AWS Well-Architected Framework

Säule „Betriebliche Exzellenz“

Säule „Betriebliche Exzellenz“: AWS Well-Architected Framework

Table of Contents

Säule „Operative Exzellenz“ – AWS-Well-Architected-Framework

Veröffentlichungsdatum: 27. Juni 2024 (Dokumentversionen)

In diesem Dokument geht es speziell um die Säule der operativen Exzellenz des AWS-Well-Architected-Framework. Es enthält bewährte Methoden für die Konzeption, Übermittlung und Wartung von AWS-Workloads.

Einführung

Das AWS Well-Architected Framework unterstützt Sie dabei, die Vor- und Nachteile der Entscheidungen nachzuvollziehen, die Sie beim Aufbau von Workloads in AWS treffen. Das Framework hilft Ihnen, bewährte Betriebs- und Architekturmethoden für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Workloads in der Cloud zu ermitteln. Es bietet eine Möglichkeit, Ihre Betriebsabläufe und Architekturen konsistent auf die Einhaltung bewährter Methoden zu prüfen und Verbesserungspotenzial zu identifizieren. Wir sind der Meinung, dass eine gute auf den Betrieb ausgerichtete Workload-Architektur die Wahrscheinlichkeit für den geschäftlichen Erfolg deutlich erhöht.

Das Framework basiert auf den folgenden sechs Säulen:

- Operative Exzellenz
- Sicherheit
- Zuverlässigkeit
- Leistungseffizienz
- Kostenoptimierung
- Nachhaltigkeit

In diesem Dokument geht es speziell um die Säule der operativen Exzellenz und darum, wie Sie diese als Grundlage für architektonisch gute Lösungen anwenden. Operative Exzellenz ist eine Herausforderung in Umgebungen, in denen das operative Geschäft als eine isolierte und von den unterstützten Geschäftsbereichen und Entwicklungsteams getrennte Funktion wahrgenommen wird. Mithilfe der in diesem Dokument aufgeführten Methoden können Sie Architekturen aufbauen, die

Statuseinblicke geben, für einen effektiven und effizienten Betrieb ausgelegt sind, auf Ereignisse reagieren können und Ihre geschäftlichen Ziele unterstützen.

Dieses Dokument richtet sich an Nutzer in technologischen Rollen, z. B. CTOs (Chief Technology Officers), Architekten, Entwickler und Mitglieder von Operations-Teams. Sie erfahren darin mehr über die bewährten Methoden und Strategien von AWS für die Entwicklung sicherer Cloud-Architekturen für operative Exzellenz. Implementierungsdetails oder Architekturmodelle enthält dieses Dokument nicht. Allerdings beinhaltet es Verweise auf die entsprechenden Ressourcen, in denen Sie solche Informationen finden.

Operational Excellence

Bei Amazon definieren wir betriebliche Exzellenz als Verpflichtung, Software korrekt zu entwickeln und dabei einheitlich ein hervorragendes Kundenerlebnis zu bieten. Sie umfasst bewährte Methoden für die Organisation Ihres Teams, die Gestaltung Ihres Workloads, den Betrieb in großem Maßstab und die Weiterentwicklung im Laufe der Zeit. Betriebliche Exzellenz ermöglicht es Ihrem Team, mehr Zeit für die Entwicklung neuer Funktionen, von denen Kunden profitieren, aufzuwenden und weniger Zeit für Wartung und Fehlerbehebung. Für eine korrekte Entwicklung halten wir uns an bewährte Methoden, die zu gut funktionierenden Systemen, einer ausgewogenen Workload für Sie und Ihr Team und vor allem zu einem hervorragenden Kundenerlebnis führen.

Ziel betrieblicher Exzellenz ist es, neue Funktionen und Fehlerkorrekturen schnell und zuverlässig in die Hände der Kunden zu geben. Unternehmen, die in betriebliche Exzellenz investieren, stellen ihre Kunden durchweg bei der Entwicklung neuer Funktionen, Vornahme von Änderungen und beim Umgang mit Ausfällen zufrieden. Auf dem Weg dorthin unterstützt die betriebliche Exzellenz die Continuous Integration und Continuous Delivery (CI/CD) (kontinuierliche Integration und kontinuierliche Bereitstellung), indem sie Entwickler dabei unterstützt, durchgängig qualitativ hochwertige Ergebnisse zu erzielen.

Designprinzipien

Nachfolgend finden Sie die konzeptionellen Grundsätze für betriebliche Exzellenz in der Cloud:

- Organisieren der Teams nach Geschäftsergebnissen: Die Fähigkeit eines Teams, Geschäftsergebnisse zu erzielen, hängt von der Vision der Führung, effektiven Abläufen und einem geschäftsorientierten Betriebsmodell ab. Die Führungskräfte sollten sich voll und ganz für eine CloudOps-Transformation mit einem geeigneten Cloud-Betriebsmodell einsetzen, das die Teams dazu anregt, möglichst effizient zu arbeiten und Geschäftsergebnisse zu erzielen. Ein geeignetes Betriebsmodell nutzt Personal-, Prozess- und Technologiekapazitäten, um zu skalieren, die Produktivität zu optimieren und und durch Agilität, Reaktionsfähigkeit und Anpassung einen Wettbewerbsvorteil zu erlangen. Die langfristige Vision der Organisation wird in Ziele umgesetzt, die Stakeholdern und Verbrauchern Ihrer Cloud-Services unternehmensweit vermittelt werden. Ziele und operative KPIs sind auf allen Ebenen aufeinander abgestimmt. Diese Vorgehensweise sorgt dafür, dass der langfristige Mehrwert, der sich aus der Umsetzung der folgenden Gestaltungsprinzipien ergibt, dauerhaft gewährleistet ist.
- Implementieren von Beobachtbarkeit für umsetzbare Erkenntnisse: Gewinnen Sie ein umfassendes Verständnis hinsichtlich Workload-Verhalten, -Leistung, -Zuverlässigkeit, -Kosten und -Zustand.

Legen Sie wichtige Key Performance Indicators (KPIs, Leistungskennzahlen) fest und nutzen Sie die Telemetrie zur Beobachtung, um fundierte Entscheidungen zu treffen und sofort einzugreifen, wenn die Geschäftsergebnisse gefährdet sind. Verbessern Sie proaktiv Leistung, Zuverlässigkeit und Kosten auf der Grundlage von verwertbaren Daten zur Beobachtbarkeit.

- Sicher automatisieren wenn möglich: In der Cloud können Sie die gleichen technischen Vorgehensweisen wie beim Anwendungscode in Ihrer gesamten Umgebung anwenden. Sie können Ihren gesamten Workload und seinen Betrieb (Anwendungen, Infrastruktur, Konfiguration und Verfahren) als Code definieren und aktualisieren. Anschließend können Sie den Betrieb Ihrer Workloads automatisieren, indem Sie sie als Reaktion auf Ereignisse initiieren. In der Cloud können Sie Automatisierungssicherheit einsetzen, indem Sie einen Integritätsschutz wie Ratenkontrolle, Fehlerschwellenwerte und Genehmigungen einrichten. Durch eine effektive Automatisierung können Sie konsistente Reaktionen auf Ereignisse durchsetzen, menschliche Fehler begrenzen und den Arbeitsaufwand der Mitarbeiter reduzieren.
- Durchführen häufiger, kleiner, umkehrbarer Änderungen: Entwerfen Sie Workloads, die skalierbar und lose gekoppelt sind, damit die Komponenten regelmäßig aktualisiert werden können. Automatisierte Bereitstellungstechniken in Verbindung mit kleineren, inkrementellen Änderungen verringern den „Blast Radius“ und ermöglichen eine schnellere Umkehrung bei Fehlern. Dadurch erhöht sich das Vertrauen, vorteilhafte Änderungen an Ihrem Workload vornehmen zu können, während die Qualität erhalten bleibt und Sie sich schnell an veränderte Marktbedingungen anpassen können.
- Betriebliche Verfahren regelmäßig nachbessern: Wenn Sie Ihre Workloads weiterentwickeln, müssen Sie auch Ihre Abläufe entsprechend anpassen. Suchen Sie beim Einsatz betrieblicher Verfahren nach Möglichkeiten, diese zu verbessern. Führen Sie regelmäßige Überprüfungen durch und vergewissern Sie sich, dass alle Verfahren effektiv sind und dass die Teams mit ihnen vertraut sind. Wenn Lücken festgestellt werden, aktualisieren Sie die Verfahren entsprechend. Informieren Sie alle Beteiligten und Teams über Aktualisierungen der Verfahren. Gamifizieren Sie Ihren Betrieb zum Weitergeben von bewährten Methoden und zur Schulung von Teams.
- Antizipieren von Ausfällen: Maximieren Sie den betrieblichen Erfolg, indem Sie Fehlerszenarien erstellen, um das Risikoprofil des Workloads und seine Auswirkungen auf Ihre Geschäftsergebnisse zu verstehen. Testen Sie die Wirksamkeit Ihrer Verfahren und die Reaktion Ihres Teams auf diese simulierten Fehler. Treffen Sie fundierte Entscheidungen, um offene Risiken zu auszuräumen, die anhand Ihrer Tests identifiziert wurden.
- Lernen aus allen betrieblichen Ereignissen und Metriken: Steigern Sie die Verbesserung durch die Erkenntnisse, die aus allen betrieblichen Ereignissen und Fehlern gewonnen werden. Geben Sie

Ihre Erkenntnisse an alle Teams in Ihrer gesamten Organisation weiter. Die Erkenntnisse sollten Daten und Anekdoten enthalten, wie die Betriebsabläufe zu den Geschäftsergebnissen beitragen.

- Nutzen verwalteter Services: Verringern Sie den betrieblichen Aufwand, indem Sie verwaltete AWS-Services nutzen, wo immer dies möglich ist. Erstellen Sie operative Verfahren für die Interaktion mit diesen Services.

Definition

Die bewährte Methoden für betriebliche Exzellenz in der Cloud lassen sich in vier Bereiche einteilen:

- Organisation
- Vorbereitung
- Betrieb
- Weiterentwicklung

Die Geschäftsleitung Ihres Unternehmens definiert Geschäftsziele. Anforderungen und Prioritäten müssen in Ihrem Unternehmen bekannt sein, damit Aufgaben entsprechend organisiert und durchgeführt und die Geschäftsergebnisse erreicht werden können. Ihr Workload muss die Informationen ausgeben, die für die Unterstützung dessen erforderlich sind. Die Implementierung von Services zur Integration, Bereitstellung und Lieferung Ihres Workloads schafft einen erhöhten Fluss nützlicher Änderungen in die Produktion, indem wiederkehrende Prozesse automatisiert werden.

Es kann Risiken im Zusammenhang mit dem Betrieb Ihres Workloads geben. Sie müssen diese Risiken verstehen und eine fundierte Entscheidung dazu treffen, ob der Übergang in die Produktion vollzogen werden sollte. Ihre Teams müssen in der Lage sein, den Workload zu unterstützen. Geschäfts- und Betriebsmetriken, die von den gewünschten Geschäftsergebnissen abgeleitet werden, helfen Ihnen, den Zustand Ihres Workloads und Ihrer Betriebsaktivitäten nachzuvollziehen und auf Vorfälle zu reagieren. Ihre Prioritäten ändern sich, wenn sich Ihre geschäftlichen Anforderungen und die geschäftliche Umgebung ändern. Verwenden Sie diese als Feedback-Schleife, um Ihr Unternehmen und den Betrieb Ihres Workloads kontinuierlich zu verbessern.

Organisation

Sie müssen die Prioritäten Ihres Unternehmens, die Unternehmensstruktur und die Unterstützung Ihrer Teammitglieder durch Ihr Unternehmen verstehen, damit sie Ihre Geschäftsergebnisse unterstützen können.

Um operative Exzellenz zu ermöglichen, müssen Sie Folgendes verstehen:

Themen

Unternehmensprioritäten

Um die Prioritäten festlegen zu können, die den geschäftlichen Erfolg ermöglichen, müssen Ihre Teams gemeinsam in Erfahrung bringen, wie sämtliche Workloads aussehen, welche Rolle die einzelnen Teams dabei spielen und was für geschäftliche Ziele damit erreicht werden sollen. Mit gut definierten Prioritäten erzielen Ihre Bemühungen den größtmöglichen Nutzen. Überprüfen Sie Ihre Prioritäten regelmäßig, damit sie aktualisiert werden können, wenn sich die Anforderungen Ihrer Organisation ändern.

Bewährte Methoden

OPS01-BP01 Kundenbedürfnisse bewerten

Binden Sie alle wichtigen Stakeholder ein, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams, um zu bestimmen, welche Bereiche verstärkt auf die Bedürfnisse der externen

Kunden ausgerichtet werden müssen. Dadurch wird sichergestellt, dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um die gewünschten geschäftlichen Ergebnisse zu erzielen.

Gewünschtes Ergebnis:

- Sie arbeiten rückwärts von den Kundenergebnissen aus.
- Sie wissen, wie Ihre betrieblichen Praktiken Geschäftsergebnisse und -ziele unterstützen.
- Sie binden alle relevanten Parteien ein.
- Sie verfügen über Mechanismen, um Kundenbedürfnisse zu erfassen.

Typische Anti-Muster:

- Sie haben sich entschieden, außerhalb der Kerngeschäftszeiten keinen Kundenservice zu bieten, aber Sie haben dazu keine historischen Supportanfragedaten analysiert. Daher wissen Sie nicht, ob diese Entscheidung Auswirkungen auf Ihre Kunden hat.
- Sie entwickeln ein neues Feature, haben aber Ihre Kunden nicht miteinbezogen, um herauszufinden, ob die Funktion erwünscht ist und wie sie genau aussehen sollte. Außerdem haben Sie keine Tests durchgeführt, um die Nachfrage und die Methode der Bereitstellung zu validieren.

Vorteile der Einführung dieser bewährten Methode: Kunden, deren Anforderungen erfüllt sind, bleiben mit höherer Wahrscheinlichkeit als Kunden erhalten. Die Bewertung und das Verständnis externer Kundenbedürfnisse liefert die Grundlage dafür, wie Sie Ihre Anstrengungen zur Bereitstellung eines geschäftlichen Mehrwerts priorisieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Verstehen Sie die geschäftlichen Anforderungen: Der geschäftliche Erfolg basiert auf gemeinsamen Zielen und der Kommunikation zwischen allen Stakeholdern, zu denen auch die Teams aus den Bereichen Geschäft, Entwicklung und Betrieb gehören.

Überprüfen Sie die geschäftlichen Ziele, Anforderungen und Prioritäten externer Kunden: Führen Sie wichtige Stakeholder zusammen, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams, um die Ziele, Anforderungen und Prioritäten externer Kunden zu besprechen. Dadurch wird sichergestellt,

dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um die gewünschten Geschäfts- und Kundenergebnisse zu erzielen.

Schaffen Sie ein gemeinsames Verständnis: Sorgen Sie dafür, dass alle Beteiligten die Geschäftsfunktionen des Workloads und die Rollen der einzelnen Teams bei den Workload-spezifischen betrieblichen Abläufen kennen. Außerdem sollte bekannt sein, wie diese Faktoren Ihre gemeinsamen Geschäftsziele mit internen und externen Kunden beeinflussen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS11-BP03 Implementieren von Feedback-Schleifen

OPS01-BP02 Bedürfnisse interner Kunden bewerten

Binden Sie alle wichtigen Stakeholder ein, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams, um zu bestimmen, welche Bereiche verstärkt auf die Bedürfnisse der internen Kunden ausgerichtet werden müssen. Dadurch wird sichergestellt, dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um geschäftliche Ergebnisse zu erzielen.

Gewünschtes Ergebnis:

- Anhand Ihrer etablierten Prioritäten können Sie erkennen, an welchen Stellen die Verbesserungsbemühungen konzentriert werden sollten (z. B. Teamfähigkeiten entwickeln, die Workload-Leistung verbessern, Kosten senken, Runbooks automatisieren oder die Überwachung ausbauen).
- Wenn sich Anforderungen ändern, aktualisieren Sie Ihre Prioritäten entsprechend.

Typische Anti-Muster:

- Sie haben sich entschieden, die Zuweisung von IP-Adressen für Ihre Produktteams zu ändern, um die Netzwerkverwaltung zu vereinfachen. Dabei haben Sie jedoch nicht mit den Mitarbeitern gesprochen. Sie wissen also nicht, welche Auswirkungen diese Änderung auf Ihre Produktteams haben wird.
- Sie implementieren ein neues Entwicklungstool, haben aber Ihre internen Kunden nicht einbezogen, um herauszufinden, ob das Tool benötigt wird oder mit den Abläufen der Kunden kompatibel ist.

- Sie implementieren ein neues Überwachungssystem, haben aber Ihre internen Kunden nicht kontaktiert, um herauszufinden, ob spezifische Überwachungs- oder Berichtsanforderungen vorliegen, die berücksichtigt werden sollten.

Vorteile der Einführung dieser bewährten Methode: Die Bewertung und das Verständnis interner Kundenbedürfnisse liefert die Grundlage dafür, wie Sie Ihre Anstrengungen zur Bereitstellung eines geschäftlichen Mehrwerts priorisieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

- Verstehen Sie die geschäftlichen Anforderungen: Der geschäftliche Erfolg basiert auf gemeinsamen Zielen und der Kommunikation zwischen allen Stakeholdern, zu denen auch die Teams aus den Bereichen Geschäft, Entwicklung und Betrieb gehören.
- Überprüfen Sie die geschäftlichen Ziele, Anforderungen und Prioritäten interner Kunden: Führen Sie wichtige Stakeholder zusammen, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams, um die Ziele, Anforderungen und Prioritäten interner Kunden zu besprechen. Dadurch wird sichergestellt, dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um die gewünschten Geschäfts- und Kundenergebnisse zu erzielen.
- Schaffen Sie ein gemeinsames Verständnis: Sorgen Sie dafür, dass alle Beteiligten die Geschäftsfunktionen des Workloads und die Rollen der einzelnen Teams bei den Workload-spezifischen betrieblichen Abläufen kennen. Außerdem sollte bekannt sein, wie diese Faktoren die gemeinsamen Geschäftsziele mit internen und externen Kunden beeinflussen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS11-BP03 Implementieren von Feedback-Schleifen

OPS01-BP03 Bewerten der Governance-Anforderungen

Governance bezeichnet die Reihe von Richtlinien, Regeln oder Rahmen, die ein Unternehmen nutzt, um die geschäftlichen Ziele zu erreichen. Die Governance-Anforderungen werden innerhalb Ihrer Organisation erstellt. Sie können sich darauf auswirken, welche Arten von Technologien Sie nutzen oder wie Sie Ihren Workload betreiben. Integrieren Sie die Governance-Anforderungen

Ihrer Organisation in Ihren Workload. Konformität ist die Fähigkeit, nachzuweisen, dass Sie die Governance-Anforderungen implementiert haben.

Gewünschtes Ergebnis:

- Die Governance-Anforderungen werden in das Architekturdesign und den Betrieb Ihres Workloads integriert.
- Sie können nachweisen, dass Sie den Governance-Anforderungen nachkommen.
- Die Governance-Anforderungen werden regelmäßig überprüft und aktualisiert.

