amazon EFS nicht im Plan enthalten AWS Backup
  - c18d2gz105 — Netzwerklastenausgleichsdienst — Cross-Load-Balancing

        - c1qf5bt026 — Der Amazon RDS-Parameter synchronous_commit ist ausgeschaltet
        - c1qf5bt030 — Der Amazon RDS-Parameter innodb_flush_log_at_trx_commit ist nicht 1
        - c1qf5bt031 — Der Amazon RDS-Parameter sync_binlog ist ausgeschaltet
        - c1qf5bt036 — Amazon RDS-Parametereinstellung innodb_default_row_format ist unsicher
        - c18d2gz144 — Detaillierte Amazon-Überwachung nicht aktiviert EC2
    - Operational Excellence
        - c18d2gz125 — Amazon API Gateway protokolliert keine Ausführungsprotokolle
        - c18d2gz168 — Elastic Load Protection ist für Load Balancer nicht aktiviert Balancing Deletion
        - c1qf5bt012 — Amazon RDS Performance Insights ist ausgeschaltet
    - Performance

	• c1qf5bt021 — Amazon RDS-Parameter innodb_change_buffering, der weniger als den optimalen Wert verwendet • c1qf5bt025 — Der Amazon RDS-Autovacuum-Parameter ist ausgeschaltet • c1qf5bt028 — Der Amazon RDS-Parameter enable_indexonlyscan ist ausgeschaltet • c1qf5bt029 — Der Amazon RDS-Parameter enable_indexscan ist ausgeschaltet • c1qf5bt032 — Der Amazon RDS-Parameter innodb_stats_persistent ist ausgeschaltet • c1qf5bt037 — Der Amazon _logging-Parameter ist aktiviert RDSgeneral	
Die Tabelle mit dem Ressourceninventar wurde aktualisiert	Die Tabelle mit dem Ressourceninventar wurde aktualisiert.	23. Januar 2025

Neue AMS-Funktion: Aggregierte Self-Service-Berichte	Aggregierte Self-Service-Berichte (SSR) bieten Ihnen einen Überblick über bestehende Self-Service-Berichte, die auf Organisationsebene kontenübergreifend aggregiert wurden.	21. Januar 2025
Neue Funktion zum Beschleunigen von Patches: Patch Hooks	Verwenden Sie diese Funktion, um „Hooks“ mit SSM-Befehlsdokumenten zu konfigurieren, um Befehle auf Betriebssystemebene vor oder nach dem Patchen auszuführen.	16. Januar 2025
Aktualisierung des Abschnitts „So funktioniert die Überwachung“	Es wurden Informationen zu einer neuen Funktion hinzugefügt, mit der Warnmeldungen nach Ressourcen- oder Instanz-ID statt nach Vorfall konfiguriert werden.	8. Januar 2025
Aktualisierung des Onboarding-Bereichs von EKS Monitoring and Incident Management	Der Hinweis zum Onboarding-Verfahren wurde aktualisiert, um klarzustellen, wann Warnsignale ausgesetzt und wieder aufgenommen werden.	19. Dezember 2024
Das Mitgliedskontoprotokoll wurde zu Trusted Remediator hinzugefügt	Sie können das Mitgliedskontenprotokoll verwenden, um die Konto-ID, das Onboarding AWS-Regionen und die Ausführungszeit jedes Mitgliedskontos zu ermitteln.	19. Dezember 2024

Voraussetzungen für die Verwendung des SSM-Agenten	Der Inhalt zum Blockieren von ausgehendem Verkehr wurde aktualisiert.	4. Dezember 2024
Accelerate Monitoring and Incident Management für EKS wird jetzt im asiatisch-pazifischen Raum (Hongkong) unterstützt AWS-Region	Der asiatisch-pazifische Raum (Hongkong) wird jetzt von Accelerate Monitoring and Incident Management für EKS unterstützt	21. November 2024
Die Tabelle mit den Angeboten für Operations On Demand wurde aktualisiert	Die folgenden Betriebssysteme werden für direkte Upgrades unterstützt: • Microsoft Windows 2016 bis Microsoft Windows 2022 und höher	11. November 2024
Accelerate Monitoring and Incident Management für EKS wird jetzt in Afrika (Kapstadt) unterstützt AWS-Region.	Afrika (Kapstadt) wird jetzt von Accelerate Monitoring and Incident Management für EKS unterstützt	4. November 2024

Die Tabelle mit den Operations On Demand-Angeboten wurde aktualisiert	Die folgenden Betriebssysteme werden für direkte Upgrades unterstützt: • Microsoft Windows 2012 R2 auf Microsoft Windows 2016 und höher • Von Red Hat Enterprise Linux 7 auf Red Hat Enterprise Linux 8 • Von Red Hat Enterprise Linux 8 auf Red Hat Enterprise Linux 9 • Von Oracle Linux 7 auf Oracle Linux 8	1. November 2024
Schnellstart-Vorlage aktualisiert	Das Diagramm, die Vorlagenparameter und die Yaml-Vorlagendatei wurden aktualisiert.	28. Oktober 2024

Trusted Advisor Prüfungen wurden zu Trusted Remediator in AMS hinzugefügt	Die folgenden Trusted Advisor Prüfungen sind jetzt in Trusted Remediator verfügbar: • Z4 AUBRNSmz — Nicht verknüpfte Elastic IP-Adressen • c18d2gz128 — Amazon ECR-Repository ohne konfigurierte Lebenszyklusrichtlinie • c18d2gz138 - DynamoDB-Wiederherstellung Point-in-time • Hs4Ma3G323 — In Dynamo sollte der Löschschutz aktiviert sein DBtables • Hs4Ma3G247 — Amazon EC2 Transit Gateway sollte VPC-Anhangsanfragen nicht automatisch akzeptieren • Hs4Ma3G308 — Bei Amazon DocumentDB-Clustern sollte der Löschschutz aktiviert sein • Hs4Ma3G299 - Bei Neptune-DB-Clustern sollte der Löschschutz aktiviert sein • Hs4Ma3G306 — Manuelle Cluster-Snapshots von Amazon DocumentDB sollten nicht öffentlich sein • Hs4Ma3G109 — Die Überprüfung der Protokoll	25. Oktober 2024

	datei sollte aktiviert sein CloudTrail • Hs4Ma3G217 — CodeBuild Projektumgebungen sollten eine protokollierende AWS-Konfiguration haben4 • Hs4Ma3G158 — SSM-Dokumente sollten nicht öffentlich sein • Hs4Ma3G319 — Bei Netzwerk-Firewall-Firewalls sollte der Löschschutz aktiviert sein	
Unterstützte Konfigurationen wurden aktualisiert	Die unterstützten Oracle Linux-Betriebssysteme wurden auf 9.0-9.3, 8.0-8.9, 7.5-7.9 aktualisiert.	24. Oktober 2024
Ein neuer Abschnitt von AMS Accelerate wurde zu Offboard hinzugefügt	Anweisungen zum Offboardi ng mit den Abhängigkeiten von Alarm Manager und Resource Tagger wurden zu Offboard von AMS Accelerate hinzugefü gt.	24. Oktober 2024
Das Resource Tagger-Da shboard ist jetzt verfügbar.	Das Resource Tagger-Da shboard ist jetzt in Self-Serv ice-Berichten verfügbar.	26. September 2024
Sie können jetzt mehrere E-Mail-Adressen in tagbasier te Benachrichtigungen aufnehmen.	In tagbasierten Benachric htigungen werden jetzt mehrere E-Mail-Adressen unterstützt.	20. September 2024