Typische Anti-Muster:

- Ihre Organisation verlangt Multi-Faktor-Authentifizierung für das Stammkonto. Sie haben diese Anforderung nicht implementiert und das Stammkonto wurde kompromittiert.
- Während des Entwurfs Ihres Workloads wählen Sie einen Instance-Typ, der nicht von der IT-Abteilung genehmigt wurde. Sie können Ihren Workload nicht starten und müssen ihn überarbeiten.
- Sie sind verpflichtet, über einen Plan für die Notfallwiederherstellung zu verfügen. Sie haben keinen Plan erstellt und Ihr Workload ist von einem längeren Ausfall betroffen.
- Ihr Team möchte neue Instances verwenden, Ihre Governance-Anforderungen wurden jedoch nicht aktualisiert, sodass die Instances nicht zulässig sind.

Vorteile der Nutzung dieser bewährten Methode:

- Durch das Erfüllen der Governance-Anforderungen wird Ihr Workload auf die größeren Organisationsrichtlinien abgestimmt.
- Die Governance-Anforderungen spiegeln Branchenstandards und bewährte Methoden für Ihre Organisation wider.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Ermitteln Sie Governance-Anforderungen, indem Sie mit Stakeholdern und Governance-Organisationen zusammenarbeiten. Integrieren Sie die Governance-Anforderungen in Ihren Workload. Seien Sie in der Lage, nachzuweisen, dass Sie den Governance-Anforderungen nachkommen.

Kundenbeispiel

Das Cloud-Operations-Team bei AnyCompany Retail arbeitet mit Stakeholdern im gesamten Unternehmen zusammen, um Governance-Anforderungen zu entwickeln. Beispielsweise wird SSH-Zugriff auf Amazon EC2-Instances verboten. Wenn Teams Systemzugriff benötigen, müssen Sie AWS Systems Manager Session Manager verwenden. Das Cloud-Operations-Team aktualisiert die Governance-Anforderungen regelmäßig, sobald neue Services verfügbar sind.

Implementierungsschritte

1. Identifizieren Sie die Stakeholder für Ihren Workload, einschließlich zentralisierter Teams.
2. Arbeiten Sie mit den Stakeholdern zusammen, um Governance-Anforderungen zu ermitteln.
3. Nachdem Sie eine Liste erstellt haben, ordnen Sie die Verbesserungspunkte entsprechend der Priorität und beginnen Sie damit, sie in Ihren Workload zu implementieren.
   a. Nutzen Sie Services wie AWS Config, um Governance-as-Code zu erstellen und zu überprüfen, ob die Governance-Anforderungen erfüllt werden.
   b. Wenn Sie AWS Organizations nutzen, können Sie Service-Kontrollrichtlinien verwenden, um die Governance-Anforderungen zu implementieren.
4. Stellen Sie Unterlagen bereit, die die Implementierung bestätigen.

Grad des Aufwands für den Implementierungsplan: mittel. Die Implementierung fehlender Governance-Anforderungen kann dazu führen, dass Sie Ihren Workload überarbeiten müssen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP04 Bewerten der Compliance-Anforderungen – Compliance ist wie Governance, stammt jedoch von außerhalb eines Unternehmens.

Zugehörige Dokumente:

- AWS Management and Governance Cloud Environment Guide (AWS-Leitfaden zur Verwaltung und Governance der Cloud-Umgebung)
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment (Bewährte Methoden für AWS Organizations-Service-Kontrollrichtlinien in einer Umgebung mit mehreren Konten)

- Governance in the AWS Cloud: The Right Balance Between Agility and Safety (Governance in der AWS Cloud: Das richtige Gleichgewicht zwischen Agilität und Sicherheit)
- What is Governance, Risk, And Compliance (GRC)? (Was ist Governance, Risiko und Compliance (GRC)?)

Zugehörige Videos:

- AWS Management and Governance: Configuration, Compliance, and Audit - AWS Online Tech Talks (Verwaltung und Governance in AWS: Konfiguration, Compliance und Audit – AWS Online Tech Talks)
- AWS re:Inforce 2019: Governance for the Cloud Age (DEM12-R1) (AWS re:Inforce 2019: Governance für das Cloud-Zeitalter (DEM12-R1))
- AWS re:Invent 2020: Achieve compliance as code using AWS Config(AWS re:Invent 2020: Mit AWS Config Compliance als Code erzielen)
- AWS re:Invent 2020: Agile governance on AWS GovCloud (US)(AWS re:Invent 2020: Agile Governance in AWS GovCloud (US))

Zugehörige Beispiele:

- AWS Config Conformance Pack Samples (AWS Config-Conformance-Pack-Beispielvorlagen)

Zugehörige Services:

- AWS Config
- AWS Organizations – Service-Kontrollrichtlinien

OPS01-BP04 Bewerten der Compliance-Anforderungen

Regulatorische, branchenspezifische und interne Compliance-Anforderungen sind ein wichtiger Faktor, wenn Sie die Prioritäten Ihrer Organisation definieren. Ihr Compliance-Regelwerk hindert Sie möglicherweise daran, spezifische Technologien oder geografische Standorte zu nutzen. Wenden Sie die erforderliche Sorgfalt an, wenn keine externen Compliance-Regelwerke identifiziert sind. Erstellen Sie Audits oder Berichte, die die Compliance bestätigen.

Wenn Sie damit werben, dass Ihr Produkt bestimmte Compliance-Standards erfüllt, benötigen Sie einen internen Prozess zur kontinuierlichen Gewährleistung der Compliance. Beispiele für

Compliance-Standards sind PCI DSS, FedRamp und HIPAA. Die geltenden Compliance-Standards werden durch verschiedene Faktoren bestimmt, beispielsweise dadurch, welche Datentypen von der Lösung gespeichert oder gesendet werden und welche geografischen Regionen die Lösung unterstützt.

Gewünschtes Ergebnis:

- Die regulatorischen, branchenspezifischen und internen Compliance-Anforderungen werden bei der Auswahl der Architektur berücksichtigt.
- Sie können die Compliance bestätigen und Audit-Berichte erstellen.

Typische Anti-Muster:

- Teile Ihres Workloads fallen unter das Regelwerk des Payment Card Industry Data Security Standard (PCI-DSS), Ihr Workload speichert Kreditkartendaten jedoch unverschlüsselt.
- Ihren Software-Entwicklern und -Architekten ist das Compliance-Regelwerk, das Ihre Organisation einhalten muss, nicht bekannt.
- Das jährliche Audit Systems and Organizations Control (SOC2) Type II steht bevor und Sie können nicht nachweisen, dass Kontrollelemente implementiert sind.

Vorteile der Nutzung dieser bewährten Methode:

- Die Bewertung und das Verständnis der Compliance-Anforderungen für Ihren Workload liefern die Grundlage dafür, wie Sie Ihre Anstrengungen zur Bereitstellung eines geschäftlichen Mehrwerts priorisieren.
- Sie wählen die Ihrem Compliance-Regelwerk entsprechenden Standorte und Technologien.
- Indem Sie Ihren Workload so entwerfen, dass Überprüfungen möglich sind, können Sie nachweisen, dass Sie das Compliance-Regelwerk einhalten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Wenn Sie diese bewährte Methode implementieren, bedeutet dies, dass Sie Compliance-Anforderungen in den Entwurfsprozess für Ihre Architektur integrieren. Ihren Teammitgliedern ist das erforderliche Compliance-Regelwerk bekannt. Sie bestätigen Ihre Compliance mit diesem Regelwerk.

Kundenbeispiel

AnyCompany Retail speichert Kreditkarteninformationen für Kunden. Die Entwickler im Team für die Kartenspeicherung wissen, dass sie das PCI-DSS-Regelwerk einhalten müssen. Sie haben Schritte unternommen, um nachzuweisen, dass die Kreditkarteninformationen in Übereinstimmung mit dem PCI-DSS-Regelwerk sicher gespeichert und aufgerufen werden. Jedes Jahr arbeiten sie mit dem Sicherheitsteam zusammen, um die Compliance zu bestätigen.

Implementierungsschritte

1. Arbeiten Sie mit Ihrem Sicherheits- und Governance-Team zusammen, um zu ermitteln, welche branchenspezifischen, regulatorischen oder internen Compliance-Regelwerke Ihr Workload einhalten muss. Integrieren Sie die Compliance-Regelwerke in Ihren Workload.
   a. Bestätigen Sie die durchgängige Compliance von AWS-Ressourcen mit Services wie AWS Compute Optimizer und AWS Security Hub.
2. Informieren Sie Ihre Teammitglieder über die Compliance-Anforderungen, damit diese den Workload in Übereinstimmung mit den Anforderungen betreiben und weiterentwickeln können. Die Compliance-Anforderungen sollten bei architektur- und technologiebezogenen Entscheidungen berücksichtigt werden.
3. Je nach Compliance-Regelwerk müssen Sie möglicherweise einen Audit- oder Compliance-Bericht erstellen. Arbeiten Sie mit Ihrer Organisation zusammen, um diesen Prozess so weit wie möglich zu automatisieren.
   a. Verwenden Sie Services wie AWS Audit Manager, um die Compliance zu bestätigen und Audit-Berichte zu erstellen.
   b. AWS-Dokumente zu Sicherheit und Compliance können mit AWS Artifact heruntergeladen werden.

Grad des Aufwands für den Implementierungsplan: mittel. Die Implementierung von Compliance-Regelwerken kann eine Herausforderung darstellen. Das Erstellen von Audit-Berichten oder Compliance-Dokumenten sorgt für zusätzlichen Aufwand.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP03 Identifizieren und Validieren von Kontrollzielen – Sicherheitskontrollziele sind ein wichtiger Bestandteil der allgemeinen Compliance.

- SEC01-BP06 Automatisieren von Tests und Validierung von Sicherheitskontrollen in Pipelines – Validieren Sie die Sicherheitskontrollen als Teil Ihrer Pipelines. Sie können auch eine Compliance-Dokumentation für neue Änderungen erstellen.
- SEC07-BP02 Definieren von Datenschutzkontrollen – Viele Compliance-Regelwerke umfassen Richtlinien für den Umgang mit und die Speicherung von Daten.
- SEC10-BP03 Vorbereiten forensischer Funktionen – Forensische Funktionen können mitunter bei Prüfungen der Compliance verwendet werden.

Zugehörige Dokumente:

- AWS Compliance Center
- AWS-Compliance-Ressourcen
- AWS Risk and Compliance Whitepaper (AWS-Whitepaper: Risiko und Compliance)
- AWS-Modell der geteilten Verantwortung
- AWS-Services im Rahmen des Compliance-Programms

Zugehörige Videos:

- AWS re:Invent 2020: Achieve compliance as code using AWS Compute Optimizer(AWS re:Invent 2020: Mit AWS Compute Optimizer Compliance als Code erzielen)
- AWS re:Invent 2021 - Cloud compliance, assurance, and auditing (AWS re:Invent 2021 – Cloud-Compliance, Sicherheit und Prüfungen)
- AWS Summit ATL 2022 - Implementing compliance, assurance, and auditing on AWS (COP202) (AWS Summit ATL 2022 – Compliance, Sicherheit und Prüfungen für AWS implementieren (COP202))

Zugehörige Beispiele:

- Bewährte Methoden für PCI DSS und AWS Foundational Security auf AWS

Zugehörige Services:

- AWS Artifact
- AWS Audit Manager

- AWS Compute Optimizer
- AWS Security Hub

OPS01-BP05 Bewerten der Bedrohungsszenarien

Bewerten Sie Bedrohungen für das Unternehmen (z. B. Wettbewerb, Geschäftsrisiken und -verpflichtungen, operative Risiken und Bedrohungen der Informationssicherheit) und pflegen Sie aktuelle Informationen in einem Risikoregister. Berücksichtigen Sie die Auswirkungen von Risiken, wenn Sie bestimmen, auf welche Bereiche die Anstrengungen fokussiert werden sollen.

Das Well-Architected Framework legt den Schwerpunkt auf Lernen, Messen und Verbessern. Es bietet einen konsistenten Ansatz, mit dem Sie Architekturen bewerten und Designs implementieren können, die sich im Laufe der Zeit skalieren lassen. AWS stellt das AWS Well-Architected Tool bereit, mit dem Sie Ihren Ansatz vor der Entwicklung, den Status Ihrer Workloads vor der Produktion und den Status Ihrer Workloads in der Produktion überprüfen können. Sie können sie mit den neuesten bewährten Methoden für die AWS-Architektur vergleichen, den Gesamtstatus Ihrer Workloads überwachen und Einblicke in potenzielle Risiken erhalten.

AWS-Kunden haben auch die Möglichkeit, die Architektur ihrer geschäftskritischen Workloads auf die Einhaltung bewährter AWS-Methoden hin überprüfen zu lassen (Well-Architected Review). Für Kunden mit Enterprise Support wird eine Überprüfung des Betriebs (Operations Review) angeboten. Damit haben sie die Möglichkeit, Lücken in ihrem Cloud-Ansatz aufzuzeigen.

Aufgrund der teamübergreifenden Natur dieser Überprüfungen erhalten Sie ein allgemeines Verständnis Ihrer Workloads und können erkennen, wie Team-Rollen zum Erfolg beitragen. Die bei den Überprüfungen gefundenen Punkte können Ihnen beim Festlegen Ihrer Prioritäten helfen.

AWS Trusted Advisor bietet als Tool Zugriff auf verschiedene wichtige Prüfungen, die Optimierungsempfehlungen ausgeben. Diese Informationen können Ihnen beim Festlegen Ihrer Prioritäten helfen. Kunden mit Business und Enterprise Support erhalten Zugriff auf weitere Prüfungen in den Bereichen Sicherheit, Zuverlässigkeit, Leistung und Kostenoptimierung, die beim Festlegen von Prioritäten noch hilfreicher sind.

Gewünschtes Ergebnis:

- Sie überprüfen regelmäßig Well-Architected und Trusted Advisor-Ergebnisse und reagieren darauf.
- Sie sind über den neuesten Patch-Status Ihrer Services informiert.
- Sie kennen das Risiko und die Auswirkungen bekannter Bedrohungen und handeln entsprechend.

- Sie implementieren bei Bedarf Abhilfemaßnahmen.
- Sie kommunizieren Aktionen und Kontext.

Typische Anti-Muster:

- Sie verwenden in Ihrem Produkt eine alte Version einer Softwarebibliothek. Ihnen ist nicht bewusst, dass für die Bibliothek Sicherheitsaktualisierungen vorliegen, mit denen Probleme behoben werden, die unbeabsichtigte Auswirkungen auf Ihren Workload haben können.
- Ein Mitbewerber hat soeben eine Version seines Produkts veröffentlicht, in der viele Probleme behoben werden, die Kunden an Ihrem Produkt bemängeln. Die Behebung dieser bekannten Probleme hatte für Sie bisher keine Priorität.
- Regulierungsbehörden nehmen Unternehmen wie Ihres, die nicht den gesetzlichen Compliance-Anforderungen entsprechen, verstärkt ins Visier. Sie haben Ihre ausstehenden Compliance-Anforderungen nicht priorisiert.

Vorteile der Einführung dieser bewährten Methode: Sie identifizieren und verstehen die Bedrohungen für Ihre Organisation und Ihren Workload, was Ihnen bei der Entscheidung hilft, welche Bedrohungen angegangen werden müssen, wo die Prioritäten liegen und welche Ressourcen dafür erforderlich sind.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

- Bewerten Sie die Bedrohungslandschaft: Bewerten Sie Bedrohungen für das Unternehmen (z. B. Konkurrenz, Geschäftsrisiken und -verpflichtungen, operative Risiken und Bedrohungen der Informationssicherheit), damit Sie die jeweiligen Auswirkungen berücksichtigen können, wenn Sie bestimmen, auf welche Bereiche die operativen Anstrengungen konzentriert werden sollten.
  - Aktuelle AWS-Sicherheitsmitteilungen
  - AWS Trusted Advisor
- Verwalten Sie ein Bedrohungsmodell: Erstellen und verwalten Sie ein Bedrohungsmodell, in dem potenzielle Bedrohungen, geplante und vorhandene Maßnahmen und deren Priorität festgehalten werden. Untersuchen Sie, wie wahrscheinlich es ist, dass sich Bedrohungen als Vorfälle äußern, wie hoch die Kosten für die Wiederherstellung nach diesen Vorfällen sind, welche Schäden zu erwarten sind und wie viel es kostet, diese Vorfälle zu verhindern. Überarbeiten Sie die Prioritäten, wenn sich der Inhalt des Bedrohungsmodells ändert.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP07 Identifizieren von Bedrohungen und Priorisieren von Abhilfemaßnahmen unter Verwendung eines Bedrohungsmodells

Zugehörige Dokumente:

- AWS Cloud-Compliance
- Aktuelle AWS-Sicherheitsmitteilungen
- AWS Trusted Advisor

Zugehörige Videos:

- AWS re:Inforce 2023 – Ein Tool zur Verbesserung Ihrer Bedrohungsmodellierung

OPS01-BP06 Bewerten von Kompromissen und Abwägen der Vorteile und Risiken

Konkurrierende Interessen mehrerer Parteien können eine Herausforderung darstellen, wenn es darum geht, Anstrengungen zu priorisieren, Fähigkeiten aufzubauen und Ergebnisse zu erzielen, die auf die Geschäftsstrategien abgestimmt sind. So können Sie möglicherweise aufgefordert werden, die Markteinführung neuer Features zu beschleunigen, anstatt die Kosten für die IT-Infrastruktur zu optimieren. Dies kann dazu führen, dass die Interessen zweier Parteien miteinander in Widerspruch stehen. In solchen Situationen muss eine höhere Stelle hinzugezogen werden, um eine Entscheidung zur Lösung des Konflikts zu treffen. Daten sind erforderlich, um den Entscheidungsprozess von emotionalen Komponenten zu befreien.

Ähnliche Herausforderungen können auf taktischer Ebene auftreten. Beispielsweise kann die Wahl zwischen relationalen oder nicht relationalen Datenbanktechnologien erhebliche Auswirkungen auf den Betrieb einer Anwendung haben. Daher ist es wichtig, die voraussichtlichen Ergebnisse verschiedener Entscheidungen zu verstehen.

AWS kann Ihnen helfen, Ihre Teams über AWS und die verfügbaren Services zu schulen, sodass alle Mitarbeiter wissen, welche Auswirkungen ihre Entscheidungen auf Ihren Workload haben können. Nutzen Sie bei der Schulung Ihrer Teams die vom AWS Support (AWS Knowledge Center, AWS-

Diskussionsforen und AWS Support Center) bereitgestellten Ressourcen und AWS-Dokumente. Bei weiteren Fragen wenden Sie sich bitte an AWS Support.

AWS teilt auch bewährte operative Methoden und Muster in der Amazon Builders' Library. Eine Vielzahl weiterer nützlicher Informationen finden Sie im AWS-Blogund im offiziellen AWS-Podcast.

Gewünschtes Ergebnis: Ein klar definiertes Framework zur Entscheidungsfindung, das das Treffen wichtiger Entscheidungen auf allen Ebenen Ihrer Cloud-Bereitstellungsorganisation erleichtert. Dieses Framework umfasst Features wie ein Risikoregister, definierte Rollen mit Entscheidungsbefugnissen und definierte Modelle für die einzelnen Entscheidungsebenen. Dieses Framework legt im Voraus fest, wie Konflikte gelöst werden, welche Daten präsentiert werden müssen und wie Optionen priorisiert werden, sodass Sie einmal gefasste Beschlüsse sofort umsetzen können. Das Framework zur Entscheidungsfindung beinhaltet einen standardisierten Ansatz zur Überprüfung und Abwägung der Vorteile und Risiken einzelner Entscheidungen, um die Tragweite etwaiger Kompromisse abzuschätzen. Dazu können externe Faktoren gehören wie die Einhaltung gesetzlicher Vorschriften.

Typische Anti-Muster:

- Ihre Investoren fordern, dass Sie die Compliance mit Payment Card Industry Data Security Standards (PCI DSS) nachweisen. Sie denken nicht über einen möglichen Kompromiss zwischen der Erfüllung dieser Anfrage und der Fortsetzung Ihrer derzeitigen Entwicklungsaktivitäten nach. Stattdessen fahren Sie mit der Entwicklung fort, ohne einen Compliance-Nachweis zu erbringen. Ihre Investoren beenden die Unterstützung Ihres Unternehmens, da sie Bedenken bezüglich der Sicherheit Ihrer Plattform und ihrer Investitionen haben.
- Sie haben sich entschieden, eine Bibliothek einzubinden, die einer Ihrer Entwickler „im Internet entdeckt“ hat. Sie haben keine Bewertung der Risiken durchgeführt, die die Einführung dieser Bibliothek aus einer unbekannten Quelle bergen kann, und wissen nicht, ob sie Schwachstellen oder schädlichen Code enthält.
- Die ursprüngliche geschäftliche Begründung für Ihre Migration basierte auf der Modernisierung von 60 % Ihrer Anwendungsworkloads. Aufgrund technischer Schwierigkeiten wurde jedoch beschlossen, nur 20 % zu modernisieren. Dies führte langfristig zu einer Reduzierung der geplanten Leistungen, zu einem erhöhten Aufwand für die Infrastrukturteams bei der manuellen Wartung von Legacy-Systemen und zu einer stärkeren Abhängigkeit von der Entwicklung neuer Fähigkeiten in Ihren Infrastrukturteams, die diese Änderung nicht geplant hatten.

Vorteile der Einführung dieser bewährten Methode: Umfassende Abstimmung und Unterstützung der Geschäftsprioritäten auf Vorstandsebene, Kenntnis der Erfolgsrisiken, Treffen fundierter

Entscheidungen und angemessenes Handeln, wenn Risiken die Erfolgsaussichten trüben. Indem Sie die Auswirkungen und Konsequenzen Ihrer Entscheidungen verstehen, können Sie Ihre Optionen priorisieren und Führungskräfte schneller zu einer Einigung bringen, was zu besseren Geschäftsergebnissen führt. Wenn Sie die Vorteile Ihrer Entscheidungen erkennen und sich der Risiken für Ihre Organisation bewusst sind, können Sie datengestützte Entscheidungen treffen, anstatt sich auf Anekdoten verlassen zu müssen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Die Abwägung von Nutzen und Risiken sollte von einem Leitungsorgan übernommen werden, das die Anforderungen für wichtige Entscheidungen festlegt. Sie möchten, dass Entscheidungen basierend auf ihrem Nutzen für die Organisation getroffen und priorisiert werden und die damit verbundenen Risiken bekannt sind. Präzise Informationen bilden die Grundlage für die Entscheidungen Ihrer Organisation. Diese sollten auf soliden Messungen beruhen und durch branchenübliche Verfahren der Kosten-Nutzen-Analyse definiert werden. Damit Entscheidungen auf diese Art getroffen werden können, müssen Sie ein Gleichgewicht zwischen zentralisierter und dezentralisierter Autorität herstellen. Es gibt immer einen Kompromiss. Daher ist es wichtig zu verstehen, wie sich jede Entscheidung auf definierte Strategien und angestrebte Geschäftsergebnisse auswirkt.

Implementierungsschritte

1. Formalisieren Sie die Verfahren zur Leistungsmessung innerhalb eines ganzheitlichen Cloud-Governance-Frameworks.
   a. Bringen Sie die zentrale Kontrolle der Entscheidungsfindung in Einklang mit konkreten dezentralen Entscheidungsbefugnissen.
   b. Machen Sie sich bewusst, dass nicht für jeden Beschluss aufwendige Entscheidungsprozesse vonnöten sind, da sie Sie verlangsamen können.
   c. Integrieren Sie externe Faktoren in Ihren Entscheidungsprozess (wie Compliance-Anforderungen).
2. Richten Sie ein gemeinsames Framework zur Entscheidungsfindung für verschiedene Entscheidungsebenen ein, in dem festgelegt ist, wer Entscheidungen bei widersprüchlichen Interessen trifft.
   a. Zentralisieren Sie einseitige Entscheidungen, die irreversibel sein könnten.
   b. Lassen Sie leicht revidierbare Entscheidungen von Führungskräften auf niedrigerer Ebene treffen.

3. Machen Sie sich mit den Nutzen und Risiken vertraut und wägen Sie sie ab. Wägen Sie den Nutzen von Entscheidungen gegen die damit einhergehenden Risiken ab.
   a. Ermitteln von Vorteilen: Ermitteln Sie die Vorteile auf Basis der geschäftlichen Ziele, Anforderungen und Prioritäten. Beispiele hierfür sind die Auswirkungen auf den Business Case, die Markteinführungszeit, Sicherheit, Zuverlässigkeit, Leistung und Kosten.
   b. Ermitteln von Risiken: Ermitteln Sie die Risiken auf Basis der geschäftlichen Ziele, Anforderungen und Prioritäten. Zu diesen Prioritäten zählen beispielsweise eine kurze Markteinführungszeit, Sicherheit, Zuverlässigkeit, Leistung und Kosten.
   c. Abwägen von Vorteilen und Risiken und Treffen fundierter Entscheidungen: Ermitteln Sie die Auswirkungen von Vorteilen und Risiken basierend auf den Zielen, Bedürfnissen und Prioritäten Ihrer wichtigsten Stakeholder, zu denen auch die Bereiche Betriebswirtschaft, Entwicklung und Operationen zählen. Bewerten Sie den Wert eines Vorteils anhand der Wahrscheinlichkeit, dass sich das Risiko tatsächlich bewahrheitet, sowie der Kosten der jeweiligen Auswirkungen. Eine schnellere Markteinführung zu Lasten der Zuverlässigkeit könnte beispielsweise einen Wettbewerbsvorteil bedeuten. Wenn jedoch Probleme mit der Zuverlässigkeit auftreten, kann dies zu einer verringerten Betriebszeit führen.
4. Setzen Sie wichtige Entscheidungen programmatisch um, um die Einhaltung von Compliance-Anforderungen zu automatisieren.
5. Nutzen Sie branchenübliche Frameworks und Funktionen wie Value Stream Analysis und LEAN, um die aktuelle Leistung und Geschäftsmetriken abzubilden und Iterationen der Fortschritte zur Verbesserung dieser Metriken zu definieren.

Aufwand des Implementierungsplans: mittel bis hoch

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP05 Bewerten der Bedrohungsszenarien

Zugehörige Dokumente:

- Elemente der Day-1-Kultur von Amazon | Schnell gute Entscheidungen treffen
- Cloud-Governance
- Cloud-Umgebung für Management und Governance
- Governance in der Cloud und im digitalen Zeitalter: Teil 1 und 2

Zugehörige Videos:

- Podcast | Jeff Bezos | Über das Treffen von Entscheidungen

Zugehörige Beispiele:

- Fundierte Entscheidungen mithilfe von Daten treffen (The DevOps Sagas)
- Nutzung von Wertstromanalysen in der Entwicklung zur Identifizierung von Einschränkungen bei DevOps-Ergebnissen

Betriebsmodell

Ihre Teams müssen ihre Rolle beim Erreichen von Geschäftsergebnissen verstehen. Teams müssen ihre Rollen beim Erfolg anderer Teams verstehen, die Rolle anderer Teams bei ihrem eigenen Erfolg und sie müssen gemeinsame Ziele haben. Wenn sie Verantwortlichkeit, Zuständigkeit und Entscheidungsfindung nachvollziehen können und wissen, wer dazu berechtigt ist, Entscheidungen zu treffen, können ihre Anstrengungen fokussiert und der Nutzen Ihrer Teams maximiert werden.

Die Anforderungen eines Teams werden durch die Branche, das Unternehmen, die Zusammensetzung des Teams und die Merkmale seiner Workloads beeinflusst. Es ist nicht sinnvoll, davon auszugehen, dass ein einziges Betriebsmodell alle Teams und ihre Workloads unterstützen kann.

Die Anzahl der Betriebsmodelle in einem Unternehmen wird mit der Anzahl der Entwicklungsteams wahrscheinlich steigen. Möglicherweise müssen Sie eine Kombination aus Betriebsmodellen verwenden.

Die Übernahme von Standards und die Nutzung von Services kann den Betrieb vereinfachen und den Support-Aufwand in Ihrem Betriebsmodell begrenzen. Der Vorteil der Entwicklungsbemühungen zu gemeinsamen Standards wird durch die Anzahl der Teams verstärkt, die den Standard eingeführt haben und neue Funktionen übernehmen werden.

Es ist wichtig, dass Mechanismen vorhanden sind, um Ergänzungen, Änderungen und Ausnahmen zu Standards zur Unterstützung der Aktivitäten der Teams anzufordern. Ohne diese Option werden Standards zu einer Einschränkung der Innovation. Anträge sollten nach einer Bewertung der Vorteile und Risiken genehmigt werden, wenn sie sinnvoll sind.

Eine klar definierte Gruppe von Verantwortlichkeiten verringert die Häufigkeit widersprüchlicher und redundanter Bemühungen. Geschäftsergebnisse sind leichter zu erzielen, wenn es eine starke Ausrichtung und Beziehungen zwischen Geschäfts-, Entwicklungs- und Betriebsteams gibt.

Betriebsmodell-2-mal-2-Darstellungen

Diese Betriebsmodell-2-mal-2-Darstellungen sind Abbildungen, die Ihnen helfen, die Beziehungen zwischen Teams in Ihrer Umgebung zu verstehen. Diese Diagramme konzentrieren sich darauf, wer was tut und welche Beziehungen zwischen Teams bestehen. Wir werden jedoch auch Governance und Entscheidungsfindung im Kontext dieser Beispiele besprechen.

Unsere Teams haben möglicherweise Zuständigkeiten in mehreren Teilen mehrerer Modelle, abhängig von den Workloads, die sie unterstützen. Möglicherweise möchten Sie spezialisiertere Disziplinbereiche als die beschriebenen High-Level-Bereiche aufschlüsseln. Es besteht das Potenzial für endlose Variationen bei diesen Modellen, wenn Sie Aktivitäten trennen oder aggregieren oder Teams überlagern und spezifischere Details bereitstellen.

Sie können feststellen, dass Sie sich überschneidende oder nicht erkannte Funktionen in Teams haben, die einen zusätzlichen Vorteil bieten oder zu Effizienzsteigerungen führen können. Sie können auch unbefriedigte Bedürfnisse in Ihrem Unternehmen identifizieren, die Sie berücksichtigen können.

Prüfen Sie bei der Bewertung der organisatorischen Veränderungen die Kompromisse zwischen Modellen, wo sich Ihre einzelnen Teams innerhalb der Modelle befinden (jetzt und nach der Änderung), wie sich die Beziehung und Verantwortlichkeiten Ihrer Teams ändern werden und ob die Vorteile die Auswirkungen auf Ihr Unternehmen rechtfertigen.

Sie können mit jedem der folgenden vier Betriebsmodelle erfolgreich sein. Einige Modelle eignen sich besser für bestimmte Anwendungsfälle oder an bestimmten Punkten in Ihrer Entwicklung. Einige dieser Modelle bieten möglicherweise Vorteile gegenüber denjenigen, die in Ihrer Umgebung verwendet werden.

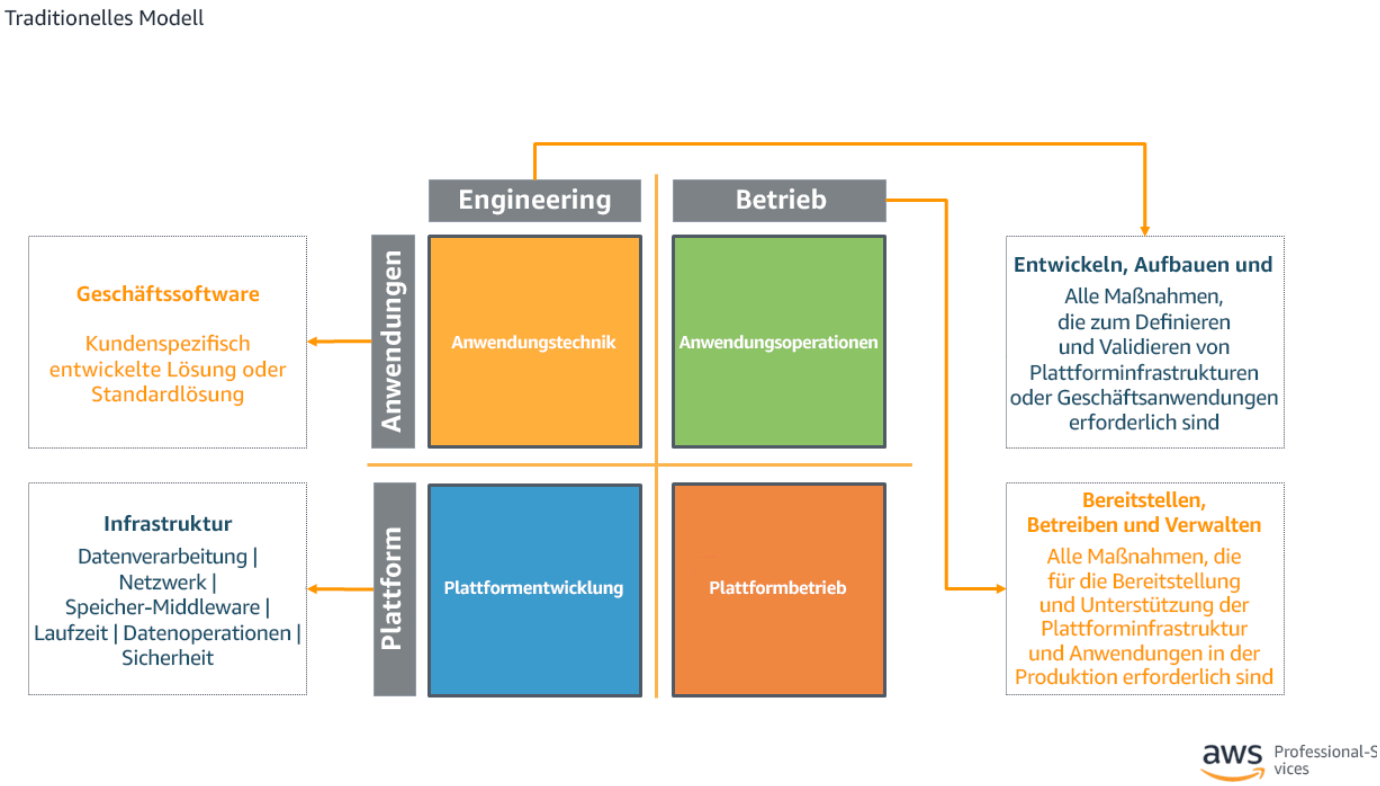
Themen

- Getrennte AEO und IEO mit dezentralisierter Governance

Vollständig getrenntes Betriebsmodell

Im folgenden Diagramm werden auf der vertikalen Achse Anwendungen und Infrastruktur angezeigt. Anwendungen beziehen sich auf den Workload, der einem Geschäftsergebnis dient, und können kundenspezifisch entwickelte oder gekaufte Software sein. Infrastruktur bezieht sich auf die physische und virtuelle Infrastruktur und andere Software, die diesen Workload unterstützt.

Auf der horizontalen Achse haben wir Engineering und Operations. Engineering bezieht sich auf die Entwicklung, Erstellung und das Testen von Anwendungen und Infrastruktur. Operations ist die Bereitstellung, Aktualisierung und laufende Unterstützung von Anwendungen und Infrastruktur.



In vielen Unternehmen ist dieses „vollständig getrennte“ Modell vorhanden. Die Aktivitäten in jedem Quadranten werden von einem separaten Team ausgeführt. Die Arbeit wird zwischen Teams über Mechanismen wie Arbeitsanfragen, Arbeitswarteschlangen, Tickets oder über ein IT-Service-Management (ITSM)-System weitergegeben.

Der Übergang von Aufgaben zu oder zwischen Teams erhöht die Komplexität und schafft Engpässe und Verzögerungen. Anfragen können verzögert werden, bis sie eine Priorität haben.

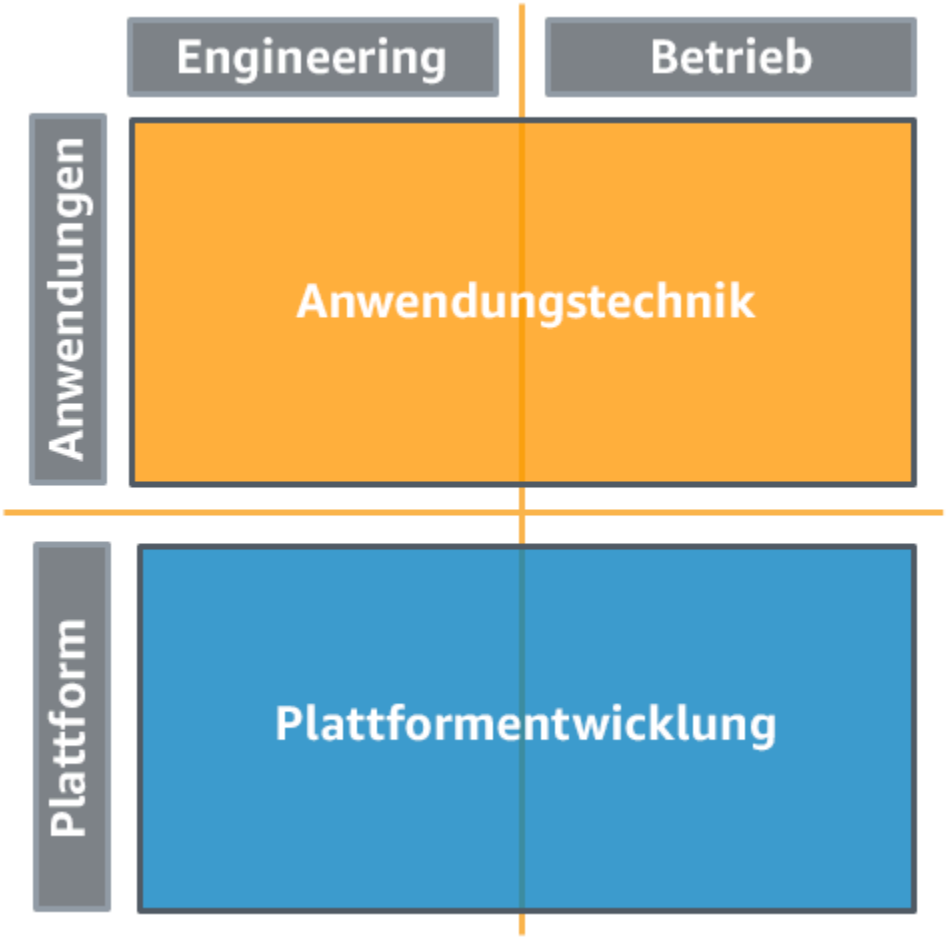
Verspätet erkannte Fehler erfordern möglicherweise eine erhebliche Nachbearbeitung und müssen möglicherweise die gleichen Teams und ihre Funktionen erneut durchlaufen. Wenn es Vorfälle gibt, die Maßnahmen durch Technikerteams erfordern, verzögern sich ihre Antworten durch die Übergabe der Aktivität.