AMS Accelerate-Grenzwerte sind jetzt im AMS-Patch-Management enthalten.	AMS Accelerate-Grenzwerte sind in Patch Management — Patch-Wartungsfenster erstellen enthalten.	30. August 2024
Update für AMS Accelerate Account Discovery	In Account Discovery wurde ein neuer Abschnitt für die Amazon EC2 Instance Evaluation hinzugefügt.	29. August 2024
Die Standard-Patch-Baseline von AMS Accelerate ist jetzt für Ubuntu-Betriebssysteme verfügbar.	Die Standard-Patch-Baseline von AMS Accelerate ist jetzt für Ubuntu-Betriebssysteme verfügbar.	22. August 2024
Update für AMS Accelerate Account Discovery	Vier neue AWS API-Aufrufe wurden dem Abschnitt „ AWS CloudTrail Evaluierung“ in der Tabelle mit den Betriebsprüfungen hinzugefügt.	2. August 2024
Trusted Remediator unterstützt jetzt eine zusätzliche Prüfung	Trusted Remediator unterstützt jetzt die Sicherheitsüberprüfung Hs4Ma3G192 — RDS-DB-Instances sollten den öffentlichen Zugriff verbieten.	30. Juli 2024
AMS unterstützt jetzt Amazon Route 53 Resolver DNS Firewall	AMS unterstützt jetzt Amazon Route 53 Resolver DNS Firewall	30. Juli 2024
AMS Accelerate onboarding_role_minimal.zip enthält jetzt Terraform-Code	AMS Accelerate onboarding_role_minimal.zip enthält jetzt Terraform-Code.	30. Juli 2024

Dashboard mit Regeln für Sicherheitskonfigurationen	Das Security Config Rules Dashboard ist jetzt in der Self-Service-Berichterstattung verfügbar.	24. Juli 2024
AMS Accelerate unterstützt jetzt Oracle Linux 8.9, RHEL 8.10 und RHEL 9.4.	AMS Accelerate unterstützt jetzt Oracle Linux 8.9, RHEL 8.10 und RHEL 9.4.	5. Juli 2024
Der Prozess zur Kontoermittlung bei AMS Accelerate wurde aktualisiert.	Der Prozess zur Kontoermittlung, der beim Onboarding bei AMS Accelerate verwendet wurde AWS-Konten , wurde aktualisiert.	1. Juli 2024
Trusted Remediator ist jetzt verfügbar.	Trusted Remediator, eine AWS Managed Services Services-Lösung, die die Behebung von AWS Trusted Advisor Prüfungen automatisiert, ist jetzt verfügbar.	24. Juni 2024
DNS-Firewall-Ereignisse von Amazon Route 53 Resolver in Security Incident Response.	AMS überwacht jetzt DNS-Firewall-Ereignisse von Amazon Route 53 Resolver in Security Incident Response	21. Juni 2024
Unterstützte Betriebssysteme wurden aktualisiert	AMS Accelerate unterstützt jetzt AlmaLinux 8.3-8.9, 9.0-9.2 (AlmaLinux wird nur mit der x86-Architektur unterstützt)	19. Juni 2024
Das Limit für automatische Instanzprofile wird jetzt erhöht, wenn die Standardeinstellung eingehalten wird.	AMS erhöht jetzt das standardmäßige Limit für Instanzprofile auf 20, wenn das Standardlimit von 10 erreicht wird.	18. Juni 2024

Die automatische Installat ionsfunktion des AMS SSM Agents ist jetzt standardmäßig aktiviert.	Die automatische Installat ionsfunktion des AMS SSM Agents ist standardmäßig für Konten aktiviert, die nach dem 06.03.2024 eingerichtet wurden.	7. Juni 2024
Häufig gestellte Fragen zur Sicherheit wurden zur Sicherheitsverwaltung hinzugefügt.	Es ist jetzt eine häufig gestellte Frage zur Sicherheit verfügbar , die häufig gestellte Fragen zu bewährten Sicherhei tsmethoden, Kontrolle n, Zugriffsmodellen und Prüfmechanismen behandelt , die verwendet werden, wenn ein AMS-Betriebsingenieur oder ein Automatisierungste chniker auf Ihre Konten zugreift.	3. Juni 2024
Zusätzliche AWS Regionen werden jetzt von Monitoring and Incident Management für Amazon EKS unterstützt.	Drei weitere AWS Regionen werden jetzt von Monitoring and Incident Management für Amazon EKS unterstützt.	23. Mai 2024
Patch-Benachrichtigungen über Serviceanfragen werden jetzt vor Beginn des Patch-Wartungsfensters gesendet.	AMS Accelerate Patching erstellt 4 Tage vor Beginn des Patch-Wartungsfensters eine neue Serviceanfrage. Sie können die Servicean frage verwenden, um mit AMS zu kommunizieren, um Anpassungen am Patch vorzunehmen oder einen Patch zu überspringen.	3. Mai 2024

Warnschwellenwerte wurden der Tabelle mit den Basiswarnungen für die AMS Accelerate EKS-Überwachung hinzugefügt.	Detaillierte Schwellenwerte für Warnmeldungen sind jetzt in der Tabelle mit den Basiswarnungen für die Amazon EKS-Überwachung verfügbar.	3. Mai 2024
Aktualisiert: Alarm Manager-Konfigurationsprofile.	Es wurden Hinweise zur Erstellung von Alarmen bei der Erkennung von Anomalien mit dem Alarm Manager hinzugefügt.	25. April 2024
Ergänzungen zu den Resource Tagger-Konfigurationsprofilen.	DynamoDB-Tabellen und Amazon S3 S3-Buckets sind jetzt in Resource Tagger verfügbar	25. April 2024
Informationsbereich für Planned Event Management (PEM) hinzugefügt.	Detaillierte Informationen zum PEM-Serviceangebot sind jetzt im AMS Accelerate-Benutzerhandbuch verfügbar.	25. April 2024
AMS unterstützt Red Hat Enterprise Linux (RHEL) 9.x.	AMS unterstützt Red Hat Enterprise Linux (RHEL) 9.x.	25. April 2024
AMS Accelerate unterstützt die Berichterstattung für alle AWS Regionskonfigurationen.	AMS Accelerate unterstützt SSM-Inventarberichte für alle AWS Regionskonfigurationen.	25. April 2024
Aktualisiert: AWS verwaltete Richtlinien.	Das wurde AWSManagedServicesDeploymentToolkitPolicy mit neuen ECR-Berechtigungen aktualisiert.	4. April 2024
Aktualisiert: Abschnitt „Resource Tagger-Konfigurationsprofile“	`AWS::EFS::FileSystem` Zur ResourceTypeListe hinzugefügt.	21. März 2024

Aktualisiert: Berichte über Vorfälle und Serviceanfragen im Bereich Accelerate.	Der Titel des Themas wurde in Accelerate in Incident-Berichte, Serviceanfragen und Abrechnungsfragen geändert. Ein neuer Abschnitt , Fragen zur Abrechnung, wurde hinzugefügt.	21. März 2024
Aktualisiert: Abschnitt „So funktioniert die Verwaltung von Serviceanfragen“.	Es wurde klargestellt, wie AMS mit Serviceanfragen umgeht, die eine Funktionsanfrage oder einen Fehler enthalten.	21. März 2024
Aktualisiert: Die Rolle aws_managedservices_onboarding_role mit Abschnitt erstellen CloudFormation	Befehle zum Erstellen der Rolle hinzugefügt. AWS CloudShell	21. März 2024
Aktualisiert: (Optionale) Schnellstart-Vorlage	Befehle zum Herunterladen der Vorlage wurden hinzugefügt AWS CloudShell.	21. März 2024
Neue Ressourcentypen sind für Alarm Manager-Konfigurationsprofile verfügbar.	Ressourcentypen für Amazon FSx, Amazon EFS und Elasticsearch wurden den Alarm Manager-Konfigurationsprofilen hinzugefügt.	21. März 2024
Zusätzliche Substitutionen von Pseudoparametern sind für das Konfigurationsprofil verfügbar.	Amazon EFS- und FSx Amazon-Pseudoparameter-Substitutionen hinzugefügt.	21. März 2024
Im Thema Servicebeschreibung wurde ein neuer Abschnitt zu den Funktionen hinzugefügt.	Ein neuer Abschnitt, Verwaltung von Serviceanfragen, wurde unter den Funktionen von AMS Accelerate hinzugefügt.	21. März 2024

Dem wöchentlichen Incident-Bericht zur Self-Service-Berichterstattung wurden neue Spalten hinzugefügt	Dem Bericht „Wöchentliche Vorfälle“ wurden neue Spalten hinzugefügt, sodass Sie nach Vorfällen nach dem Quartal, Monat, Woche oder Tag filtern können, an dem der Vorfall erstellt oder gelöst wurde.	11. März 2024

Frühere Aktualisierungen

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation des AMS Accelerate-Handbuchs vor März 2024 beschrieben.