Es besteht ein höheres Risiko einer Fehlausrichtung, wenn Geschäfts-, Entwicklungs- und Betriebsteams um die ausgeführten Aktivitäten oder Funktionen herum organisiert sind. Dies kann dazu führen, dass Teams sich auf ihre spezifischen Verantwortlichkeiten konzentrieren, anstatt sich auf das Erreichen von Geschäftsergebnissen zu konzentrieren. Teams können eng spezifiziert, physisch isoliert oder logisch isoliert sein, was die Kommunikation und Zusammenarbeit behindert.

Getrenntes Application Engineering and Operations (AEO) und Infrastructure Engineering and Operations (IEO) mit zentralisierter Governance

Dieses Modell "Getrennte AEO und IEO" folgt einer "You build it you run it"-Methodik.

Ihre Anwendungstechniker und Entwickler führen sowohl das Engineering als auch den Betrieb ihrer Workloads durch. Ebenso führen Ihre Infrastrukturtechniker sowohl das Engineering als auch den Betrieb der Plattformen durch, die sie zur Unterstützung von Anwendungsteams verwenden.



In diesem Beispiel behandeln wir Governance als zentralisiert. Standards werden an die Anwendungsteams verteilt, bereitgestellt oder weitergegeben.

Sie sollten Tools oder Services verwenden, mit denen Sie Ihre Umgebungen kontenübergreifend verwalten können, z. B. AWS Organizations. Services wie AWS Control Tower erweitern diese Verwaltungsfunktion, sodass Sie Pläne (die Ihre Betriebsmodelle unterstützen) für die Einrichtung von Konten definieren, laufende Governance mit AWS Organizations anwenden und die Bereitstellung neuer Konten automatisieren können.

"You build it you run it" bedeutet nicht, dass das Anwendungsteam für den gesamten Stack, die Tool-Chain und die Plattform verantwortlich ist.

Das Plattform-Engineering-Team bietet eine standardisierte Reihe von Services (z. B. Entwicklungstools, Überwachungstools, Sicherungs- und Wiederherstellungstools sowie Netzwerk) für das Anwendungsteam. Das Plattformteam kann dem Anwendungsteam auch Zugriff auf genehmigte Cloud-Anbieter-Services, bestimmte Konfigurationen derselben oder beides gewähren.

Mechanismen, die eine Self-Service-Funktion für die Bereitstellung genehmigter Services und Konfigurationen bereitstellen, wie z. B. Service Catalog, können helfen, Verzögerungen im Zusammenhang mit Erfüllungsanfragen einzuschränken und gleichzeitig Governance zu erzwingen.

Das Plattformteam ermöglicht eine vollständige Stack-Transparenz, sodass Anwendungsteams, die ihre Anwendungen nutzen, zwischen Problemen mit ihren Anwendungskomponenten und den Services und Infrastrukturkomponenten unterscheiden können. Das Plattformteam kann auch Unterstützung bei der Konfiguration dieser Services leisten und Anleitungen zur Verbesserung des Betriebs der Anwendungsteams bieten.

Wie bereits erwähnt, ist es wichtig, dass für das Anwendungsteam Mechanismen vorhanden sind, um Ergänzungen, Änderungen und Ausnahmen zu Standards zur Unterstützung der Aktivitäten der Teams und der Innovation ihrer Anwendung anzufordern.

Das "Separated AEO IEO"-Modell bietet starke Feedback-Schleifen für Anwendungsteams. Der tägliche Betrieb eines Workloads erhöht den Kontakt mit Kunden entweder durch direkte Interaktion oder indirekt durch Support- und Funktionsanfragen. Durch diese erhöhte Sichtbarkeit können Anwendungsteams Probleme schneller beheben. Das tiefere Engagement und die engere Beziehung bieten Einblicke in die Kundenbedürfnisse und ermöglichen schnellere Innovationen.

All dies gilt auch für das Plattformteam, das die Anwendungsteams unterstützt.

Übernommene Standards können vorab für die Verwendung genehmigt werden, wodurch der für die Produktion erforderliche Prüfungsumfang reduziert wird. Durch den Einsatz von durch das Plattformteam bereitgestellte unterstützte und getestete Standards kann die Häufigkeit von Problemen mit diesen Services reduziert werden. Durch die Übernahme von Standards können sich Anwendungsteams auf die Differenzierung ihrer Workloads konzentrieren.

Getrennte AEO und IEO mit zentralisierter Governance und einem Serviceanbieter

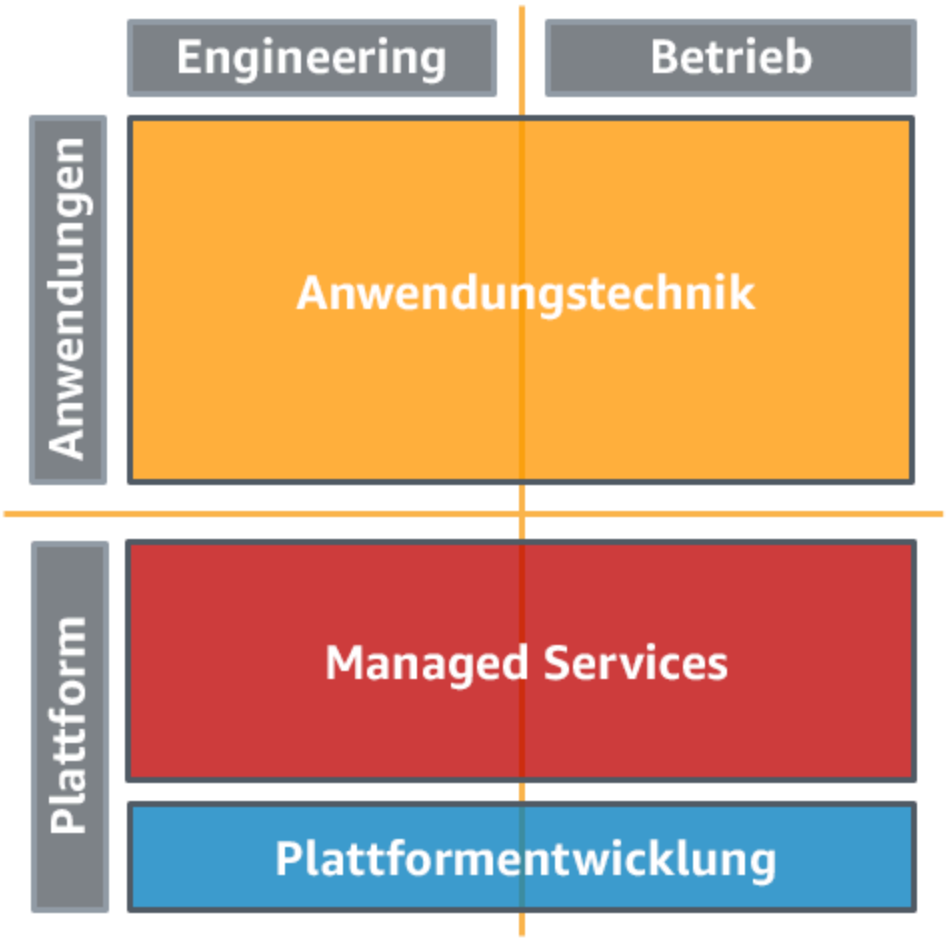
Dieses Modell "Getrennte AEO und IEO" folgt einer "You build it you run it"-Methodik.

Ihre Anwendungstechniker und Entwickler führen sowohl das Engineering als auch den Betrieb ihrer Workloads durch.

Ihr Unternehmen verfügt möglicherweise nicht über die vorhandenen Fähigkeiten oder Teammitglieder, um ein dediziertes Plattform-Engineering- und Betriebsteam zu unterstützen, oder Sie möchten nicht mehr Zeit und Aufwand dafür investieren.

Alternativ können Sie ein Plattformteam haben, das sich auf die Entwicklung von Funktionen konzentriert, die Ihr Unternehmen differenzieren, aber Sie möchten den undifferenzierten täglichen Betrieb an einen Outsourcer auslagern.

Anbieter von verwalteten Services wie AWS Managed Services, AWS Managed Services-Partneroder Anbieter von verwalteten Services im AWS-Partnernetzwerkstellen Fachwissen zur Implementierung von Cloud-Umgebungen bereit und unterstützen Ihre Sicherheits- und Compliance-Anforderungen und Geschäftsziele.



Für diese Variante behandeln wir Governance als zentralisiert und verwaltet durch das Plattformteam, wobei die Kontoerstellung und Richtlinien mit AWS Organizations und AWS Control Tower verwaltet werden.

Dieses Modell erfordert, dass Sie Ihre Mechanismen so ändern, dass sie mit denen Ihres Serviceproviders zusammenarbeiten. Es löst nicht Engpässe und Verzögerungen, die durch den Übergang von Aufgaben zwischen Teams, einschließlich Ihres Serviceproviders, oder durch den

potenziellen Nachbearbeitungsaufwand im Zusammenhang mit der verspäteten Fehlererkennung entstehen.

Sie profitieren von den Standards, bewährten Methoden, Prozessen und dem Fachwissen Ihrer Anbieter. Außerdem profitieren Sie von den Vorteilen der fortlaufenden Entwicklung ihrer Service-Angebote.

Durch die Erweiterung Ihres Betriebsmodells um Managed Services können Sie Zeit und Ressourcen sparen, Ihre internen Teams klein halten und sich auf strategische Ergebnisse konzentrieren, die Ihr Unternehmen auszeichnen, anstatt neue Fähigkeiten und Kompetenzen zu entwickeln.

Getrennte AEO und IEO mit zentralisierter Governance und einem internen Serviceanbieter-Beratungspartner

Dieses „Getrennte AEO und IEO“-Modell folgt einer „You build it you run it“-Methodik.

Sie möchten, dass Ihre Anwendungsteams die technischen und betrieblichen Aktivitäten für ihre Workloads durchführen und eine eher DevOps-ähnliche Kultur annehmen.

Ihre Anwendungsteams sind möglicherweise gerade dabei zu migrieren, die Cloud einzuführen oder Ihre Workloads zu modernisieren, und verfügen nicht über die erforderlichen Fähigkeiten, um die Cloud und den Cloud-Betrieb adäquat zu unterstützen. Dieser Mangel an Fähigkeiten oder Vertrautheit des Anwendungsteams kann Ihre Bemühungen behindern.

Richten Sie ein Cloud Center of Enablement-Team (CCoE) ein, das ein Forum bietet, um Fragen zu stellen, Bedürfnisse zu diskutieren und Lösungen zu finden und diesem Problem so zu begegnen. Je nach den Bedürfnissen Ihres Unternehmens kann das CCoE ein spezielles Expertenteam oder ein virtuelles Team sein, dessen Teilnehmer aus Ihrem gesamten Unternehmen ausgewählt werden. Das CCoE ermöglicht die Cloud-Transformation für Teams, etabliert eine zentralisierte Cloud-Governance und definiert Standards für das Konto- und Organisationsmanagement. Außerdem identifizieren sie erfolgreiche Referenzarchitekturen und Muster für den Einsatz in Unternehmen.

Wir bezeichnen CCoE als Cloud Center of Enablement und nicht als Cloud Center of Excellence, um den Erfolg der unterstützten Teams und das Erreichen von Geschäftsergebnissen in den Vordergrund zu stellen.

Ihr Plattform-Engineering-Team entwickelt die wichtigsten gemeinsamen Plattformfunktionen auf der Grundlage dieser Standards, die von den Anwendungsteams übernommen werden können. Sie kodifizieren die Unternehmensreferenzarchitekturen und -muster, die den Anwendungsteams über

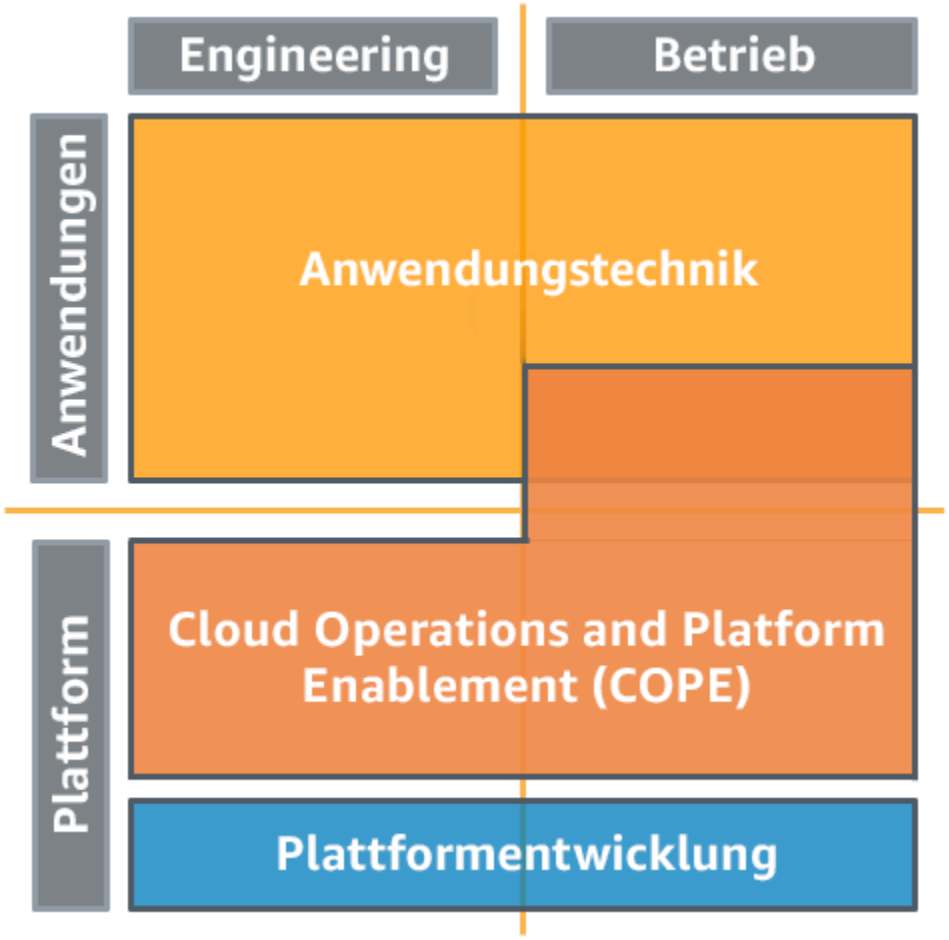
einen Selbstbedienungsmechanismus zur Verfügung gestellt werden. Mithilfe eines Services wie AWS Service Catalog können die Anwendungsteams genehmigte Referenzarchitekturen, -muster, -dienste und -konfigurationen einsetzen, die standardmäßig mit den zentralisierten Governance- und Sicherheitsstandards konform sind.

Das Plattform-Engineering-Team bietet eine standardisierte Reihe von Services (z. B. Entwicklungstools, Überwachungstools, Sicherungs- und Wiederherstellungstools sowie Netzwerk) für das Anwendungsteam.

Ihr Unternehmen verfügt über einen „internen MSP- und Beratungspartner“, der die standardisierten Services verwaltet und unterstützt und den Anwendungsteams beim Aufbau ihrer Cloud-Präsenz auf der Grundlage der Referenzarchitekturen und -muster behilflich ist. Dieses „Cloud Operations and Platform Enablement (COPE)“-Team arbeitet mit den Anwendungsteams zusammen, um sie bei der Einrichtung eines Basisbetriebs zu unterstützen, wobei die Anwendungsteams im Laufe der Zeit immer mehr Verantwortung für ihre Systeme und Ressourcen übernehmen. Das COPE-Team treibt gemeinsam mit den CCoE- und Platform-Engineering-Teams kontinuierliche Verbesserungen voran und fungiert als Ansprechpartner für die Anwendungsteams.

Die Anwendungsteams erhalten Unterstützung bei der Einrichtung von Umgebungen, CICD-Pipelines, Änderungsverwaltung, Beobachtbarkeit und Überwachung sowie bei der Einrichtung von Incident- und Event-Management-Prozessen, die bei Bedarf mit denen des Unternehmens integriert werden. Das COPE-Team beteiligt sich gemeinsam mit den Anwendungsteams an der Durchführung dieser operativen Tätigkeiten, wobei die Beteiligung des COPE-Teams im Laufe der Zeit abnimmt, wenn die Anwendungsteams die Verantwortung übernehmen.

Das Anwendungsteam profitiert von den Fähigkeiten des COPE-Teams und den Erfahrungen, die das Unternehmen gemacht hat. Sie werden durch den Integritätsschutz geschützt, der durch die zentralisierte Governance geschaffen wurden. Das Anwendungsteam baut auf anerkannten Erfolgen auf und profitiert von der kontinuierlichen Weiterentwicklung der von ihm angenommenen Organisationsstandards. Durch den Prozess der Beobachtung und Überwachung erhalten sie einen besseren Einblick in die Funktionsweise ihres Workloads und können die Auswirkungen von Änderungen, die sie an ihrem Workload vornehmen, besser verstehen.



Das COPE-Team behält den Zugang, der für die Unterstützung von Betriebsaktivitäten, die Bereitstellung einer Unternehmenssicht, die das Anwendungsteam übergreift, und die Unterstützung beim Management kritischer Vorfälle erforderlich ist. Das COPE-Team behält die Verantwortung für Tätigkeiten, die als undifferenzierte Schwerstarbeit angesehen werden und die es durch Standardlösungen, die in großem Umfang unterstützt werden können, erfüllt. Sie verwalten auch weiterhin gut verstandene programmatische und automatisierte Betriebsaktivitäten für die Anwendungsteams, damit diese sich auf die Differenzierung ihrer Anwendungen konzentrieren können.

Sie profitieren von den Standards, bewährten Verfahren, Prozessen und dem Fachwissen Ihres Unternehmens, das sich aus den Erfolgen Ihrer Teams ergibt. Sie schaffen einen Mechanismus, um diese erfolgreichen Muster für neue Teams, die die Cloud einführen oder modernisieren, zu reproduzieren. Bei diesem Modell liegt der Schwerpunkt auf der Fähigkeit des COPE-Teams, das Anwendungsteam bei der Etablierung und dem Übergang von Wissen und Artefakten zu unterstützen. Es verringert die operative Belastung der Anwendungsteams und birgt das Risiko, dass

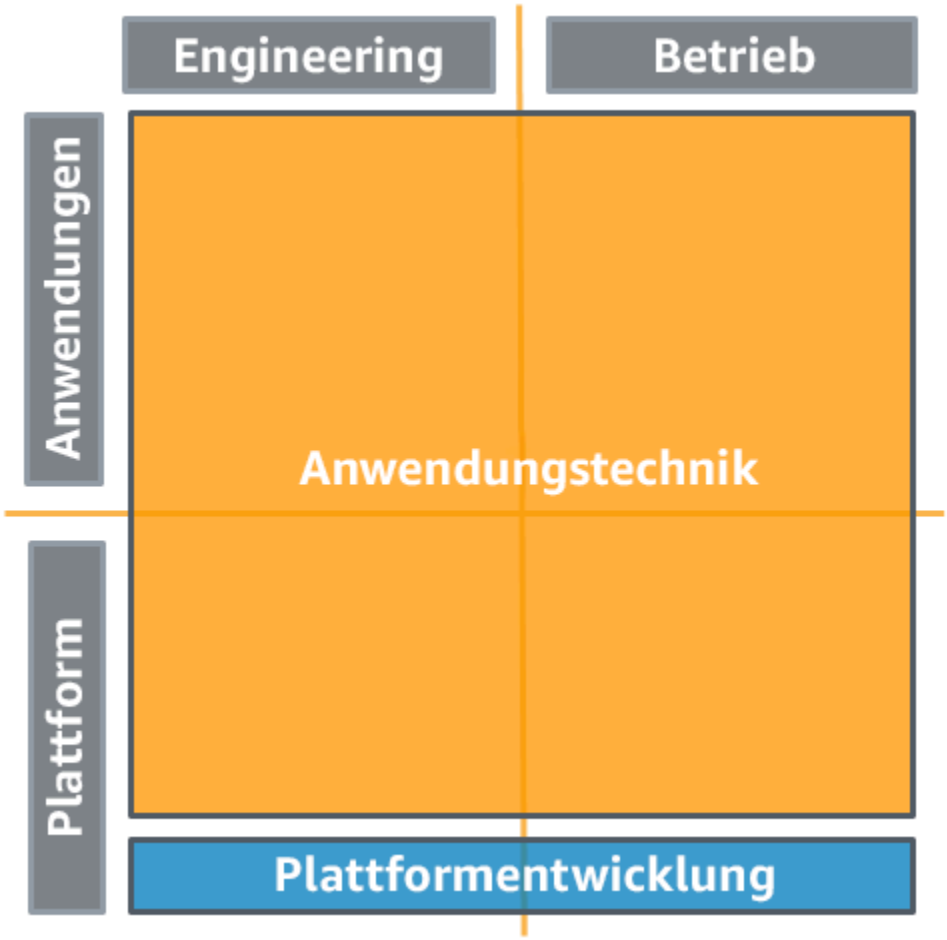
die Anwendungsteams nicht weitgehend unabhängig werden. Es stellt Beziehungen zwischen CCoE, COPE und Anwendungsteams her und schafft so eine Feedbackschleife, die weitere Entwicklungen und Innovationen unterstützt.

Die Einrichtung von CCoE- und COPE-Teams und die Festlegung unternehmensweiter Standards können die Cloud-Einführung erleichtern und Modernisierungsbemühungen unterstützen. Durch die zusätzliche Unterstützung eines COPE-Teams, das Ihren Anwendungsteams als Berater und Partner zur Seite steht, können Sie Hindernisse aus dem Weg räumen, die die Annahme der nützlichen Cloud-Funktionen durch die Anwendungsteams verzögern.

Getrennte AEO und IEO mit dezentralisierter Governance

Dieses Modell "Getrennte AEO und IEO" folgt einer "You build it you run it"-Methodik.

Ihre Anwendungstechniker und Entwickler führen sowohl das Engineering als auch den Betrieb ihrer Workloads durch. Ebenso führen Ihre Infrastrukturtechniker sowohl das Engineering als auch den Betrieb der Plattformen durch, die sie zur Unterstützung von Anwendungsteams verwenden.



In diesem Beispiel behandeln wir Governance als dezentralisiert.

Standards werden nach wie vor vom Plattformteam verteilt, bereitgestellt oder an Anwendungsteams weitergegeben, aber Anwendungsteams können neue Plattformfunktionen zur Unterstützung ihres Workloads entwickeln und betreiben.

Bei diesem Modell gibt es weniger Einschränkungen für das Anwendungsteam, aber das ist mit einer erheblichen Zunahme der Verantwortlichkeiten verbunden. Zusätzliche Fähigkeiten und potenziell auch zusätzliche Teammitglieder müssen vorhanden sein, um die zusätzlichen Plattformfunktionen zu unterstützen. Das Risiko signifikanter Nachbearbeitung wird erhöht, wenn die Qualifikationen nicht ausreichend sind und Fehler nicht frühzeitig erkannt werden.

Sie sollten Richtlinien erzwingen, die nicht spezifisch an Anwendungsteams delegiert sind. Verwenden Sie Tools oder Services, mit denen Sie Ihre Umgebungen kontenübergreifend zentral steuern können, z. B. AWS Organizations. Services wie AWS Control Tower erweitern diese Verwaltungsfunktion, sodass Sie Pläne (die Ihre Betriebsmodelle unterstützen) für die Einrichtung von Konten definieren, laufende Governance mit AWS Organizations anwenden und die Bereitstellung neuer Konten automatisieren können.

Es ist vorteilhaft, dass das Anwendungsteam Mechanismen hat, um Ergänzungen und Änderungen an Standards anzufordern. Sie können möglicherweise neue Standards bereitstellen, die anderen Anwendungsteams Vorteile bieten können. Die Plattformteams können entscheiden, dass die direkte Unterstützung für diese zusätzlichen Funktionen eine effektive Unterstützung für Geschäftsergebnisse darstellt.

Dieses Modell begrenzt Einschränkungen bei einer Innovation mit erheblichen Anforderungen an Fähigkeiten und Teammitglieder. Es behebt viele der Engpässe und Verzögerungen, die durch den Übergang von Aufgaben zwischen Teams entstehen, und fördert gleichzeitig die Entwicklung effektiver Beziehungen zwischen Teams und Kunden.

Beziehungen und Eigentümerschaft

Ihr Betriebsmodell definiert die Beziehungen zwischen Teams und unterstützt identifizierbare Eigentümerschaft und Verantwortlichkeit.

Bewährte Methoden

- OPS02-BP01 Ressourcen haben feste Verantwortliche
- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer

- OPS02-BP03 Betriebsaktivitäten haben feste Besitzer, die für ihre Leistung verantwortlich sind
- OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Zuständigkeiten
- OPS02-BP05 Mechanismen zum Anfordern von Ergänzungen, Änderungen und Ausnahmen sind vorhanden
- OPS02-BP06 Zuständigkeiten zwischen Teams werden vordefiniert oder ausgehandelt

OPS02-BP01 Ressourcen haben feste Verantwortliche

Die Ressourcen für Ihren Workload müssen für die Änderungskontrolle, die Fehlerbehebung und andere Funktionen feste Verantwortliche haben. Verantwortliche werden für Workloads, Konten, Infrastruktur, Plattformen und Anwendungen zugewiesen. Die Verantwortlichkeit wird mit Tools wie einem Zentralverzeichnis oder Metadaten zu Ressourcen erfasst. Der Unternehmenswert der Komponenten bestimmt, welche Prozesse und Verfahren auf diese angewendet werden.

Gewünschtes Ergebnis:

- Mithilfe von Metadaten oder einem Zentralverzeichnis werden feste Verantwortliche für die Ressourcen identifiziert.
- Die Teammitglieder können erkennen, wer für eine bestimmte Ressource verantwortlich ist.
- Konten haben wenn möglich einen festen Verantwortlichen.

Typische Anti-Muster:

- Die alternativen Kontakte für Ihre AWS-Konten sind nicht eingepflegt.
- Die Ressourcen sind nicht mit Tags markiert, die kennzeichnen, wer dafür verantwortlich ist.
- Sie haben eine ITSM-Warteschlange ohne E-Mail-Zuordnung.
- Zwei Teams haben sich überschneidende Verantwortlichkeit für einen wichtigen Teil der Infrastruktur.

Vorteile der Nutzung dieser bewährten Methode:

- Dank der zugewiesenen Verantwortlichkeit ist die Änderungskontrolle ganz einfach.
- Wenn Probleme auftreten, können die richtigen Verantwortlichen einbezogen werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Definieren Sie, was Verantwortlichkeit für die Ressourcen-Anwendungsfälle in Ihrer Umgebung bedeutet. Verantwortlichkeit kann bedeuten, Änderungen an der Ressource zu beaufsichtigen, die Ressource während der Fehlerbehebung zu unterstützen oder die finanzielle Verantwortung zu tragen. Legen Sie Verantwortliche für Ressourcen fest und dokumentieren Sie diese. Die Angaben sollten den Namen, die Kontaktinformationen, die Organisation und das Team beinhalten.

Kundenbeispiel

Bei AnyCompany Retail bezeichnet die Verantwortlichkeit das Team oder die Person, das/die für Änderungen und Support für Ressourcen verantwortlich ist. Das Unternehmen verwendet AWS Organizations für die Verwaltung seiner AWS-Konten. Die alternativen Kontakte für die Konten werden mit Gruppenpostfächern konfiguriert. Jede ITSM-Warteschlange ist einem E-Mail-Alias zugeordnet. Tags kennzeichnen, wer für AWS-Ressourcen verantwortlich ist. Für andere Plattformen und Infrastruktur gibt es eine Wiki-Seite, auf der die Verantwortlichkeiten und die Kontaktinformationen angegeben sind.

Implementierungsschritte

1. Beginnen Sie damit, die Verantwortlichkeiten für Ihre Organisation zu definieren. Verantwortlichkeit kann bedeuten, wer für das Risiko für die Ressource oder für Änderungen an der Ressource verantwortlich ist oder wer die Ressource im Fall einer Fehlerbehebung unterstützt. Verantwortlichkeit kann auch die finanzielle oder administrative Verantwortlichkeit für die Ressource umfassen.
2. Verwenden Sie AWS Organizations zum Verwalten der Konten. Sie können die alternativen Kontakte für Ihre Konten zentral verwalten.
   a. Durch die Verwendung von E-Mail-Adressen und Telefonnummern des Unternehmens als Kontaktdaten können Sie auch dann auf sie zugreifen, wenn die Personen, zu denen sie gehören, nicht mehr Teil Ihrer Organisation sind. Erstellen Sie beispielsweise separate E-Mail-Verteilerlisten für die Abrechnung, die Produktion und die Sicherheit und konfigurieren Sie sie in jedem aktiven AWS-Konto als Abrechnungs-, Sicherheits- und Produktionskontakte. Mehrere Personen erhalten AWS-Benachrichtigungen und können auch dann reagieren, wenn jemand im Urlaub ist, die Rolle wechselt oder das Unternehmen verlässt.
   b. Wenn ein Konto nicht von AWS Organizations verwaltet wird, tragen die alternativen Kontakte für Konten dazu bei, dass AWS nötigenfalls mit den richtigen Mitarbeitern in Kontakt treten kann. Konfigurieren Sie die alternativen Kontakte für ein Konto so, dass sie auf eine Gruppe verweisen, und nicht auf eine Einzelperson.

3. Verwenden Sie Tags, um die Verantwortlichen für AWS-Ressourcen zu kennzeichnen. Sie können die Verantwortlichen und ihre Kontaktdaten in verschiedenen Tags angeben.
   a. Mit Regeln in AWS Config können Sie erzwingen, dass die Ressourcen die erforderlichen Tags zur Verantwortlichkeit aufweisen.
   b. Ausführliche Anleitungen zur Entwicklung einer Tagging-Strategie für Ihre Organisation finden Sie im AWS-Whitepaper „Bewährte Methoden für das Tagging“.
4. Verwenden Sie Amazon Q Business, einen Gesprächsassistenten, der generative KI nutzt, um die Produktivität der Belegschaft zu steigern, Fragen zu beantworten und Aufgaben basierend auf Informationen in Ihren Unternehmenssystemen zu erledigen.
   a. Verbinden Sie Amazon Q Business mit der Datenquelle Ihres Unternehmens. Amazon Q Business bietet vorgefertigte Konnektoren zu über 40 unterstützten Datenquellen, darunter Amazon Simple Storage Service (Amazon S3), Microsoft SharePoint, Salesforce und Atlassian Confluence. Weitere Informationen finden Sie unter Amazon Q Business-Konnektoren.
5. Erstellen Sie für andere Ressourcen, Plattformen und Infrastruktur eine Dokumentation mit Informationen zur jeweiligen Verantwortlichkeit. Diese sollte für alle Teammitglieder zugänglich sein.

Aufwand des Implementierungsplans: niedrig. Nutzen Sie die Kontaktinformationen zum Konto sowie Tags, um die Verantwortlichkeit für AWS-Ressourcen zuzuweisen. Für andere Ressourcen können Sie beispielsweise eine einfache Tabelle in einem Wiki verwenden, um die Verantwortlichkeit und Kontaktinformationen zu erfassen, oder nutzen Sie ein ITSM-Tool, um die Verantwortlichkeit zuzuordnen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer
- OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Zuständigkeiten

Zugehörige Dokumente:

- AWS-Account Management – Aktualisieren der Kontaktinformationen
- AWS Organizations – Aktualisieren alternativer Kontakte in Ihrer Organisation
- Bewährte Methoden für das Tagging von AWS – Whitepaper

- Erstellung privater und sicherer Apps mit generativer KI für Unternehmen mit Amazon Q Business und AWS IAM Identity Center
- Amazon Q Business, jetzt allgemein verfügbar, zur Steigerung der Mitarbeiterproduktivität mithilfe generativer KI
- Blog zum Thema AWS Cloud-Operations und -Migrationen – Implementierung automatisierter und zentralisierter Tagging-Kontrollen mit AWS Config und AWS Organizations
- Blog zum Thema AWS-Sicherheit – Erweitern von Pre-Commit-Hooks mit AWS CloudFormation Guard
- Blog zum Thema AWS DevOps – Integration von AWS CloudFormation Guard in CI/CD-Pipelines

Zugehörige Workshops:

- AWS-Workshop – Tagging

Zugehörige Beispiele:

- AWS-Config-Regeln – Amazon EC2 mit erforderlichen Tags und gültigen Werten

Zugehörige Services:

- AWS-Config-Regeln – erforderliche Tags
- AWS Organizations

OPS02-BP02 Prozesse und Verfahren haben feste Besitzer

Verschaffen Sie sich einen Überblick darüber, wer für die Definition einzelner Prozesse und Verfahren zuständig ist, warum diese spezifischen Prozesse und Verfahren verwendet werden und warum diese Zuständigkeit besteht. Wenn Sie wissen, warum bestimmte Prozesse und Verfahren verwendet werden, können Sie Verbesserungsmöglichkeiten identifizieren.

Gewünschtes Ergebnis: Ihre Organisation verfügt über gut definierte und verwaltete Prozesse und Verfahren für betriebliche Aufgaben. Der Prozess und die Verfahren werden an einem zentralen Ort gespeichert und stehen Ihren Teammitgliedern zur Verfügung. Prozesse und Verfahren werden regelmäßig aktualisiert, wobei die Zuständigkeit eindeutig zugewiesen wird. Wo möglich, werden Skripte, Vorlagen und Automatisierungsdokumente als Code implementiert.

Typische Anti-Muster:

- Prozesse sind nicht dokumentiert. Es können fragmentierte Skripte auf isolierten Bedienerarbeitsplätzen existieren.
- Das Wissen über den Umgang mit Skripten wird von wenigen Personen oder informell als Teamwissen vermittelt.
- Ein veralteter Prozess muss aktualisiert werden, aber die Zuständigkeit für die Aktualisierung ist unklar, und der ursprüngliche Autor gehört nicht mehr zur Organisation.
- Prozesse und Skripte sind nicht auffindbar und daher nicht sofort verfügbar, wenn sie benötigt werden (z. B. als Reaktion auf einen Vorfall).

Vorteile der Nutzung dieser bewährten Methode:

- Prozesse und Verfahren unterstützen Sie bei der Bewältigung Ihrer Workloads.
- Neue Teammitglieder werden schneller handlungsfähig.
- Die Zeit bis zur Behebung von Vorfällen wird reduziert.
- Verschiedene Teammitglieder (und Teams) können dieselben Prozesse und Verfahren auf einheitliche Weise verwenden.
- Teams können ihre Prozesse durch wiederholbare Prozesse skalieren.
- Standardisierte Prozesse und Verfahren tragen dazu bei, die Auswirkungen der Übertragung von Workload-Verantwortlichkeiten zwischen Teams abzumildern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

- Prozesse und Verfahren haben feste Besitzer, die für ihre Definition verantwortlich sind.
  - Identifizieren Sie die Betriebsaktivitäten, die zur Unterstützung Ihrer Workloads durchgeführt werden. Dokumentieren Sie diese Aktivitäten an einem auffindbaren Ort.
  - Legen Sie die Person oder Personen fest, die für die Spezifikation einer Aktivität verantwortlich sind. Sie sind dafür verantwortlich, sicherzustellen, dass die Aktivität von einem ausreichend qualifizierten Teammitglied durchgeführt wird, das die entsprechenden Berechtigungen, Zugriffsrechte und Tools hat. Wenn bei der Durchführung dieser Aktivität Probleme auftreten, sind die zuständigen Teammitglieder dafür zuständig, detailliertes Feedback bereitzustellen, damit die Aktivität verbessert werden kann.

  - Erfassen Sie die Zuständigkeit in den Metadaten des Aktivitätsartefakts durch Services wie AWS Systems Manager, durch Dokumente und AWS Lambda. Erfassen Sie die Ressourcenzuständigkeit mithilfe von Tags oder Ressourcengruppen und geben Sie Zuständigkeits- und Kontaktinformationen an. Verwenden Sie AWS Organizations, um Markierungsrichtlinien zu erstellen sowie Zuständigkeits- und Kontaktinformationen zu erfassen.
- Mit der Zeit sollten diese Verfahren so weiterentwickelt werden, dass sie als Code ausgeführt werden können, damit weniger menschliche Eingriffe erforderlich sind.
  - Erwägen Sie beispielsweise AWS Lambda-Funktionen, CloudFormation-Vorlagen oder AWS Systems Manager-Automatisierungsdokumente.
  - Führen Sie die Versionskontrolle in den entsprechenden Repositorys durch.
  - Fügen Sie geeignetes Ressourcen-Tagging hinzu, damit Eigentümer und Dokumentation leicht identifiziert werden können.