Änderungen	Beschreibung	Datum
Verbesserungen für das CloudTrail Trail-Onboarding von AMS Accelerate	Verbesserungen für AMS Accelerate CloudTrail Trail Onboarding: • Sammeln Sie alle Bucket-Richtlinien in einem einzigen Block • Entfernen Sie die zweite AWS Organisations-ID aus den Richtlinienerklärungen • Klären Sie die Anforderungen an die Kundenumgebung Weitere Informationen finden Sie unter Überprüfen und aktualisieren Sie Ihre Konfigurationen, damit AMS Accelerate Ihren CloudTrail Trail nutzen kann.	23. Februar 2024
Aktualisiert: Onboarding-Prozess für das Konto.	Der Abschnitt zum Onboarding-Prozess für das Konto wurde neu strukturiert, um die Schritte klarer zu gestalten. Außerdem wurde eine optionale Schnellstart-Vorlage für Onboarding-Funktionen hinzugefügt.	22. Februar 2024

Änderungen	Beschreibung	Datum
	Siehe (Optional) Schnellstart-Vorlage in Accelerate.	
Aktualisiert: Offboarding AMS Accelerate.	Der Abschnitt mit den Überlegungen zum Offboarding bei AMS Accelerate wurde aktualisiert und weist nun darauf hin, dass der `ams-access-management` CloudFormation Stack und die `ams-access-management` IAM-Rolle nicht durch den Offboarding-Prozess gelöscht werden. Siehe Die Offboarding-Effekte von AMS Accelerate.	22. Februar 2024
Aktualisiert: Konformität mit der Konfiguration in Accelerate.	Sofern zutreffend, wurde „Incident Report“ in „Service Request“ geändert, um Unklarheiten in Bezug auf diese Bedingungen zu vermeiden. Siehe Konformität mit der Konfiguration in Accelerate.	22. Februar 2024
Aktualisiert: Kontoerkennung in Accelerate.	Die Kontoermittlung in Accelerate wurde neu organisiert, um die Voraussetzungen für Gruppen mit dem entsprechenden Abschnitt zu verbessern. Siehe Schritt 1. Kontoermittlung in Accelerate.	22. Februar 2024
Umbenannt: AMS-Patch-Berichterstattung an die AMS-Hostverwaltung.	AMS-Patch-Reporting wurde in AMS-Host-Management umbenannt und der Bericht, Patch-Details-Bericht, in SSM Agent Coverage Report umbenannt. Siehe AMS-Host-Management-Berichte.	22. Februar 2024

Änderungen	Beschreibung	Datum
Der Katalog „Operations on Demand“ wurde aktualisiert	Die Tabelle mit den Angeboten von Operations on Demand wurde aktualisiert und enthält nun keine Verweise auf „Health“ mehr`Amazon EKS cluster maintenance` . Siehe AMS Operations on Demand anfordern.	22. Februar 2024
AMS Event Router wurde aktualisiert	Der Abschnitt `AMSCoreRule` im Bereich AMS Event Router wurde aktualisiert. Siehe Verwenden von Amazon EventBridge Managed Rules in AMS.	22. Februar 2024
Unterstützte Betriebssysteme aktualisiert.	Die unterstützten Betriebssysteme wurden um SUSE Linux Enterprise Server 15 SP5 aktualisiert. Siehe Unterstützte Konfigurationen.	22. Februar 2024
Die Automatisierung zur Behebung der EC2 Volumenauslastung wurde aktualisiert	Der Abschnitt zur Automatisierung der EC2 Volumenauslastung wurde mit dem richtigen Zeitplan für die Kapazitätserweiterung aktualisiert. Siehe EC2 Automatisierung der Behebung der Volumennutzung.	22. Februar 2024
Aktualisiert: Überprüfe und aktualisiere deine Konfigurationen, damit Accelerate deinen Trail nutzen kann CloudTrail	Der Abschnitt mit der CloudTrail S3-Bucket -Richtlinie für AMS Accelerate Organization wurde aktualisiert. Siehe Überprüfen und aktualisieren Sie Ihre Konfigurationen, damit AMS Accelerate Ihren CloudTrail Trail nutzen kann	15. Februar 2024