Kundenbeispiel

AnyCompany Retail legt fest, dass das Team oder die Person, die für die Prozesse einer Anwendung oder einer Gruppe von Anwendungen (die gemeinsame architektonische Praktiken und Technologien nutzen) zuständig ist, der Besitzer ist. Zunächst werden der Prozess und die Verfahren in Form von schrittweisen Anleitungen im Dokumentenverwaltungssystem dokumentiert, die über Tags für das AWS-Konto, das die Anwendung hostet, und für bestimmte Ressourcengruppen innerhalb des Kontos auffindbar sind. Das Unternehmen verwendet AWS Organizations für die Verwaltung seiner AWS-Konten. Im Laufe der Zeit werden diese Prozesse in Code umgewandelt und Ressourcen werden mithilfe von Infrastructure as Code (z. B. CloudFormation oder AWS Cloud Development Kit (AWS CDK)-Vorlagen) definiert. Die Betriebsprozesse werden zu Automatisierungsdokumenten in AWS Systems Manager- oder AWS Lambda-Funktionen, die als geplante Aufgaben, als Reaktion auf Ereignisse wie AWS CloudWatch-Alarme oder AWS EventBridge-Ereignisse oder durch Anfragen innerhalb einer IT-Servicemanagement-Plattform (ITSM) gestartet werden können. Alle Prozesse sind mit Tags versehen, um die Zuständigkeit zu identifizieren. Die Dokumentation für die Automatisierung und den Prozess wird auf den Wiki-Seiten verwaltet, die vom Code-Repository für den Prozess generiert werden.

Implementierungsschritte

1. Dokumentieren Sie die bestehenden Prozesse und Verfahren.
   a. Überprüfen Sie sie und halten Sie sie auf dem neuesten Stand.
   b. Identifizieren Sie einen Besitzer für jeden Prozess und jede Prozedur.

   c. Stellen Sie sie unter Versionskontrolle.
   d. Wenn möglich, nutzen Sie Prozesse und Verfahren für Workloads und Umgebungen mit gemeinsamen Architekturentwürfen.
2. Richten Sie Mechanismen für Feedback und Verbesserung ein.
   a. Definieren Sie Richtlinien dafür, wie oft Prozesse überprüft werden sollten.
   b. Definieren Sie Prozesse für Prüfende und Genehmigende.
   c. Implementieren Sie Probleme oder eine Ticket-Warteschlange, um Feedback zu geben und zu verfolgen.
   d. Wo immer es möglich ist, sollten Prozesse und Verfahren vorab von einem Gremium zur Genehmigung von Änderungen genehmigt und in eine Risikoklasse eingestuft werden.
3. Stellen Sie sicher, dass Prozesse und Verfahren für diejenigen, die sie ausführen müssen, zugänglich und auffindbar sind.
   a. Verwenden Sie Tags, um anzugeben, wo der Prozess und die Verfahren für den Workload aufgerufen werden können.
   b. Verwenden Sie aussagekräftige Fehler- und Ereignismeldungen, um die geeigneten Prozesse oder Verfahren zur Behebung eines Problems anzugeben.
   c. Verwenden Sie Wikis und Dokumentenmanagement und machen Sie Prozesse und Verfahren organisationsweit durchsuchbar.
4. Automatisieren Sie gegebenenfalls.
   a. Automatisierungen sollten entwickelt werden, wenn Services und Technologien eine API bereitstellen.
   b. Informieren Sie angemessen über Prozesse. Entwickeln Sie die Benutzerszenarien und Anforderungen, um diese Prozesse zu automatisieren.
   c. Messen Sie die erfolgreiche Nutzung Ihrer Prozesse und Verfahren und geben Sie dabei Probleme an, die eine iterative Verbesserung unterstützen.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP01 Ressourcen haben feste Verantwortliche
- OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Zuständigkeiten

- OPS11-BP04 Wissensmanagement

Zugehörige Dokumente:

- AWS Whitepaper – Einführung in DevOps in AWS
- AWS-Whitepaper – Bewährte Methoden für das Tagging von AWS-Ressourcen
- AWS-Whitepaper – Organisieren der AWS-Umgebung mithilfe mehrerer Konten
- Blog zum Thema AWS Cloud-Betrieb und -Migrationen – Entwicklung eines Cloud-Automatisierungsverfahrens für Operational Excellence: Bewährte Methoden von AWS Managed Services
- Blog zum Thema AWS Cloud-Operations und -Migrationen – Implementierung automatisierter und zentralisierter Tagging-Kontrollen mit AWS Config und AWS Organizations
- Blog zum Thema AWS-Sicherheit – Erweitern von Pre-Commit-Hooks mit AWS CloudFormation Guard
- Blog zum Thema AWS DevOps – Integration von AWS CloudFormation Guard in CI/CD-Pipelines

Zugehörige Workshops:

- Workshop zum Thema AWS Well-Architected Operational Excellence
- AWS-Workshop – Tagging

Zugehörige Videos:

- Automatisierung von IT-Abläufen in AWS
- AWS re:Invent 2020 – Automatisierung mit AWS Systems Manager
- AWS re:Inforce 2022 – Automatisierung der Patch-Verwaltung und -Compliance mit AWS (NIS306)
- Unterstützung durch AWS – Vertiefung in AWS Systems Manager

Zugehörige Services:

- AWS Systems Manager – Automatisierung
- AWS Service Management Connector

OPS02-BP03 Betriebsaktivitäten haben feste Besitzer, die für ihre Leistung verantwortlich sind

Verschaffen Sie sich einen Überblick darüber, wer für spezifische Aktivitäten in festgelegten Workloads verantwortlich ist und warum diese Zuständigkeit besteht. Wenn Sie wissen, wer für die Durchführung von Aktivitäten verantwortlich ist, können Sie nachvollziehen, wer die Aktivität durchführen, das Ergebnis validieren und dem Besitzer der Aktivität Feedback geben wird.

Gewünschtes Ergebnis:

Ihre Organisation definiert klar die Verantwortlichkeiten, um bestimmte Aktivitäten anhand definierter Workloads durchzuführen und auf Ereignisse zu reagieren, die durch die Workloads verursacht werden. Die Organisation dokumentiert die Zuständigkeit für Prozesse und deren Erfüllung und macht diese Informationen auffindbar. Sie überprüfen und aktualisieren die Zuständigkeiten, wenn organisatorische Änderungen stattfinden, und die Teams verfolgen und messen die Leistung der Aktivitäten zur Identifizierung von Fehlern und Ineffizienzen. Sie implementieren Feedback-Mechanismen, um Fehler und Verbesserungen nachzuverfolgen und iterative Verbesserungen zu unterstützen.

Typische Anti-Muster:

- Sie dokumentieren keine Verantwortlichkeiten.
- Fragmentierte Skripte existieren auf isolierten Bedienerarbeitsplätzen. Nur wenige Personen wissen, wie man sie benutzt, oder bezeichnen sie informell als Teamwissen.
- Ein veralteter Prozess muss aktualisiert werden, aber niemand weiß, wer für den Prozess zuständig ist, und der ursprüngliche Autor gehört nicht mehr zur Organisation.
- Prozesse und Skripte sind nicht auffindbar und nicht sofort verfügbar, wenn sie benötigt werden (z. B. als Reaktion auf einen Vorfall).

Vorteile der Nutzung dieser bewährten Methode:

- Sie wissen, wer die verantwortliche Person für die Durchführung einer Aktivität ist, wer benachrichtigt werden muss, wenn eine Aktion erforderlich ist, und wer die Aktion ausführen, das Ergebnis validieren und dem Besitzer der Aktivität Feedback geben wird.
- Prozesse und Verfahren unterstützen Sie bei der Bewältigung Ihrer Workloads.
- Neue Teammitglieder werden schneller handlungsfähig.
- Sie reduzieren die Zeit, die zur Behebung von Vorfällen benötigt wird.

- Verschiedene Teams verwenden dieselben Prozesse und Verfahren, um Aufgaben auf einheitliche Weise auszuführen.
- Teams können ihre Prozesse durch wiederholbare Prozesse skalieren.
- Standardisierte Prozesse und Verfahren tragen dazu bei, die Auswirkungen der Übertragung von Workload-Verantwortlichkeiten zwischen Teams abzumildern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Um mit der Definition von Verantwortlichkeiten zu beginnen, beginnen Sie mit der vorhandenen Dokumentation, wie Zuständigkeitsmatrizen, Prozessen und Verfahren, Rollen und Verantwortlichkeiten sowie Tools und Automatisierung. Überprüfen und besprechen Sie die Verantwortlichkeiten für dokumentierte Prozesse. Ermitteln Sie gemeinsam mit den Teams, ob Abweichungen zwischen den Dokumenten zu Zuständigkeiten und Prozessen vorliegen. Besprechen Sie die angebotenen Dienstleistungen mit internen Kunden dieses Teams, um unterschiedliche Erwartungen zwischen den Teams zu identifizieren.

Analysieren und beheben Sie die Diskrepanzen. Identifizieren Sie Verbesserungsmöglichkeiten und suchen Sie nach häufig nachgefragten, ressourcenintensiven Aktivitäten, bei denen es sich in der Regel um gute Kandidaten für Verbesserungen handelt. Informieren Sie sich über bewährte Methoden, Muster und präskriptive Anleitungen, um Verbesserungen zu vereinfachen und zu standardisieren. Erfassen Sie Verbesserungsmöglichkeiten und verfolgen Sie die Verbesserungen bis zur Fertigstellung.

Mit der Zeit sollten diese Verfahren so weiterentwickelt werden, dass sie als Code ausgeführt werden, sodass weniger menschliche Eingriffe erforderlich sind. Beispielsweise können Verfahren als AWS Lambda-Funktionen, AWS CloudFormation-Vorlagen oder AWS Systems Manager-Automatisierungsdokumente initiiert werden. Stellen Sie sicher, dass diese Verfahren in den entsprechenden Repositorys versionskontrolliert sind und ein geeignetes Ressourcen-Tagging enthalten, sodass die Teams die Eigentümer und die Dokumentation leicht identifizieren können. Dokumentieren Sie die Verantwortung für die Durchführung der Aktivitäten und überwachen Sie dann die Automatisierungen, um sicherzustellen, dass sie erfolgreich initiiert und ausgeführt werden und dass die gewünschten Ergebnisse erzielt werden.

Kundenbeispiel

AnyCompany Retail legt fest, dass das Team oder die Person, die für die Prozesse einer Anwendung oder einer Gruppe von Anwendungen (die gemeinsame architektonische Praktiken und Technologien

nutzen) zuständig ist, der Besitzer ist. Zunächst dokumentiert das Unternehmen die Prozesse und Verfahren als schrittweise Anleitungen im Dokumentenmanagementsystem. Es macht die Verfahren mithilfe von Tags auf dem AWS-Konto, das die Anwendung hostet, und anhand bestimmter Gruppen von Ressourcen innerhalb des Kontos auffindbar und verwendet AWS Organizations zur Verwaltung der AWS-Konten. Im Laufe der Zeit konvertiert AnyCompany Retail diese Prozesse in Code und definiert Ressourcen mithilfe von Infrastructure as Code (über Services wie CloudFormation oder AWS Cloud Development Kit (AWS CDK)-Vorlagen). Die Betriebsprozesse werden zu Automatisierungsdokumenten in AWS Systems Manager- oder AWS Lambda-Funktionen, die als geplante Aufgaben als Reaktion auf Ereignisse wie Amazon CloudWatch-Alarme oder Amazon EventBridge-Ereignisse oder durch Anfragen innerhalb einer IT-Servicemanagement-Plattform (ITSM) gestartet werden können. Alle Prozesse sind mit Tags versehen, um die Zuständigkeit zu identifizieren. Teams verwalten die Dokumentation für die Automatisierung und den Prozess auf den Wiki-Seiten, die vom Code-Repository für den Prozess generiert werden.

Implementierungsschritte

1. Dokumentieren Sie die bestehenden Prozesse und Verfahren.
    a. Überprüfen und vergewissern Sie sich, dass sie auf dem neuesten Stand sind.
    b. Stellen Sie sicher, dass jeder Prozess oder jedes Verfahren einen Besitzer hat.
    c. Stellen Sie die Verfahren unter Versionskontrolle.
    d. Wenn möglich, nutzen Sie Prozesse und Verfahren für Workloads und Umgebungen mit gemeinsamen Architekturentwürfen.
2. Richten Sie Mechanismen für Feedback und Verbesserung ein.
    a. Definieren Sie Richtlinien dafür, wie oft Prozesse überprüft werden sollten.
    b. Definieren Sie Prozesse für Prüfende und Genehmigende.
    c. Implementieren Sie Probleme oder eine Ticket-Warteschlange, um Feedback zu geben und zu verfolgen.
    d. Wo immer es möglich ist, sollten Prozesse und Verfahren vorab von einem Gremium zur Genehmigung von Änderungen genehmigt und in eine Risikoklasse eingestuft werden.
3. Machen Sie Prozesse und Verfahren für Benutzer zugänglich und auffindbar, die sie ausführen müssen.
    a. Verwenden Sie Tags, um anzugeben, wo der Prozess und die Verfahren für den Workload aufgerufen werden können.
    b. Verwenden Sie aussagekräftige Fehler- und Ereignismeldungen, um die geeigneten Prozesse oder Verfahren zur Behebung des Problems anzugeben.

   c. Verwenden Sie Wikis oder Dokumentenmanagement, um Prozesse und Verfahren unternehmensweit durchsuchbar zu machen.

4. Automatisieren Sie, wenn es angemessen ist.
   a. Entwickeln Sie Automatisierungen, wenn Services und Technologien eine API bereitstellen.
   b. Stellen Sie sicher, dass die Prozesse gut verstanden werden, und entwickeln Sie Benutzerberichte und Anforderungen, um diese Prozesse zu automatisieren.
   c. Messen Sie die erfolgreiche Nutzung der Prozesse und Verfahren und unterstützen Sie eine iterative Verbesserung anhand der Problemverfolgung.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP01 Ressourcen haben feste Verantwortliche
- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer
- OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Zuständigkeiten
- OPS02-BP05 Mechanismen zur Identifizierung von Verantwortlichkeiten und Eigentümerschaft sind vorhanden
- OPS11-BP04 Wissensmanagement

Zugehörige Dokumente:

- AWS Whitepaper | Einführung in DevOps in AWS
- AWSWhitepaper | Bewährte Methoden für das Tagging von AWS-Ressourcen
- AWS-Whitepaper | Organisation der AWS-Umgebung mithilfe mehrerer Konten
- Blog zum Thema AWS Cloud-Betrieb und -Migrationen | Entwicklung eines Cloud-Automatisierungsverfahrens für Operational Excellence: Bewährte Methoden von AWS Managed Services
- AWS-Workshop – Tagging
- AWS Service Management Connector

Zugehörige Videos:

- AWS Knowledge Center Live | Tagging von AWS-Ressourcen
- AWS re:Invent 2020 | Automatisierung mit AWS Systems Manager
- AWS re:Inforce 2022 | Automatisierung der Patch-Verwaltung und -Compliance mit AWS (NIS306)
- Unterstützung durch AWS | Vertiefung in AWS Systems Manager

Zugehörige Beispiele:

- Workshop zum Thema AWS Well-Architected Operational Excellence

OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Zuständigkeiten

Verstehen Sie die die Verantwortlichkeiten Ihrer Rolle und, wie Sie zu Geschäftsergebnissen beitragen, da Ihnen dieses Wissen ermöglicht, Ihre Aufgaben entsprechend zu priorisieren und die Bedeutung Ihrer Rolle nachzuvollziehen. Auf diese Weise können Teammitglieder Anforderungen erkennen und entsprechend reagieren. Wenn die Teammitglieder ihre Rolle kennen, können sie Verantwortung übernehmen, Verbesserungsmöglichkeiten erkennen und verstehen, wie sie Einfluss nehmen oder entsprechende Änderungen vornehmen können.

Gelegentlich kann es vorkommen, dass eine Verantwortlichkeit keinen eindeutigen Besitzer hat. Entwerfen Sie in diesen Situationen einen Mechanismus, um diese Lücke zu schließen. Erstellen Sie einen klar definierten Eskalationspfad zu jemandem, der die Befugnis hat, die Verantwortung zu übertragen, oder entwickeln Sie einen Plan zur Deckung des Bedarfs.

Gewünschtes Ergebnis: Die Teams in Ihrer Organisation haben klar definierte Verantwortlichkeiten, was auch umfasst, wie sie mit Ressourcen, auszuführenden Maßnahmen, Prozessen und Verfahren zusammenhängen. Diese Verantwortlichkeiten entsprechen den Verantwortlichkeiten und Zielen des Teams sowie den Verantwortlichkeiten anderer Teams. Sie dokumentieren die Eskalationswege auf konsistente und nachvollziehbare Weise und nehmen diese Entscheidungen in Dokumentationsartefakte wie Zuständigkeitsmatrizen, Teamdefinitionen oder Wiki-Seiten auf.

Typische Anti-Muster:

- Die Verantwortlichkeiten des Teams sind mehrdeutig oder schlecht definiert.
- Das Team stimmt Rollen nicht mit Verantwortlichkeiten ab.
- Das Team stimmt seine Ziele und Verantwortlichkeiten nicht aufeinander ab, was es schwierig macht, den Erfolg zu messen.

- Die Verantwortlichkeiten der Teammitglieder sind nicht am Team und der gesamten Organisation ausgerichtet.
- Ihr Team hält die Verantwortlichkeiten nicht auf dem neuesten Stand, was dazu führt, dass sie nicht mit den vom Team ausgeführten Aufgaben übereinstimmen.
- Eskalationswege zur Festlegung von Zuständigkeiten sind nicht definiert oder unklar.
- Eskalationspfade haben keinen eindeutigen Besitzer, um eine zeitnahe Reaktion zu gewährleisten.
- Rollen, Zuständigkeiten und Eskalationswege sind nicht auffindbar und bei Bedarf nicht sofort verfügbar (z. B. als Reaktion auf einen Vorfall).

Vorteile der Nutzung dieser bewährten Methode:

- Wenn Sie wissen, wer verantwortlich oder zuständig ist, können Sie sich an das entsprechende Team oder Teammitglied wenden, um eine Anfrage zu stellen oder eine Aufgabe zu übergeben.
- Um das Risiko von Untätigkeit und ungedecktem Bedarf zu verringern, haben Sie eine Person festgelegt, die befugt ist, Verantwortung und Zuständigkeit zu übertragen.
- Wenn Sie den Umfang einer Verantwortlichkeit klar definieren, gewinnen Ihre Teammitglieder an Autonomie und Eigenverantwortung.
- Ihre Verantwortlichkeiten wirken sich auf Ihre Entscheidungen, Ihre Aktionen und die Übergabe von Aktivitäten an die ordnungsgemäßen Besitzer aus.
- Es ist einfach, aufgegebene Verantwortlichkeiten zu identifizieren, da Sie genau wissen, was außerhalb der Verantwortung Ihres Teams liegt, was die Eskalation zur Aufklärung erleichtert.
- Es kommt innerhalb der Teams zu weniger Verwirrung und Spannungen und sie können ihre Workloads und Ressourcen besser verwalten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Legen Sie die Rollen und Verantwortlichkeiten von Teammitgliedern fest und vergewissern Sie sich, dass sie die Anforderungen ihrer Rolle kennen. Diese Informationen sollten leicht auffindbar sein, damit Mitglieder Ihrer Organisation herausfinden können, an wen sie sich für bestimmte Anforderungen wenden müssen (an ein Team oder eine Person). In dem Bestreben, die Chancen der Migration und Modernisierung auf AWS zu nutzen, können sich auch die Rollen und Verantwortlichkeiten ändern. Sorgen Sie dafür, dass sich Ihre Teams und ihre Mitglieder ihrer

Verantwortlichkeiten bewusst sind, und schulen Sie sie angemessen, damit sie ihre Aufgaben während dieser Veränderung erfüllen.