Änderungen	Beschreibung	Datum
Neue Funktion hinzugefügt: auto Installation des SSM-Agenten	Ein neuer Abschnitt für die auto Installation des SSM-Agenten wurde hinzugefügt Siehe Automatische Installation des SSM-Agenten.	26. Januar 2024
Aktualisiert: Unterstützte Konfigurationen	Es wurden Informationen zu den unterstützten Versionen von hinzugefügt AWS Control Tower Siehe Unterstützte Konfigurationen.	26. Januar 2024
Aktualisiert: AMS-Patch-Berichterstattung.	Drei Abschnitte wurden aus der AMS-Patch-Berichterstattung entfernt: • Bericht mit Zusammenfassung der Details zur Patch-Instanz • Bericht mit den Patch-Details • Instances, die Patches verpasst haben, melden Siehe AMS-Host-Management-Berichte.	22. Dezember 2023
Aktualisiert: Beschleunigen Sie die Voraussetzungen für das Onboarding.	Die für die Integration von AMS Accelerate erforderlichen Supportpläne wurden aktualisiert. Siehe Beschleunigen Sie die Onboarding-Voraussetzungen.	15. Dezember 2023
Aktualisiert: Erstellt ein Patch-Wartungsfenster.	Der Abschnitt „Standard-Patch-Zyklus“ wurde entfernt, da diese Funktion veraltet ist. Siehe Erstellen Sie ein Patch-Wartungsfenster in AMS.	13. Dezember 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Benachrichtigungseinstellungen in Accelerate.	Es wurde klargestellt, welche E-Mail für Benachrichtigungen verwendet wird. Weitere Informationen finden Sie unter Benachrichtigungseinstellungen in Accelerate.	12. Dezember 2023
Aktualisiert: `AMSAccelerateCustomerAccessPolicies` Vorlage.	Die `AMSAccelerateCustomerAccessPolicies` Vorlage wurde aktualisiert, um einen Syntaxfehler zu korrigieren. Weitere Informationen finden Sie unter Berechtigungen zur Nutzung von AMS-Funktionen.	12. Dezember 2023
Hinzugefügt: Sicherheitsüberprüfungen für Änderungsanfragen	Unter Sicherheitsmanagement wurde ein neuer Abschnitt „Sicherheitsüberprüfungen für Änderungsanfragen“ hinzugefügt. Weitere Informationen finden Sie unter Sicherheitsüberprüfungen für Änderungsanfragen.	11. Dezember 2023
Aktualisiert: resource_inventory.xlsx	Die Datei resource_inventory.xlsx wurde aktualisiert, sodass sie Security Analyst-Rollen enthält. Weitere Informationen finden Sie unter Ressourceninventar für Accelerate.	17. November 2023
Aktualisiert: Beschreibung der Rolle ams-access-admin-operations	Die ams-access-admin-operationsBeschreibung wurde aktualisiert. Weitere Informationen finden Sie unter Warum und wann AMS auf Ihr Konto zugreift und Authentifizierung mit Identitäten in AMS Accelerate.	17. November 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Überlegungen zum Offboarding von AMS Accelerate	Der Sicherheitsbereich wurde aktualisiert, um zu verdeutlichen, was bei Amazon erhältlich ist GuardDuty und welche AWS Config Regeln nach dem Offboarding gelten. Weitere Informationen finden Sie unter Die Offboarding-Effekte von AMS Accelerate.	17. November 2023
Hinzugefügt: Überwachung und Incident Management für Amazon EKS	Monitoring and Incident Management für Amazon EKS überwacht Ihre Amazon EKS-Ressourcen auf Ausfälle, Leistungseinbußen und Sicherheitsprobleme. Weitere Informationen finden Sie unter Überwachung und Vorfallmanagement für Amazon EKS in AMS Accelerate.	14. November 2023
Aktualisiert: Tagging	Es wurden Informationen zum vom Kunden bereitgestellten Tagging hinzugefügt. Weitere Informationen finden Sie unter Vom Kunden bereitgestellte Tags in Accelerate.	7. November 2023
Aktualisiert: Resource Tagger-Konfigurationsprofile	AWS::AutoScaling::AutoScalingGroup, AWS::EKS::Cluster, AWS::Elasticsearch ::Domain, and AWS::FSx::FileSystem Zum Abschnitt Filter hinzugefügt. Weitere Informationen finden Sie unter Resource Tagger-Konfigurationsprofile in AMS Accelerate.	27. Oktober 2023
Aktualisiert: Servicebe schreibung	Ubuntu 22.04 wurde zu den unterstützten Betriebssystemen hinzugefügt. Siehe Service description (Service-Beschreibung)	29. September 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Voraussetzungen für das Onboarding von AMS Accelerate	AMS Accelerate VPC-Endpoints wurde ein Hinweis hinzugefügt, um eine Vorlage einzubeziehen CloudFormation . Siehe Beschleunigen Sie die Onboarding-Voraussetzungen.	29. September 2023
Aktualisiert: Erkennen	Der Endpunktschutztyp wurde aus der Sicherheitslösung AMS Accelerate entfernt. Siehe Detect.	29. September 2023
Aktualisiert: Warnmeldungen von Baseline Monitoring in AMS	AWS Outposts Zur Tabelle „Alerts from Baseline Monitoring“ hinzugefügt. Siehe Detect monitoring-default-metrics.	29. September 2023
Aktualisiert: Erstellen Sie die Rolle aws_managedservices_onboarding_role mit CloudFormation	Der Screenshot für Specify Stack Details wurde aktualisiert. Siehe Erstellen `aws_managedservices_onboarding_role` mit CloudFormation for Accelerate.	29. September 2023
Aktualisiert: Von AMS Accelerate bereitgestellte Amazon EventBridge Managed Rules	Neue AMS Accelerate Amazon EventBridge Managed Rule Rule Rule AMSCoreRule hinzugefügt. AMS Accelerate Amazon EventBridge Managed Rule wurde aktualisiert AMSAccessRolesRule, um eine neue Rolle hinzuzufügen. Weitere Informationen finden Sie unter Von AMS bereitgestellte Amazon EventBridge Managed Rules.	19. September 2023
Aktualisiert: Alarm Manager-Konfigurationsprofile	AWS Outposts Pseudoparameter-Substitutions-Identifikatoren hinzugefügt. Siehe Überwachung und Eventmanagement in AMS Accelerate.	11. September 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Resource Tagger-Konfigurationsprofile	Der Ressourcentyp AWS Outposts wurde hinzugefügt. Siehe Beschleunigtes Konfigurationsprofil: Substitution von Pseudoparametern.	11. September 2023
Aktualisiert: Unterstützte Dienste	Amazon Elastic File System wurde dem Abschnitt „Von CloudWatch Alarmen überwachte Dienste“ hinzugefügt. Weitere Informationen finden Sie unter Service description (Service-Beschreibung).	6. September 2023
Aktualisiert: Patch-Überwachung und Fehlerkorrektur	Dem Abschnitt „Patch Orchestrator verwenden“ wurde der folgende Hinweis hinzugefügt: „Patch-Fehlerwarnungen werden nicht für Instanzen erstellt, deren Betriebssysteme nicht unterstützt werden oder die während des Wartungsfensters gestoppt werden“ Weitere Informationen finden Sie unter Patch-Management in AMS Accelerate verstehen.	6. September 2023
Aktualisiert: Runbook zur Reaktion auf Malware-Ereignisse wurde klargestellt	Das Runbook „Reaktion auf Malware-Ereignisse“ für die Reaktion auf Sicherheitsvorfälle wurde klarer formuliert. Weitere Informationen finden Sie unter Reaktion auf Sicherheitsvorfälle in AMS.	6. September 2023
Aktualisiert: Verbinden Sie Ihr Accelerate-Konto mit Transit Gateway	Die Schritte zum Verbinden einer neuen Accelerate-Account-VPC mit dem AMS Multi-Account Landing Zone-Netzwerk (Erstellen eines TGW-VPC-Anhangs) wurden geklärt: Weitere Informationen finden Sie unter Verbinden Ihres Accelerate-Kontos mit Transit Gateway.	5. September 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Warnmeldungen von der Basisüberwachung in AMS	Der Verweis auf zwei veraltete Alarme AMSRead LatencyAlarm und wurde entfernt. AMSWrite LatencyAlarm Weitere Informati onen finden Sie unter Warnmeldungen aus der Basisüberwachung in AMS.	5. September 2023
Hinzugefügt: AMS Event Router	Dokumentation für AMS Event Router hinzugefügt. Verwenden von Amazon EventBridge Managed Rules in AMS Weitere Informationen finden Sie unter.	5. September 2023
Aktualisiert: Liste der Alarm Manager-Pseudoparameter.	Die Liste der Alarm Manager-Pseudopara meter wurde aktualisiert. EC2 Der Parameter Instanzname wurde den Alarm-Konfigurationen für Instanzen und Festplatten hinzugefügt EC2 . EC2 Weitere Informationen finden Sie unter Beschleunigtes Konfigurationsprofil: Substitut ion von Pseudoparametern.	29. August 2023
Hinzugefügt: AMS Access Offboarding	Zusätzliche Überlegungen beim Offboarding von AMS Access wurden hinzugefügt. Siehe Die Offboarding-Effekte von AMS Accelerate.	24. August 2023
Hinzugefügt: Reaktion auf Sicherheitsvorfälle bei AMS	Dokumentation zur Verwendung von AMS Security Incident Response hinzugefügt. Siehe Reaktion auf Sicherheitsvorfälle in AMS.	18. August 2023
Aktualisiert: AMS Accelerate-Zugriffsrollen	Ein Tippfehler in den Rollennamen wurde korrigiert. Siehe AWS Identity and Access Management in AMS Accelerate.	10. August 2023
Aktualisiert: Grundsatz erklärungen	Festcodierte Rollennamen wurden durch Platzhalter ersetzt. Siehe Überprüfen und aktualisieren Sie Ihre Konfigurationen, damit AMS Accelerate Ihren CloudTrail Trail nutzen kann.	10. August 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Liste der überwachten Dienste mit EFS-Warnungen.	Die Liste der Überwachungsdienste wurde mit neuen EFS-Alerts für die AMS-Basisüberwachung aktualisiert. 4 neue EFS-Warnungstypen wurden hinzugefügt. Weitere Informationen finden Sie unter Warnmeldungen aus der Basisüberwachung in AMS.	03. August 2023
Aktualisiert: Schnellere Ressourceninventartabelle	ams-backup-config-rule-stack und zugehörige Ressourcen wurden entfernt. Siehe Ressourceninventar für Accelerate.	18. Juli 2023
Aktualisiert: AMS Accelerate-Zugriffsrollen	<8-digit hash>Die Rollen ams-backup-config-rule -st- amsBackupAlert ConfigRule - <8-digit hash>und ams-backup-config-rule -st- amsBackupPlan ConfigRule H- wurden entfernt. Siehe AWS Identity and Access Management in AMS Accelerate.	18. Juli 2023
Aktualisiert: Liste der überwachten RDS-Warnmeldungen.	Die Liste der RDS-Warnmeldungen für die AMS-Basisüberwachung wurde aktualisiert. 9 neue RDS-Warntypen wurden hinzugefügt und 3 bestehende RDS-Warntypen wurden entfernt. Weitere Informationen finden Sie unter Warnmeldungen aus der Basisüberwachung in AMS.	19. Juni 2023
Neu: AMS Accelerate-Zugriffsrollen	Neue Zugriffsrollen für AMS Security hinzugefügt.	16. Juni 2023

Änderungen	Beschreibung	Datum
Neu: Die CloudTrail Protokoll verwaltung von AMS Accelerat e kann jetzt CloudTrail Kunden-Trails verwenden.	Aktualisierte, von Accelerate unterstützte Optionen für die CloudTrail Protokollverwaltun g, darunter Accelerate Deployed Trail oder Integration mit kundenverwaltetem CloudTrai l Account oder Organization Trail. Weitere Informationen finden Sie unter Überprüfen und aktualisieren Sie Ihre Konfigurationen, damit AMS Accelerate Ihren CloudTrail Trail nutzen kann.	09. Juni 2023
Aktualisiert: Bericht zur Konfiguration der Antwort von AMS Accelerate Config Rules.	Aktualisierte Berichterstattung auf Anfrage für den AWS Config Rules Response Configura tion Report. Weitere Informationen finden Sie unter Schnellere Aktualisierungen der Berichterstattung auf Anfrage. Siehe Bericht zur Konfiguration der Antwort von AMS Config Rules.	26. Mai 2023
Aktualisiert: Richtlinie zum Startdatum der Serviceab rechnung.	Aktualisierte Definitionen des Startdatums der Abrechnung inDie wichtigsten Begriffe von AMS.	15. Mai 2023
Aktualisiert: AWS verwaltete Richtlinien.	Das wurde AWSManaged ServicesDeployment ToolkitPolicy mit neuen CFN- und ECR-Berec htigungen aktualisiert und bestehende Aktionen mit Platzhaltern eingeschränkt. Weitere Informationen finden Sie unter Beschleunigen von Aktualisierungen für serviceverknüpfte Rollen. Siehe Beschleunigen Sie die Aktualisi erung von serviceverknüpften Rollen.	09. Mai 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Zugriff auf Links zu Rollenrichtlinien.	Die Zugriffsrollen können jetzt direkt von den Accelerate S3-Bucket-Speicherorten heruntergeladen werden. Siehe Warum und wann AMS auf Ihr Konto zugreift und AWS Identity and Access Management in AMS Accelerate.	
Aktualisiert: Monatlicher Self-Service-Bericht zur Abrechnung.	Hinweis hinzugefügt: Die monatlichen Abrechnungsberichte sind nur in einem Management Payer-Konto (AMS Advanced-Landezone für mehrere Konten) verfügbar, aber sie sind für alle verknüpften AMS Accelerate-verwalteten Konten verfügbar. Siehe Abrechnungsbericht (monatlich).	13. April 2023
Aktualisiert: Liste der Benachrichtigungen.	CloudTrail Verweise wurden entfernt. Siehe Protokollverwaltung in AMS Accelerate.	13. April 2023
Aktualisiert: Liste der Benachrichtigungen.	Drei neue SSM-Agent-Benachrichtigungen wurden hinzugefügt. Siehe Warnmeldungen aus der Basisüberwachung in AMS.	13. April 2023
Aktualisiert: Voraussetzungen für Accelerate.	Es wurde klargestellt, dass für Accelerate einer von vier AWS-Support-Plänen vorhanden sein muss und dass der Developer-Plan ausgeschlossen ist. Siehe Beschleunigen Sie die Onboarding-Voraussetzungen.	13. April 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Richtlinie für Rollen im Zusammenhang mit dem Service von Accelerate.	Die ZIP-Datei für die Richtlinie „Contacts Service“ wurde aktualisiert. Siehe AWS verwaltete Richtlinien für AMS Accelerate.	13. April 2023
Aktualisiert: AMS Resource Scheduler.	Falscher Rollenname, AWSManagedServices-DescribeScheduleOrPeriod, korrigiert auf AWSManagedServices-DescribeScheduleOrPeriods. Siehe Kostenoptimierung mit AMS Resource Scheduler.	13. April 2023
Aktualisiert: AWS verwaltete Richtlinien.	Aktualisiert Maßgeschneiderte Antworten auf Ergebnisse mit Anweisungen zum Aktualisieren benutzerdefinierter Antworten in einzelnen oder mehreren Konten.	13. April 2023
Aktualisiert: Resource Tagger	Es wurden Warnungen zur „Angabe des Namens für Ihre neue Konfiguration (SampleConfigurationBlock im bereitgestellten Beispiel) hinzugefügt, da Sie versehentlich die von AMS verwaltete Konfiguration mit demselben Namen überschreiben könnten“. Siehe Resource Tagger-Anwendungsfälle in AMS Accelerate.	16. März 2023
Aktualisiert: Patch RACI	Verschiedene Aktualisierungen und Klarstellungen für das RACI zum Patchen. Siehe Service description (Service-Beschreibung).	16. März 2023
Aktualisiert: Aktionen im Deployment Toolkit SLR JSON	Richtlinien und Aktionen wurden aktualisiert. Siehe: Verwenden von serviceverknüpften Rollen für AMS Accelerate.	16. März 2023
Aktualisiert: Automatische Problembehebung	Die LVM-Unterstützung für EC2 Volumenautomatisierung wurde entfernt. Siehe: Automatische AMS-Behebung von Warnmeldungen.	16. März 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Beschleunigen Sie das Onboarding.	Die Verwendung von Rollen, insbesondere der Minimalrolle, wurde klargestellt. Die Vorlage zum Erstellen von AMS-Rollen	16. März 2023
Aktualisiert: Self-Service-Berichterstattung.	Tägliche Backup-Berichte unterstützen jetzt primäre und sekundäre Regionen. Beide werden im Feld Ressourcenregion von gemeldetBackup-Bericht (täglich).	16. März 2023
Aktualisiert: Anleitung zum Patchen	Es wurde eine Warnung hinzugefügt, dass die standardmäßigen Patch-Baselines, die von AMS verwaltet werden, nicht angepasst werden sollten. Erstellen Sie stattdessen eine neue benutzerdefinierte Patch-Baseline. Siehe: Standard-Patch-Baseline und. Benutzerdefinierte Patch-Baseline mit AMS Accelerate	16. März 2023
Aktualisierte Richtlinie zur Kündigung von Diensten.	Aktualisierte Definitionen der Dienstbeendigung und des Kündigungsdatums des Dienstes inDie wichtigsten Begriffe von AMS. Kündigungsmitteilungen müssen bis zum 20. Tag des Monats vor Ihrem letzten vollen Monat ausgestellt werden.	16. März 2023
Aktualisiert: AWS verwaltete Richtlinien.	Der Name der Richtlinie wurde geklärt:Serviceverknüpfte Kontakte-Rolle für AMS Accelerate.	16. Februar 2023
Neu: AWS verwaltete Richtlinien.	Richtlinie hinzugefügt:Serviceverknüpfte Kontakte-Rolle für AMS Accelerate.	16. Februar 2023
Aktualisiert: Einhaltung der Konfiguration.	Ein falsch geschriebenes Wort wurde behoben in:. Konformität mit der Konfiguration in Accelerate	16. Februar 2023

Änderungen	Beschreibung	Datum
Neuer Inhalt: Nicht unterstützt OSes	Weitere Informationen darüber, welche Dienste AMS für nicht unterstützte Betriebssysteme anbietet (OSes), wurden hinzugefügt, siehe. Funktionen für nicht unterstützte Betriebssysteme in Accelerate	16. Februar 2023
Aktualisiert: Patchfenster erstellen	Es wurde ein Link zur Verwendung von CloudShell hinzugefügtErstellen Sie ein Wartungsfenster mit der Systems Manager Manager-Befehlszeilenschnittstelle (CLI) für AMS Accelerate.	16. Februar 2023
Aktualisierter Inhalt: Ressourcen für das Onboarding-Management	Die komprimierten JSON-Vorlagen wurden aktualisiert. Die Vorlage zum Erstellen von AMS-Rollen	16. Februar 2023
Neuer Inhalt: Einhaltung der Konfiguration	Ein neues Thema wurde hinzugefügt:Maßgeschneiderte Antworten auf Ergebnisse.	16. Februar 2023
Neu: AWS verwaltete Richtlinien.	Richtlinie hinzugefügt:Rolle im Zusammenhang mit dem Amazon EventBridge Rule Service für AMS Accelerate.	07. Februar 2023
Aktualisiert: AWS verwaltete Richtlinien.	Das wurde `AWSManagedServices DeploymentToolkitPolicy` mit neuen S3-Berechtigungen aktualisiert. Siehe Beschleunigen Sie die Aktualisierung von serviceverknüpften Rollen.	30. Januar 2023
Neue Opt-in-Region: CPT.	AMS Accelerate ist jetzt in der Opt-in-Region Capetown (CPT) verfügbar. Informationen zur Anmeldung finden Sie unter Verwalten. AWS-Regionen	12. Januar 2023