Legen Sie fest, an welche Rolle oder welches Team eskaliert werden soll, um die Verantwortlichkeit und Zuständigkeit zu bestimmen. Dieses Team kann mit verschiedenen Stakeholdern zusammenarbeiten, um eine Entscheidung zu treffen. Es sollte jedoch die Verantwortung für die Verwaltung des Entscheidungsprozesses tragen.

Stellen Sie Mitgliedern Ihrer Organisation zugängliche Mechanismen bereit, um Zuständigkeiten und Verantwortlichkeiten zu ermitteln und zuzuordnen. Diese Mechanismen vermitteln ihnen, an wen sie sich bei spezifischen Bedürfnissen wenden können.

Kundenbeispiel

AnyCompany Retail hat kürzlich eine Migration von Workloads von einer On-Premises-Umgebung zu ihrer Landing Zone in AWS mit einem Lift-and-Shift-Ansatz durchgeführt. Das Unternehmen führte eine Betriebsüberprüfung durch, um festzustellen, wie allgemeine betriebliche Aufgaben erfüllt werden, und verifizierte, dass seine bestehende Verantwortungsmatrix die Abläufe in der neuen Umgebung widerspiegelt. Bei der Migration von On-Premise zu AWS reduzierte es die Verantwortlichkeiten der Infrastrukturteams in Bezug auf die Hardware und die physische Infrastruktur. Dieser Schritt eröffnete auch neue Möglichkeiten, das Betriebsmodell für seine Workloads weiterzuentwickeln.

Es identifizierte, adressierte und dokumentierte die meisten Verantwortlichkeiten, definierte aber auch Eskalationswege für alle Verantwortlichkeiten, die übersehen wurden oder die sich im Zuge der Weiterentwicklung der betrieblichen Abläufe möglicherweise ändern müssen. Um neue Möglichkeiten zur Standardisierung und Effizienzsteigerung Ihrer Workloads zu erkunden, bieten Sie Zugriff auf Betriebstools wie AWS Systems Manager und Sicherheitstools wie AWS Security Hub und Amazon GuardDuty. AnyCompany Retail überprüft die Verantwortlichkeiten und die Strategie auf der Grundlage der Verbesserungen, die zuerst angegangen werden sollen. Wenn das Unternehmen neue Arbeitsweisen und Technologiemuster einführt, passt es seine Verantwortungsmatrix entsprechend an.

Implementierungsschritte

1. Beginnen Sie mit der vorhandenen Dokumentation. Zu den typischen Quelldokumenten gehören möglicherweise:
   a. Verantwortungs- oder RACI-Matrizen (Responsible, Accountable, Consulted, Informed)
   b. Teamdefinitionen oder Wiki-Seiten

   c. Servicedefinitionen und Angebote
   d. Rollen- oder Stellenbeschreibungen
2. Überprüfen und besprechen Sie die dokumentierten Verantwortlichkeiten:
   a. Führen Sie Besprechungen mit den Teams durch, um Abweichungen zwischen den dokumentierten Verantwortlichkeiten und den vom Team üblicherweise wahrgenommenen Verantwortlichkeiten zu identifizieren.
   b. Erörtern Sie mögliche Services, die von internen Kunden angeboten werden, um unterschiedliche Erwartungen zwischen den Teams zu identifizieren.
3. Analysieren und beheben Sie die Diskrepanzen.
4. Identifizieren Sie Verbesserungsmöglichkeiten.
   a. Identifizieren Sie häufig nachgefragte, ressourcenintensive Anfragen, bei denen es sich in der Regel um gute Verbesserungsmöglichkeiten handelt.
   b. Informieren Sie sich über bewährte Methoden, Muster und präskriptive Anleitungen und vereinfachen und standardisieren Sie Verbesserungen anhand dieser Anleitungen.
   c. Erfassen Sie Verbesserungsmöglichkeiten und verfolgen Sie sie bis zur Fertigstellung.
5. Wenn ein Team noch nicht die Verantwortung für die Verwaltung und die Verfolgung der Zuweisung von Verantwortlichkeiten trägt, benennen Sie jemanden im Team, der diese Verantwortung übernimmt.
6. Definieren Sie einen Prozess, nach dem Teams eine Klärung der Verantwortlichkeiten anfordern können.
   a. Überprüfen Sie den Prozess und stellen Sie sicher, dass er klar und einfach umzusetzen ist.
   b. Stellen Sie sicher, dass jemand die Verantwortung für die Eskalationen trägt und sie bis zu ihrem Ende verfolgt.
   c. Legen Sie betriebliche Metriken fest, um die Effektivität zu messen.
   d. Schaffen Sie Feedback-Mechanismen, um sicherzustellen, dass Teams Verbesserungsmöglichkeiten hervorheben können.
   e. Implementieren Sie einen Mechanismus für die regelmäßige Überprüfung.
7. Führen Sie Dokumente an einem auffindbaren und zugänglichen Ort.
   a. Wikis oder das Dokumentationsportal sind gängige Optionen.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP06 Bewerten von Kompromissen
- OPS03-BP02 Teammitglieder sind befugt, Maßnahmen zu ergreifen, wenn Ergebnisse gefährdet sind
- OPS03-BP03 Eskalation wird empfohlen
- OPS03-BP07 Teams mit entsprechenden Ressourcen ausstatten
- OPS09-BP01 Messen operativer Ziele und KPIs mit Metriken
- OPS09-BP03 Überprüfen der Betriebsmetriken und Priorisieren von Verbesserungen
- OPS11-BP01 Implementieren eines Prozesses für die kontinuierliche Verbesserung

Zugehörige Dokumente:

- AWS Whitepaper – Einführung in DevOps in AWS
- AWS Whitepaper – AWS Cloud Adoption Framework: Die betriebliche Perspektive
- AWS Well-Architected Framework Operational Excellence – Betriebsmodelltopologien auf Workload-Ebene
- AWS Prescriptive Guidance – Entwicklung Ihres Cloud-Betriebsmodells
- AWS Prescriptive Guidance – Erstellung einer RACI- oder RASCI-Matrix für ein Cloud-Betriebsmodell
- Blog zum Thema AWS Cloud-Betrieb und Migration – Unternehmenswert mit Cloud-Plattform-Teams
- Blog zum Thema AWS Cloud-Betrieb und Migration – Warum ein Cloud-Betriebsmodell?
- Blog zum Thema AWS DevOps – So modernisieren sich Organisationen für den Cloud-Betrieb

Zugehörige Videos:

- AWS Summit Online – Cloud-Betriebsmodelle für eine beschleunigte Transformation
- AWS re:Invent 2023 – Zukunftssichere Cloud-Sicherheit: Ein neues Betriebsmodell

OPS02-BP05 Mechanismen zum Anfordern von Ergänzungen, Änderungen und Ausnahmen sind vorhanden

Sie können Anfragen an Verantwortliche für Prozesse, Verfahren und Ressourcen stellen. Die Anfragen umfassen Ergänzungen, Änderungen und Ausnahmen. Diese Anfragen durchlaufen einen Änderungsverwaltungsprozess. Treffen Sie fundierte Entscheidungen, um angemessene Anfragen nach einer Bewertung der Vorteile und Risiken zu genehmigen.

Gewünschtes Ergebnis:

- Sie können Anfragen zum Ändern von Prozessen, Verfahren und Ressourcen basierend auf der zugewiesenen Verantwortlichkeit stellen.
- Änderungen werden nach einem sorgfältigen Abwägen der Vorteile und Risiken vorgenommen.

Typische Anti-Muster:

- Sie müssen die Art und Weise der Bereitstellung Ihrer Anwendung aktualisieren, es gibt jedoch keine Möglichkeit, eine Änderung am Bereitstellungsprozess beim Produktionsteam zu beantragen.
- Der Notfallwiederherstellungsplan muss aktualisiert werden, es ist jedoch kein Verantwortlicher kenntlich gemacht, an den Anträge auf Änderungen übermittelt werden können.

Vorteile der Nutzung dieser bewährten Methode:

- Prozesse, Verfahren und Ressourcen können sich weiterentwickeln, wenn sich die Anforderungen ändern.
- Die Verantwortlichen können fundierte Entscheidungen treffen, wann Änderungen vorgenommen werden sollten.
- Änderungen werden nach sorgfältigen Überlegungen vorgenommen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Um diese bewährte Methode zu implementieren, müssen Sie Änderungen an Prozessen, Verfahren und Ressourcen beantragen können. Der Änderungsverwaltungsprozess kann einfach sein. Dokumentieren Sie den Änderungsverwaltungsprozess.

Kundenbeispiel

AnyCompany Retail verwendet für die Angabe, wer für Änderungen an Prozessen, Verfahren und Ressourcen verantwortlich ist, eine Verantwortlichkeitsmatrix (RACI). Es gibt einen dokumentierten Änderungsverwaltungsprozess, der einfach und leicht zu befolgen ist. Mithilfe der RACI-Matrix und des Prozesses können alle Personen Änderungsanträge übermitteln.

Implementierungsschritte

1. Ermitteln Sie die Prozesse, Verfahren und Ressourcen für Ihren Workload sowie die jeweiligen Verantwortlichen. Dokumentieren Sie sie in Ihrem Wissensmanagementsystem.
   a. Wenn Sie OPS02-BP01 Ressourcen haben feste Verantwortliche, OPS02-BP02 Prozesse und Verfahren haben feste Besitzer oder OPS02-BP03 Betriebsaktivitäten haben feste Besitzer, die für ihre Leistung verantwortlich sind noch nicht implementiert haben, beginnen Sie damit.
2. Arbeiten Sie mit den Stakeholdern in Ihrer Organisation zusammen, um einen Änderungsverwaltungsprozess zu entwickeln. Der Prozess sollte Ergänzungen, Änderungen und Ausnahmen für Ressourcen, Prozesse und Verfahren umfassen.
   a. Sie können AWS Systems Manager Change Manager als Änderungsverwaltungsplattform für Workload-Ressourcen verwenden.
3. Dokumentieren Sie den Änderungsverwaltungsprozess in Ihrem Wissensmanagementsystem.

Aufwand des Implementierungsplans: mittel. Die Entwicklung eines Änderungsverwaltungsprozesses erfordert die Abstimmung mit mehreren Stakeholdern in Ihrer Organisation.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP01 Ressourcen haben feste Verantwortliche – Bevor Sie einen Änderungsverwaltungsprozess entwickeln können, müssen Verantwortliche für die Ressourcen kenntlich gemacht werden.
- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer – Bevor Sie einen Änderungsverwaltungsprozess entwickeln können, müssen Verantwortliche für die Prozesse kenntlich gemacht werden.
- OPS02-BP03 Betriebsaktivitäten haben feste Besitzer, die für ihre Leistung verantwortlich sind – Bevor Sie einen Änderungsverwaltungsprozess entwickeln können, müssen Verantwortliche für die Verfahren kenntlich gemacht werden.

Zugehörige Dokumente:

- AWS Prescriptive Guidance – Grundlagen-Playbook für umfassende AWS-Migrationen: RACI-Matrizen erstellen
- Whitepaper Change Management in the Cloud (Änderungsmanagement in der Cloud)

Zugehörige Services:

- AWS Systems Manager Change Manager

OPS02-BP06 Zuständigkeiten zwischen Teams werden vordefiniert oder ausgehandelt

Es gibt definierte oder ausgehandelte Vereinbarungen zwischen Teams, in denen die Zusammenarbeit und gegenseitige Unterstützung beschrieben wird (z. B. Reaktionszeiten, Service-Level-Ziele oder Service-Level-Agreements). Die Kanäle für die teamübergreifende Kommunikation werden dokumentiert. Wenn bekannt ist, welche Auswirkungen die Arbeit der Teams auf die Geschäftsergebnisse und die Ergebnisse anderer Teams und Organisationen hat, können die Teams ihre Aufgaben priorisieren und entsprechend handeln.

Wenn Verantwortlichkeit und Eigentümerschaft nicht definiert oder unbekannt sind, besteht das Risiko, dass sowohl die erforderlichen Aktivitäten nicht rechtzeitig ausgeführt als auch redundante und potenziell widersprüchliche Anstrengungen unternommen werden, um diese Anforderungen zu erfüllen.

Gewünschtes Ergebnis:

- Es werden Vereinbarungen zur teamübergreifenden Zusammenarbeit oder Unterstützung getroffen und dokumentiert.
- Teams, die zusammenarbeiten oder sich gegenseitig unterstützen, verfügen über definierte Kommunikationskanäle und Erwartungen in Bezug auf die Reaktion.

Typische Anti-Muster:

- Während der Produktion tritt ein Problem auf und zwei separate Teams beginnen unabhängig voneinander mit der Fehlersuche. Aufgrund der getrennten Bemühungen verlängert sich der Ausfall.
- Das Produktionsteam benötigt Unterstützung vom Entwicklungsteam, es gibt jedoch keine Vereinbarung in Bezug auf die Reaktionszeit. Die Anfrage wird zurückgestellt.

Vorteile der Nutzung dieser bewährten Methode:

- Die Teams wissen, wie sie miteinander interagieren und sich gegenseitig unterstützen können.
- Die Erwartungen in Bezug auf die Reaktionszeit sind bekannt.
- Die Kommunikationskanäle sind klar definiert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

Wenn Sie diese bewährte Methode implementieren, bedeutet dies, dass es in Bezug auf die Zusammenarbeit zwischen Teams keine Unklarheiten gibt. Mithilfe von formellen Vereinbarungen wird festgelegt, wie Teams zusammenarbeiten oder sich gegenseitig unterstützen. Die Kanäle für die teamübergreifende Kommunikation werden dokumentiert.

Kundenbeispiel

Das SRE-Team bei AnyCompany Retail hat ein Service-Level-Agreement mit dem Entwicklungsteam abgeschlossen. Wenn das Entwicklungsteam eine Anfrage über das Ticketing-System einreicht, kann es innerhalb von 15 Minuten eine Antwort erwarten. Bei Standortausfällen übernimmt das SRE-Team mit Unterstützung durch das Entwicklungsteam die Leitung der Untersuchung.

Implementierungsschritte

1. Arbeiten Sie zusammen mit den Stakeholdern in Ihrer Organisation und auf Grundlage der Prozesse und Verfahren Vereinbarungen zwischen Teams aus.
   a. Entwickeln Sie für gemeinsame Prozesse oder Verfahren von zwei Teams ein Runbook für die Zusammenarbeit.
   b. Wenn Abhängigkeiten zwischen Teams bestehen, vereinbaren Sie ein SLA für die Reaktionszeit bei Anfragen.
2. Dokumentieren Sie die Verantwortlichkeiten in Ihrem Wissensmanagementsystem.

Aufwand des Implementierungsplans: mittel. Wenn keine Vereinbarungen zwischen Teams vorhanden sind, kann es mühsam sein, eine Vereinbarung mit den Stakeholdern in Ihrer Organisation zu treffen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer – Die Verantwortlichkeit für Prozesse muss kenntlich gemacht werden, bevor Vereinbarungen zwischen Teams getroffen werden.
- OPS02-BP03 Betriebsaktivitäten haben feste Besitzer, die für ihre Leistung verantwortlich sind – Die Verantwortlichkeit für Betriebsaktivitäten muss kenntlich gemacht werden, bevor Vereinbarungen zwischen Teams getroffen werden.

Zugehörige Dokumente:

- AWS Executive Insights – Mit dem Zwei-Pizza-Team Innovationen vorantreiben
- Einführung in DevOps in AWS – Zwei-Pizza-Teams

Unternehmenskultur

Stellen Sie Ihren Teammitgliedern Unterstützung bereit, damit sie effektiver handeln und Ihr Geschäftsergebnis unterstützen können.

Bewährte Methoden

- OPS03-BP01 Förderung durch die Geschäftsführung gewährleisten
- OPS03-BP02 Teammitglieder sind befugt, Maßnahmen zu ergreifen, wenn Ergebnisse gefährdet sind
- OPS03-BP03 Eskalation wird empfohlen
- OPS03-BP04 Die Kommunikation ist zeitnah, klar und umsetzbar
- OPS03-BP05 Experimentieren wird empfohlen
- OPS03-BP06 Teammitglieder werden ermutigt, ihre Fähigkeiten zu pflegen und zu erweitern
- OPS03-BP07 Teams mit entsprechenden Ressourcen ausstatten

OPS03-BP01 Förderung durch die Geschäftsführung gewährleisten

Auf höchster Ebene fungiert die Geschäftsleitung als Executive Sponsor, um Erwartungen klar festzulegen und die Richtung für die Ergebnisse der Organisation vorzugeben sowie den Erfolg zu bewerten. Der Sponsor befürwortet und fördert die Einführung von bewährten Methoden und die Weiterentwicklung der Organisation.

Gewünschtes Ergebnis: Organisationen, die sich bemühen, ihren Cloud-Betrieb einzuführen, zu transformieren und zu optimieren, legen klare Führungs- und Rechenschaftslinien für die

gewünschten Ergebnisse fest. Die Organisation kennt jede Fähigkeit, die es benötigt, um ein neues Ergebnis zu erzielen, und überträgt den Funktionsteams die Verantwortung für die Entwicklung dieser Fähigkeiten. Die Führung gibt diese Richtung aktiv vor, weist Verantwortung zu, übernimmt Verantwortung und definiert die Arbeit. Dadurch können Mitarbeiter in der gesamten Organisation mobilisieren, sich inspiriert fühlen und aktiv auf die gewünschten Ziele hinarbeiten.

Typische Anti-Muster:

- Workload-Besitzer sind aufgefordert, Workloads zu AWS zu migrieren ohne klare Unterstützung oder einen Plan für den Cloud-Betrieb. Dies führt dazu, dass Teams nicht gezielt zusammenarbeiten, um ihre operativen Fähigkeiten zu verbessern und weiterzuentwickeln. Der Mangel an Betriebsstandards mit bewährten Methoden führt dazu, dass die Teams überfordert sind (z. B. durch Überarbeitung der Mitarbeiter, Bereitschaftsdienste und technische Schulden) und die Innovation ins Stocken gerät.
- Es wurde ein neues organisationsweites Ziel gesetzt, eine neue Technologie einzuführen, ohne die Führung, den Sponsor und die Strategie anzugeben. Die Teams interpretieren Ziele unterschiedlich, was zu Verwirrung darüber führt, worauf sie sich konzentrieren sollten, warum sie wichtig sind und wie Auswirkungen gemessen werden sollen. Folglich verliert die Organisation bei der Einführung der Technologie an Dynamik.