Änderungen	Beschreibung	Datum
Aktualisiert: Servicebe schreibung.	FSx Dienste, die durch CloudWatch Alarme überwacht werden, wurden hinzugefügtService description (Service-Beschreibung).	12. Januar 2023
Aktualisiert: Überwachung von Standardmetriken.	Es wurden 6 FSx Alarme hinzugefü gtWarnmeldungen aus der Basisüberwachung in AMS.	12. Januar 2023
Aktualisiert: AMS-Muster.	Cloudwatch-Alarmbenachrichtigungen anpassen zu AMS-Muster hinzugefügt.	12. Januar 2023
Aktualisiert: Ressourcen für das Onboarding-Management.	Die Vorlagentabelle wurde aktualisiert und eine Zeile für `ams-onboarding-ssm-execution-role` in Die Vorlage zum Erstellen von AMS-Rollen hinzugefügt.	12. Januar 2023
Aktualisiert: Einhaltung der Konfiguration.	Zusätzliche Informationen zur Anforderung benutzerdefinierter Problembehebungen (im Feld „Wichtig“) finden Sie unterKonformität mit der Konfiguration in Accelerate.	12. Januar 2023
Aktualisiert: Service-linked-rol e Berechtigungen.	Ältere oder duplizierte Berechtigungen wurden entfernt. Siehe Verwenden von serviceve rknüpften Rollen für AMS Accelerate.	15. Dezember 2022
Aktualisiert: Patch-Man agement, Wartungsfenster.	Den Konsolenanweisungen, Schritt 5, wurde eine Anleitung zum Erstellen eines Wartungsf ensters hinzugefügt. Siehe Erstellen Sie von der Systems Manager Manager-Konsole aus ein Wartungsfenster für AMS Accelerate.	15. Dezember 2022
Neu: Bereich Patch-Man agement.	Es wurde ein Abschnitt für die Wartungsfenster von Patch Tuesday hinzugefügt. Siehe Ein wiederkehrendes „Patch Tuesday“ -Wartungs fenster von der AMS-Konsole aus erstellen (empfohlen).	15. Dezember 2022

Änderungen	Beschreibung	Datum
Aktualisiert: AMS Resource Scheduler.	Der CloudFormation Stack-Name wurde aktualisiert. Siehe Ressourcen mit AMS Resource Scheduler verwenden.	15. Dezember 2022
Aktualisiert: Kennzeichnen Sie Ihre Ressourcen für Backups.	Es wurde eine Anleitung zur Verwendung von AMS Resource Tagger hinzugefügt. Siehe Kennzeichnen Sie Ihre Ressourcen, um AMS-Backup-Pläne anzuwenden.	15. Dezember 2022
Aktualisiert: Wählen Sie einen Backup-Plan aus.	Es wurde angegeben, welche Pläne ein kontinuierliches Backup bieten. Siehe Wählen Sie einen AMS-Backup-Plan.	15. Dezember 2022
Aktualisiert: AMS Resource Scheduler.	Das AWS CLI-Beispiel zum Löschen eines Zeitraums oder Zeitplans wurde aktualisiert. Siehe Arbeiten mit Zeiträumen und Zeitplänen in AWS Managed Services Resource Scheduler.	15. Dezember 2022
Aktualisiert: AWS verwaltete Richtlinien.	Das wurde hinzugefügt`AWSManagedServicesDeploymentToolkitPolicy` . Siehe AWS verwaltete Richtlinien für AMS Accelerate.	15. Dezember 2022
Neu: Abschnitt hinzugefügt, der die neue serviceverknüpfte AMS-Rolle beschreibt, AWSServiceRoleForManagedServices_DetectiveControlsConfig.	GovCloud Regionen und Berechtigungen hinzugefügt. Siehe Detective kontrolliert die dienstbezogene Rolle für AMS Accelerate.	15. Dezember 2022

Änderungen	Beschreibung	Datum
Neu: AWS-verwaltete Richtlinie	Es wurde ein Abschnitt hinzugefügt, in dem beschrieben wird, wie die AWS-verwaltete Richtlinie, AWSManagedServices_AlarmManagerPermissionsBoundary, in der Richtlinie für serviceverknüpfte Rollen, AWSManagedServices_AlarmManager _, verwendet wirdServiceRolePolicy, um die Berechtigungen von IAM-Rollen einzuschränken, die von der serviceverknüpften Rolle erstellt wurden. AWSServiceRoleForManagedServices_AlarmManager Siehe AWS verwaltete Richtlinien für AMS Accelerate.	15. Dezember 2022
Aktualisiert: Betrieb auf Abruf.	Zusätzliche Angebote: SQL Server on EC2 Operations und AMI Building and Vending. Siehe Betrieb auf Abruf.	10. November 2022
Aktualisiert: Überwachung und Eventmanagement.	Aktualisierte Erläuterung der Servicemeldungen und Vorfallberichte. Siehe So funktioniert die Überwachung.	10. November 2022
Aktualisiert: Mit Diensten verknüpfte Rollenregionen	GovCloud Regionen und Berechtigungen hinzugefügt. Siehe Verwenden von serviceverknüpften Rollen für AMS Accelerate.	10. November 2022
Neu: Dienstbezogene Rolle.	Neue Rolle hinzugefügt:`AWSServiceRoleForAMSDetectiveControls` . Siehe Detective kontrolliert die dienstbezogene Rolle für AMS Accelerate.	10. November 2022
Aktualisiert: Zugriffsverwaltung .	Die Unterabschnitte wurden mit verbesserten Anweisungen aktualisiert. Siehe Zugriffsverwaltung in AMS Accelerate.	10. November 2022

Änderungen	Beschreibung	Datum
Aktualisiert: Servicebeschreibung.	AMS-Muster in der RACI-Matrix wurden aktualisiert. Siehe Service description (Service-Beschreibung).	10. November 2022
Aktualisiert: AMS-Muster.	Kunden sind für die Bereitstellung von Mustern verantwortlich. Siehe AMS-Muster.	10. November 2022
Aktualisiert: Offboarding.	Es wurden Details darüber hinzugefügt, was mit bestimmten Backup- und Monitoring-Ressourcen beim Offboarding passiert. Siehe Offboard von AMS Accelerate.	10. November 2022
Aktualisiert: Patch-Management..	Aktualisierte und verkürzte Leitlinien zu IAM-Richtlinien. Siehe Erstellen einer IAM-Rolle für On-Demand-Patching von AMS Accelerate.	10. November 2022
Neu: Links zu Architekturdiagrammen.	Links zu AMS-Referenzarchitekturdiagrammen zu verschiedenen Themen hinzugefügt. Ein Beispiel finden Sie unter Überwachung und Eventmanagement in AMS Accelerate.	10. November 2022
Neu: Angebot „Operations on Demand“	„Landing Zone Accelerator Operations“ hinzugefügt. Siehe Betrieb auf Abruf.	13. Oktober 2022
Update: Überwachungsmanagement. Benachrichtigungen generieren Vorfallberichte, keine Serviceanfragen	So funktioniert die Überwachung.	13. Oktober 2022
Neu: Erstellung eines Patch-Wartungsfensters mit einer benutzerdefinierten CFN-Vorlage für Accelerate	CloudFormation Vorlagen für die Konfiguration von Patchfenstern. Siehe Erstellen Sie ein Patch-Wartungsfenster in AMS.	15. September 2022

Änderungen	Beschreibung	Datum
Aktualisiert: Offboarding	Es wurde betont, dass Backup-Pläne in Accelerate nach dem Offboarding nicht mehr funktionieren. Siehe Offboard von AMS Accelerate.	15. September 2022
Aktualisiert: Details zur CloudWatch Konfigura tionsänderung	Ein Fehler in den Windows- und Linux-Bei spielen wurde behoben. Siehe CloudWatch Details zur Konfigurationsänderung.	15. September 2022
Aktualisiert: Verwendung von AMS Resource Scheduler	Es wurden Hinweise zu Cost Allocation Tags hinzugefügt. Siehe Kostenschätzer im AMS Resource Scheduler.	15. September 2022
Aktualisiert: AMS Config Rule Library	Der Regeltabelle wurden zwei `ams-eks-` Konfigurationsregeln hinzugefügt. Siehe Bibliothek mit AMS-Konfigurationsregeln.	15. September 2022
Aktualisiert: Backup-Ma nagement	Die irreführende Bezeichnung PITR (point-in-time-recovery) wurde aus den Titeln und Beschreibungen von Backup-Plänen entfernt. Siehe Wählen Sie einen AMS-Backup-Plan.	15. September 2022
Aktualisiert: Accelerate-Servicebeschreibung	Die Beschreibungen der Konfigurationsrege ln und der Kanarien wurden aktualisiert. Siehe Service description (Service-Beschreibung).	15. September 2022
Aktualisiert: Servicebe schreibung, unterstützte Konfigurationen	end-of-serviceDatum für Windows 2008 R2 entfernt. Accelerate unterstützt Windows 2008 nicht. Siehe Unterstützte Konfigurationen.	11. August 2022
Aktualisiert: Servicebe schreibung, Rollen und Zuständigkeiten	Die RACI-Tabelle wurde aktualisiert. Die ELB-Zugriffsprotokolle wurden aus der letzten Zeile des Abschnitts Netzwerk entfernt. Wir aktiviere n keine ELB-Zugriffsprotokolle für Accelerate-Kunden. Siehe Rollen und Zuständigkeiten.	11. August 2022

Änderungen	Beschreibung	Datum
Aktualisiert: Einhaltung der Konfiguration	Ein Tippfehler in der Spalte „Regeltabelle“ in der Spalte „Frameworks“ wurde korrigiert. NIST-CSF wurde fälschlicherweise als NIST-CIS aufgeführt. Siehe Konformität mit der Konfiguration in Accelerate.	11. August 2022
Neu: Beschleunigen Sie das Offboarding	Überlegungen und Verfahren für das Offboardi ng. Siehe Offboarding AMS Accelerate.	11. August 2022
Aktualisiert: Liste der Betriebssysteme der vorinstal lierten SSM-Agenten	„Ubuntu Linux 18.04 und 20.04" zur Liste hinzugefügt. Siehe EC2 Instances zur Beschleunigung einbinden.	11. August 2022
Neu: Resource Scheduler	Verwenden Sie AMS Resource Scheduler zur Kostenoptimierung, indem Sie Ressource n nur bei Bedarf stoppen und starten. Siehe Kostenoptimierung mit AMS Resource Scheduler.	14. Juli 2022
Aktualisiert: Servicebe schreibung für Resource Scheduler	Verschiedene Abschnitte der Servicebe schreibung wurden für das neue Resource Scheduler-Angebot aktualisiert. Siehe Service description (Service-Beschreibung).	14. Juli 2022
Neu: AMS-Muster	AMS bietet Mustervorlagen, eine generalisierte Lösung, die für eine Reihe von Anwendung sfällen in der von AMS verwalteten Umgebung geeignet ist. Erstes angebotenes Muster:. AMS-Muster	14. Juli 2022
Neu: Hinweis zur Kostenopt imierung	Es wurde ein Hinweis hinzugefügt, in dem erklärt wird, wie die Kosten mit der Ressource nnutzung steigen können. Siehe Ressource ninventar für Accelerate.	14. Juli 2022

Änderungen	Beschreibung	Datum
Aktualisiert: AMS Config Rules	Die Tabellen in der wurden neu organisiert. Bibliothek mit AMS-Konfigurationsregeln Die HTML-Tabelle hat weniger Spalten, damit sie auf einen Blick leichter lesbar ist. Die herunterl adbare Tabelle enthält zusätzliche Spalten, um das Sortieren und Filtern zu ermöglichen.	14. Juli 2022
Aktualisiert: Zugriffsverwaltung	Die CloudFormation Beispielvorlage wurde in aktualisiertBerechtigungen zur Nutzung von AMS-Funktionen. Die `AMSAccele rateAdminAccess` Richtlinie umfasst jetzt die `IAMReadOnlyPolicy` Richtlini en `AmsResourceSchedulerPassRol ePolicy` und.	14. Juli 2022
Aktualisiert: Self-Service-Beric hterstattung	Es wurden Anweisungen zum Verschlüsseln von AWS Glue Metadaten mit KMS-Schlüsseln hinzugefügt. Siehe Feld mit der Bezeichnung Wichtig am. Self-Service-Berichte	14. Juli 2022
Aktualisiert: AMS-Basis überwachung	DeleteRecoveryPoint Backup-Warnung hinzugefügt. Warnmeldungen aus der Basisüberwachung in AMS	14. Juli 2022
Aktualisiert: Unterstützte Betriebssysteme	Datum für das Ende des Support für Amazon Linux 2 hinzugefügt. Service description (Service-Beschreibung)	14. Juli 2022
Aktualisiert: AMS Reporting	Hinweis zu Opt-in-Regionen hinzugefügt. Berichte und Optionen	14. Juli 2022

Änderungen	Beschreibung	Datum
Ressourcenplaner	Es wurden Informationen zum Onboarding und zur Verwendung von AMS Resource Scheduler hinzugefügt, um die Kostenoptimierung durch die Planung von Stopp- und Startzeiten von Ressourcen zu unterstützen. Außerdem wurde die Leistungsbeschreibung von Accelerate aktualisiert und nun auch Resource Scheduler erwähnt. Darüber hinaus wurde das Datum für das Ende des Supports für Amazon Linux 2 auf 2024 aktualisiert. Siehe Kostenoptimierung mit AMS Resource Scheduler und Service description (Service-Beschreibung)	30. Juni 2022
Neuer Alarm	Ein AWS Backup Alarm wurde hinzugefügt. Warnmeldungen aus der Basisüberwachung in AMS	21. Juni 2022
Neuer Inhalt	Der Inhalt der dienstverknüpften Rolle wurde hinzugefügt. Verwenden von serviceverknüpften Rollen für AMS Accelerate	16. Juni 2022
	AWS Network Firewall Operations wurde dem Angebotskatalog Operations on Demand (OOD) hinzugefügt. Betrieb auf Abruf	16. Juni 2022
	Beschreibung der Problemverwaltungsfunktion hinzugefügt. Service description (Service-Beschreibung)	16. Juni 2022
	Es wurde ein Hinweis zu den Konfigurationsregeln hinzugefügt, die bestimmte Opt-in-Regionen nicht unterstützen. Konformität mit der Konfiguration in Accelerate	16. Juni 2022

Änderungen	Beschreibung	Datum
Aktualisierter Inhalt	Konformität mit der Konfiguration. „AMS Config Rule library“ -> „Table of Rules“, wurde aktualisiert und nur als ZIP-Datei entfernt. Konformität mit der Konfiguration in Accelerate	16. Juni 2022
	Eskalations-E-Mails wurden entfernt. Eskalationspfad	16. Juni 2022
	Die Themenliste wurde unter die ersten Absätze verschoben. Was ist AMS Accelerate?	16. Juni 2022
	Der Inhalt der auto Remedition wurde aktualisiert. Automatische AMS-Behebung von Warnmeldungen	16. Juni 2022
Aktualisierter Inhalt: Servicebeschreibung	EKS wurde der Liste der von AMS Config Rules überwachten Dienste in hinzugefügtUnterstützte Services. Die Beschreibung der Überwachung in der RACI-Tabelle unter wurde aktualisiert. Rollen und Zuständigkeiten	12. Mai 2022
Aktualisierter Inhalt: Einhaltung der Konfiguration	EKS-bezogene Konfigurationsregeln hinzugefügt. Siehe Konformität mit der Konfiguration in Accelerate.	12. Mai 2022
Aktualisierter Inhalt: Erste Schritte, Kontoermittlung	Eine neuere Version des AwsAccountDiscoveryCli Skripts (in der Account Discovery Changelog-ZIP-Datei) wurde hinzugefügt. Schritt 1. Kontoermittlung in Accelerate	12. Mai 2022
Aktualisierter Inhalt: Überwachung, Standardmetriken	Die Auslösebedingungen für ALB-bezogene Metriken wurden aktualisiert. Siehe Warnmeldungen aus der Basisüberwachung in AMS.	12. Mai 2022

Änderungen	Beschreibung	Datum
Aktualisierter Inhalt: Onboarding patchen	Es wurde eine ausdrückliche Voraussetzung für das Patchen hinzugefügt: Sie müssen sich für EBS anmelden. Siehe Onboarding-Patching in Accelerate.	12. Mai 2022
Aktualisierter Inhalt: Schnellere Ressourceninventartabelle	Die Regeln für ams-detective-controls-config -rules-cdk wurden geändert, Regeln für ams-detective-controls-recorder -cdk und -cdk hinzugefügt. ams-detective-controls-infrastructure Siehe Ressourceninventar für Accelerate.	14. April 2022
Aktualisierter Inhalt: Einhaltung der Konfiguration	Einführung in Industriestandards, Konfigurationsregeln und Antworttypen. Betont, dass Kunden keine individuellen Konfigurationsregeln oder Antworten wählen. Konformität mit der Konfiguration in Accelerate.	14. April 2022
Aktualisierter Inhalt: Servicebeschreibung	Der bestehende Abschnitt „Umfang der Änderungen“ wurde unter Rollen und Zuständigkeiten verschoben. Siehe Rollen und Zuständigkeiten.	14. April 2022
Aktualisierter Inhalt: Tagging und Überwachung	Zu `AWS::Synthetics:Canary` den Listen der erlaubten Ressourcentypen für Tagging und Überwachung hinzugefügt. Siehe Resource Tagger-Konfigurationsprofile in AMS Accelerate und Beschleunigtes Konfigurationsprofil: Substitution von Pseudoparametern.	14. April 2022
Aktualisierter Inhalt: Voraussetzungen für Accelerate	Für SSM erforderliche Bucket-Berechtigungen wurden hinzugefügt. Amazon EC2 Systems Manager in Accelerate	14. April 2022

Änderungen	Beschreibung	Datum
Neuer Inhalt: Patchen und Überwachen	Beispielcode zur Verwendung von Cloudformation zur Bereitstellung von Tagging- und Überwachungskonfigurationen hinzugefügt. Siehe Bereitstellen eines Konfigurationsprofils mit CloudFormation for Accelerate und Verwenden CloudFormation zur Bereitstellung von Accelerate-Konfigurationsänderungen.	10. März 2022
Aktualisierter Inhalt: Patch-Wartungskonsole	Die Schritte wurden neu angeordnetErstellen Sie von der Systems Manager Manager-Konsole aus ein Wartungsfenster für AMS Accelerate, damit sie der Konsolenoberfläche entsprechen.	10. März 2022
Aktualisierter Inhalt: Patch Maintenance CLI	Aktualisierte CLI-Parameter (Zeitplan, Dauer und Cutoff) für Erstellen Sie ein Wartungsfenster mit der Systems Manager Manager-Befehlszeilenschnittstelle (CLI) für AMS Accelerate	10. März 2022
Neuer Inhalt: Auto Instance Config	Die Definition von `AMSInstanceProfile BasePolicy` to wurde hinzugefügt Details zur Änderung von IAM-Berechtigungen	10. März 2022
Neuer Inhalt: Onboarding	Ein Linux-Beispielbefehl wurde hinzugefügt Ausgehende Internetkonnektivität in Accelerate	10. März 2022
Neuer Inhalt: Onboarding	Eine Option mit den geringsten Rechten wurde hinzugefügt. Die Vorlage zum Erstellen von AMS-Rollen	10. März 2022
Aktualisierter Inhalt: Anweisungen zur beschleunigten Eskalation	Es wurden Anleitungen, Links und E-Mail-Kontakte hinzugefügt zu Eskalationspfad	10. März 2022

Änderungen	Beschreibung	Datum
Aktualisierter Inhalt: Unterstützte Konfigurationen	AMS geht davon aus, den Support für RHEL 6 und CentOs am 14. März 2023 einzustellen. Siehe Unterstützte Konfigurationen	10. März 2022
Aktualisierter Inhalt: Tabelle mit Ressourcen	Der Ressourcentabelle wurden AMS-Zugriffs-IAM-Rollen hinzugefügt Ressourceninventar für Accelerate	10. März 2022
Aktualisierter Inhalt: Onboarding und Backup	Es wurden Anweisungen hinzugefügt, um sich für und zu AWS Backup entscheid en Einführung AWS Backup in Accelerate Kontinuitätsmanagement in AMS Accelerate	10. März 2022
Aktualisierter Inhalt: Access Management	Spezifische Anweisungen für Fortgeschrittene wurden aus der Accelerate-Anleitung entfernt. Wie und wann benutzt man das Root-Benu tzerkonto in AMS	10. März 2022
Aktualisierter Inhalt: Unterstützte Konfigurationen	AMS unterstützt jetzt Oracle Linux 8.3 und Ubuntu 18.04 und 20.04. Siehe Unterstützte Konfigurationen.	28. Februar 2022
Aktualisierter Inhalt: Service Level Agreement	Das herunterladbare Service Level Agreement wurde in aktualisiertUnterstützte Services.	28. Februar 2022
Aktualisierter Inhalt: Access Management	Es wurde So greift AMS auf Ihr Konto zu mit FAQs den Rollen für AMS-Bedienkonsolen aktualisiert und es wurde eine Warnung angezeigt, diese nicht zu ändern oder zu löschen.	28. Februar 2022
Aktualisierter Inhalt: Alarm Manager	Aktualisiert Accelerate Configuration-Profil: Überwachung. Alarm Manager ist nicht mehr auf Alarme mit nur einer Metrik beschränkt.	28. Februar 2022

Änderungen	Beschreibung	Datum
Aktualisierter Inhalt: Erste Schritte	Aktualisiert Schritt 2. Einführung von Verwaltungsressourcen in Accelerate. Es wurde eine IAM-Rolle mit minimalem Zugriff auf Onboarding-Ressourcen hinzugefügt.	28. Februar 2022
Neuer Inhalt: Umfang der Änderungen in der Servicebeschreibung	Es wurde ein neuer Abschnitt hinzugefügtUmfang der von AMS Accelerate vorgenommenen Änderungen, in dem Grenzen und Aktionen hervorgehoben werden, die AMS Accelerate nicht durchführt.	10. Februar 2022
Aktualisierter Inhalt: Erste Schritte	Der neue Onboarding-Prozess beginnt mit der Einrichtung von Standardfunktionen und -konfigurationen vor der Anpassung. Unterabschnitte enthalten funktionsspezifische Ziele und verwandte Links. Siehe Erste Schritte mit AMS Accelerate.	10. Februar 2022
Aktualisierter Inhalt: AMS Backup Management.	Das Kontinuitätsmanagement in AMS Accelerate Kapitel wurde aus Gründen der besseren Lesbarkeit gekürzt und neu organisiert.	10. Februar 2022
Aktualisierter Inhalt: Tagging	Es wurde ein Abschnitt mit Tagging-Tools hinzugefügt, der Codebeispiele für CloudFormation und andere Tools enthält. Siehe Taggen in AMS Accelerate.	10. Februar 2022
Aktualisierter Inhalt: Baseline Monitoring	Die verbesserte Auslösebedingung für RedShift Cluster-Alarme reduziert Fehlalarme bei Wartungsarbeiten. Siehe Warnmeldungen aus der Basisüberwachung in AMS.	10. Februar 2022

Änderungen	Beschreibung	Datum
Aktualisierter Inhalt: Patchen	Der CLI-Beispielbefehl wurde aktualisiert, um ein Wartungsfenster zu registrieren. Siehe Erstellen Sie ein Wartungsfenster mit der Systems Manager Manager-Befehlszeilenschnittstelle (CLI) für AMS Accelerate.	10. Februar 2022
Aktualisierter Inhalt: Inventar der AWS Konfigurationsregeln.	Die veraltete Konfigurationsregel wurde `ams-nist-cis-ec2-security-group-attached-to-eni` aus der Tabelle „ AWS Config Rules Inventory“ entfernt. Siehe Tabelle der Regeln.	27. Januar 2022
Neuer Inhalt: Patch-Wartungsfenster erstellen.	Es wurde ein Link zum SSM-Tutorial und zu Beispielbefehlen zum Erstellen von Patch-Wartungsfenstern über die Befehlszeile hinzugefügt. Siehe Erstellen Sie ein Wartungsfenster mit der Systems Manager Manager-Befehlszeilenschnittstelle (CLI) für AMS Accelerate.	27. Januar 2022
Neuer Inhalt: Resource Tagger erkennt den neuen Ressourcentyp Auto Scaling Groups (ASG).	Auto Scaling Scaling-Gruppen wurden zu den Ressourcentypen hinzugefügt, die mit Resource Tagger-Konfigurationsprofilen gefiltert werden können. Siehe Syntax und Struktur.	13. Januar 2022
Neuer Inhalt: Zusätzliche Backup-Pläne und Tresore.	Es wurden neue Backup-Pläne und Tresore hinzugefügt, um Szenarien mit hohem Risiko, einschließlich Ransomware-Angriffen, zu minimieren. Siehe Backups in AMS-Tresoren anzeigen und Backups in AMS-Tresoren anzeigen.	13. Januar 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.