Vorteile der Einführung dieser bewährten Methode: Wenn das Konzept der Führung klar kommuniziert und auch Vision, Richtung und Ziele mitgeteilt werden, wissen die Teammitglieder, was von ihnen erwartet wird. Wenn sich die Führungskräfte aktiv einbringen, beginnen Einzelpersonen und Teams, ihre Bemühungen intensiv in dieselbe Richtung zu lenken, um festgelegte Ziele zu erreichen. Dadurch maximiert die Organisation ihre Erfolgsfähigkeit. Wenn Sie den Erfolg evaluieren, können Sie Barrieren besser identifizieren um anschließend von der Führung gezielt ausgeräumt werden können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

- In jeder Phase des Wegs in die Cloud (Migration, Einführung oder Optimierung) erfordert der Erfolg eine aktive Beteiligung auf höchster Führungsebene mit einem leitenden Unterstützer. Der leitende Unterstützer richtet die Denkweise, Fähigkeiten und Arbeitsweisen des Teams an der definierten Strategie aus.
  - Das Warum erläutern: Sorgen Sie für Klarheit und erläutern Sie die Gründe für die Vision und Strategie.

- Erwartungen setzen: Definieren und veröffentlichen Sie Ziele für Ihre Organisationen, einschließlich der Art und Weise, wie Fortschritt und Erfolg gemessen werden.
- Zielerreichung verfolgen: Messen Sie regelmäßig die schrittweise Erreichung von Zielen (nicht nur die Erledigung von Aufgaben). Teilen Sie die Ergebnisse mit, damit geeignete Maßnahmen ergriffen werden können, wenn die Ergebnisse gefährdet sind.
- Erforderliche Ressourcen für die Erreichung Ihrer Ziele bereitstellen: Bringen Sie Mitarbeiter und Teams an einen Tisch, um zusammenzuarbeiten und die richtigen Lösungen zu entwickeln, die zu den angestrebten Ergebnissen führen. Dies reduziert oder beseitigt Reibungspunkte in der Organisation.
- Unterstützen Ihrer Teams: Bleiben Sie mit Ihren Teams in Verbindung, um ihre Leistung im Blick zu behalten und potenzielle externe Negativfaktoren zu erkennen. Identifizieren Sie Hindernisse für den Fortschritt Ihrer Teams. Treten Sie für Ihre Teams ein und beseitigen Sie Hindernisse und unnötige Belastungen. Wenn sich äußere Faktoren negativ auf Ihre Teams auswirken, bewerten Sie die Ziele neu und passen Sie sie entsprechend an.
- Fördern der Übernahme bewährter Methoden: Würdigen Sie bewährte Methoden, die messbare Vorteile bieten, und schenken Sie ihren Entwicklern und Anwendern die gebührende Anerkennung. Ermutigen Sie Ihre Teams zur Annahme dieser Methoden, um die Vorteile zu maximieren.
- Weiterentwicklung Ihrer Teams fördern: Schaffen Sie eine Kultur der kontinuierlichen Verbesserung und lernen Sie proaktiv aus erzielten Fortschritten und Misserfolgen. Fördern Sie Wachstum und Entwicklung sowohl im Persönlichen als auch im Betrieblichen. Entwickeln Sie die Vision und Strategie anhand von Daten und Anekdoten weiter.

Kundenbeispiel

AnyCompany Retail befindet sich inmitten einer Geschäftstransformation mit dem Ziel, das Kundenerlebnis schnell neu zu erfinden, die Produktivität zu steigern und das Wachstum durch generative KI zu beschleunigen.

Implementierungsschritte

1. Ernennen Sie einen einzelnen Verantwortlichen und einen leitenden Unterstützer, der die Transformation leitet und vorantreibt.
2. Definieren Sie klare Geschäftsergebnisse für Ihre Transformation, weisen Sie Verantwortlichkeiten zu und fordern Sie Eigenverantwortung ein. Erteilen Sie der leitenden Führungskraft die Befugnis, wichtige Entscheidungen zu leiten und zu treffen.

3. Stellen Sie sicher, dass Ihre Transformationsstrategie sehr klar ist und vom leitenden Sponsor auf allen Ebenen der Organisation umfassend kommuniziert wird.
   a. Legen Sie klar definierte Geschäftsziele für IT- und Cloud-Initiativen fest.
   b. Dokumentieren Sie wichtige Geschäftsmetriken, um die IT- und Cloud-Transformation voranzutreiben.
   c. Kommunizieren Sie die Vision konsequent an alle Teams und Personen, die für Teile der Strategie verantwortlich sind.
4. Entwickeln Sie Matrizen zur Kommunikationsplanung, die vorgeben, welche Botschaft bestimmten Führungskräften, Managern und einzelnen Mitarbeitern übermittelt werden muss. Legen Sie fest, welche Person oder welches Team diese Nachricht übermitteln soll.
   a. Erfüllen Sie Kommunikationspläne konsistent und zuverlässig.
   b. Setzen und steuern Sie Ihre Erwartungen regelmäßig in persönlichen Meetings.
   c. Nehmen Sie Feedback zur Effektivität der Kommunikation an, passen Sie die Kommunikation an und planen Sie entsprechend.
   d. Planen Sie Kommunikationsveranstaltungen, um die Herausforderungen der Teams proaktiv zur Kenntnis zu nehmen, und richten Sie eine konsistente Feedback-Schleife ein, um den Kurs bei Bedarf zu korrigieren.
5. Beschäftigen Sie sich aktiv mit jeder Initiative aus der Führungsperspektive, um sicherzustellen, dass alle betroffenen Teams die Ergebnisse verstehen, für deren Erreichung sie verantwortlich sind.
6. Bei jedem Status-Meeting sollten die leitenden Unterstützer nach Hindernissen Ausschau halten, etablierte Metriken, Anekdoten oder das Feedback der Teams überprüfen und die Fortschritte bei der Erreichung der Ziele messen.

Aufwand des Implementierungsplans: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS03-BP04 Die Kommunikation ist zeitnah, klar und umsetzbar
- OP11-BP01 Implementieren eines Prozesses für die kontinuierliche Verbesserung
- OPS11-BP07 Prüfung von Betriebsmetriken

Zugehörige Dokumente:

- Entwirren im Unternehmensknäuel: Abstimmung auf höchster Ebene
- Die lebende Transformation: Veränderungen pragmatisch angehen
- Auf dem Weg zu einem zukunftsfähigen Unternehmen
- 7 Fehler, die Sie bei der Einrichtung eines CCOE vermeiden sollten
- Navigation in der Cloud: Wichtige Key Performance Indicators für den Erfolg

Zugehörige Videos:

- AWS re:Invent 2023: Ein Leitfaden für Führungskräfte zur generativen KI: Die Geschichte kennen, die Zukunft gestalten (SEG204)

Zugehörige Beispiele:

- Prosci: Rolle und Bedeutung des leitenden Unterstützers

OPS03-BP02 Teammitglieder sind befugt, Maßnahmen zu ergreifen, wenn Ergebnisse gefährdet sind

Eine von der Führung vermittelte Kultur der Eigenverantwortung führt dazu, dass sich die Mitarbeiter bestärkt fühlen, im Namen des gesamten Unternehmens über ihren definierten Rollen- und Verantwortungsbereich hinaus zu handeln. Die Mitarbeiter können handeln, um auftretende Risiken proaktiv zu erkennen und geeignete Maßnahmen ergreifen. Eine solche Kultur ermöglicht es den Mitarbeitern, die Situation zu überblicken und wichtige Entscheidungen zu treffen.

Amazon verwendet beispielsweise die Führungsprinzipien als Leitlinie, um bei den Mitarbeitern erwünschte Verhaltensweisen zu fördern, damit sie verschiedene Situationen bewältigen, Probleme und Konflikte lösen und geeignete Maßnahmen ergreifen können.

Gewünschtes Ergebnis: Die Führung hat eine neue Kultur geprägt, die es Einzelpersonen und Teams ermöglicht, wichtige Entscheidungen zu treffen, auch auf niedrigeren Führungsebenen (sofern diesen Entscheidungen überprüfbare Befugnisse und Sicherheitsmechanismen zugrunde liegen). Misserfolge werden als Lernerfahrung angesehen, und Teams lernen schrittweise, ihre Entscheidungen und Maßnahmen zu optimieren, um in Zukunft ähnliche Situationen zu bewältigen. Wenn die Maßnahmen einer Person zu einer Verbesserung führen, von der andere Teams profitieren können, werden die aus solchen Maßnahmen gewonnenen Erkenntnisse proaktiv geteilt.

Die Geschäftsführung misst betriebliche Verbesserungen und bietet dem Einzelnen sowie der Organisation Anreize für die Übernahme solcher Muster.

Typische Anti-Muster:

- In einer Organisation gibt es keine klaren Leitlinien oder Mechanismen dafür, was zu tun ist, wenn ein Risiko erkannt wird. Wenn ein Mitarbeiter beispielsweise einen Phishing-Angriff bemerkt und dies nicht dem Sicherheitsteam meldet, kann dies zur Folge haben, dass ein großer Teil der Organisation auf den Angriff hereinfällt. Dies führt zu einer Datenschutzverletzung.
- Ihre Kunden beschweren sich über die Nichtverfügbarkeit von Services, die hauptsächlich auf fehlgeschlagene Bereitstellungen zurückzuführen ist. Ihr SRE-Team ist für das Bereitstellungstool verantwortlich, und ein automatisiertes Rollback für Bereitstellungen ist Teil der langfristigen Roadmap. Bei einer kürzlichen Anwendungseinführung entwickelte einer der Engineers eine Lösung, um das Rollback seiner Anwendung auf eine frühere Version zu automatisieren. Obwohl die Lösung zum Vorbild für SRE-Teams werden könnte, wird sie von anderen Teams nicht übernommen, da kein Prozess zur Nachverfolgung solcher Verbesserungen vorhanden ist. Die Organisation wird weiterhin durch fehlgeschlagene Bereitstellungen unter Druck gesetzt, die sich auf die Kunden auswirken und die Reputation des Unternehmens gefährden.
- Zur Wahrung der Compliance überwacht Ihr Infosec-Team einen seit langem etablierten Prozess, bei dem gemeinsam genutzte SSH-Schlüssel im Namen der Betreiber, die eine Verbindung zu ihren Amazon EC2-Linux-Instances herstellen, regelmäßig rotieren. Die InfoSec-Teams brauchen mehrere Tage für die Schlüsselrotation. In dieser Zeit können Sie keine Verbindung zu diesen Instances herstellen. Bislang gab es keine Vorschläge, weder seitens von Infosec noch von außerhalb, zur Nutzung anderer Optionen in AWS, um dasselbe Ergebnis zu erzielen.

Vorteile der Etablierung dieser bewährten Methode: Indem Sie die Entscheidungsbefugnisse dezentralisieren und Ihre Teams in die Lage versetzen, wichtige Entscheidungen zu treffen, können Sie Probleme schneller lösen und die Erfolgsquoten erhöhen. Darüber hinaus beginnen die Teams, ein Gefühl der Eigenverantwortung zu entwickeln, und Misserfolge werden als Lernerfahrungen angesehen. Experimentieren wird zu einem Eckpfeiler der Unternehmenskultur. Manager und Bereichsleiter haben nicht das Gefühl, dass sie in allen Aspekten bis ins kleinste Detail gemanagt werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

1. Entwickeln Sie eine Kultur, in der damit gerechnet wird, dass Fehler auftreten können.

2. Definieren Sie klare Verantwortlichkeiten und Zuständigkeiten für verschiedene Funktionsbereiche innerhalb der Organisation.
3. Vermitteln Sie Eigenverantwortung und Rechenschaftspflicht, damit alle wissen, wo sie bei dezentralen Entscheidungen Unterstützung erhalten können.
4. Definieren Sie unumkehrbare und leicht revidierbare Entscheidungen, damit die Mitarbeiter wissen, wann sie Beschlüsse an höhere Führungsebenen eskalieren müssen.
5. Schaffen Sie in der Organisation ein Bewusstsein dafür, dass alle Mitarbeiter in der Lage sind, auf verschiedenen Ebenen Maßnahmen zu ergreifen, wenn Ergebnisse gefährdet sind. Stellen Sie Ihren Teammitgliedern Unterlagen über Governance, Befugnisebenen, Tools sowie Möglichkeiten zur Verfügung, um die erforderlichen Fähigkeiten für eine effektive Reaktion zu üben.
6. Geben Sie Ihren Teammitgliedern die Möglichkeit, die notwendigen Fähigkeiten zu üben, um auf verschiedene Entscheidungen zu reagieren. Sobald die Entscheidungsebenen festgelegt sind, führen Sie GameDays durch, um sicherzustellen, dass alle Mitarbeiter den Prozess verstehen und umsetzen können.
    a. Stellen Sie alternative sichere Umgebungen bereit, in denen Prozesse und Verfahren getestet und eingeübt werden können.
    b. Erkennen Sie an und schaffen Sie ein Bewusstsein dafür, dass Teammitglieder befugt sind, Maßnahmen zu ergreifen, wenn das Ergebnis ein vordefiniertes Risikoniveau aufweist.
    c. Verschaffen Sie den Teammitgliedern die erforderliche Autorität, um Maßnahmen zu ergreifen, indem Sie ihnen Berechtigungen und Zugriff auf ihre Workloads und Komponenten geben.
7. Bieten Sie Teams die Möglichkeit, ihre Erfahrungen (betriebliche Erfolge und Misserfolge) auszutauschen.
8. Ermöglichen Sie Teams, den Status quo in Frage zu stellen, und stellen Sie Mechanismen zur Verfügung, mit denen Verbesserungen sowie deren Auswirkungen auf die Organisation verfolgt und gemessen werden können.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP06 Bewerten von Kompromissen und Abwägen der Vorteile und Risiken
- OPS02-BP05 Mechanismen zur Identifizierung von Verantwortlichkeiten und Eigentümerschaft sind vorhanden

Zugehörige Dokumente:

- AWS-Blogbeitrag | Das agile Unternehmen
- AWS-Blogbeitrag | Erfolgsmessung: Ein Paradoxon und ein Plan
- AWS-Blogbeitrag | Loslassen: Autonomie in Teams ermöglichen
- Zentralisieren oder Dezentralisieren?

Zugehörige Videos:

- re:Invent 2023 | Wie Sie Ihre eigene Transformation nicht sabotieren (SEG201)
- re:Invent 2021 | Die Amazon Builders' Library: Operative Exzellenz von Amazon
- Zentralisierung vs. Dezentralisierung

Zugehörige Beispiele:

- Nutzung von Protokollen über Architekturentscheidungen zur Rationalisierung der technischen Entscheidungsfindung für ein Softwareentwicklungsprojekt

OPS03-BP03 Eskalation wird empfohlen

Die Teammitglieder werden von der Führung ermutigt, Probleme und Bedenken an übergeordnete Entscheidungsträger und Stakeholder zu eskalieren, wenn sie der Meinung sind, dass die gewünschten Ergebnisse gefährdet sind und die erwarteten Standards nicht erfüllt werden. Dies ist ein Merkmal der Organisationskultur und wird auf allen Ebenen vorangetrieben. Die Eskalation sollte frühzeitig und lieber zu oft vorgenommen werden, damit Risiken identifiziert und Vorfälle verhindert werden können. Die Führung tadelt Mitarbeiter nicht dafür, wenn sie ein Problem eskalieren.

Gewünschtes Ergebnis: Mitarbeiter in der gesamten Organisation fühlen sich wohl dabei, Probleme an ihre unmittelbaren Vorgesetzten und höhere Führungsebenen zu eskalieren. Die Führung hat bewusst und gezielt die Erwartung aufgestellt, dass sich ihre Teams sicher fühlen sollen, Probleme zu eskalieren. Es wurde ein Mechanismus eingerichtet, um Probleme auf allen Organisationsebenen zu eskalieren. Wenn Mitarbeiter eine Angelegenheit an ihren Vorgesetzten eskalieren, entscheiden sie gemeinsam über das Ausmaß der Auswirkungen und eine mögliche Eskalation des Problems. Eine Eskalation setzt voraus, dass die Mitarbeiter einen empfohlenen Arbeitsplan zur Behebung des Problems beifügen. Wenn die nächsthöhere Führungsebene nicht rechtzeitig Maßnahmen ergreift,

sind die Mitarbeiter angehalten, Probleme an die oberste Führungsebene weiterzuleiten, wenn sie der festen Überzeugung sind, dass die Risiken für die Organisation eine Eskalation rechtfertigen.

Typische Anti-Muster:

- Führungskräfte haken während Ihrer Statusbesprechung zum Cloud-Transformationsprogramm nicht ausreichend nach, um herauszufinden, wo Probleme und Hindernisse auftreten. Stattdessen werden nur gute Nachrichten präsentiert. Die CIO hat deutlich gemacht, dass sie nur gute Nachrichten hören möchte, um zu vermeiden, dass der CEO durch angesprochene Herausforderungen den Eindruck gewinnt, das Programm könne scheitern.
- Sie sind als Cloud-Betriebsentwickler tätig und stellen fest, dass das neue Wissensmanagementsystem von den Anwendungsteams kaum verwendet wird. Das Unternehmen investierte ein Jahr und mehrere Millionen Dollar in die Implementierung dieses neuen Wissensmanagementsystems, aber die Mitarbeiter verfassen ihre Runbooks noch immer lokal und teilen sie in einer internen Cloud-Umgebung, was die Suche nach Wissen erschwert, das für unterstützte Workloads relevant ist. Sie versuchen, die Führungskräfte darauf aufmerksam zu machen, da die konsequente Verwendung dieses Systems die betriebliche Effizienz verbessern kann. Als Sie das Problem der Bereichsleiterin vorlegen, die für die Implementierung des Wissensmanagementsystems zuständig ist, werden Sie von ihr kritisiert, weil dadurch die Investition in Frage gestellt wird.
- Das für die Absicherung der Computing-Ressourcen zuständige Infosec-Team hat beschlossen, einen Prozess einzuführen, bei dem die erforderlichen Scans durchgeführt werden müssen, um die vollständige Absicherung der EC2 Instances zu gewährleisten, bevor das Computing-Team die Ressource freigibt. Dies hat zu einer zusätzlichen Verzögerung von einer Woche für die Bereitstellung von Ressourcen und einer Verletzung des SLA geführt. Das Computing-Team hat Angst, dies über die Cloud an den VP zu eskalieren, da der VP für Informationssicherheit dadurch in ein schlechtes Licht gerückt werden könnte.

Vorteile der Nutzung dieser bewährten Methode:

Komplexe oder kritische Probleme werden angegangen, bevor sie sich auf das Geschäft auswirken. Es wird weniger Zeit verschwendet. Risiken werden minimiert. Teams werden bei der Lösung von Problemen proaktiver und ergebnisorientierter.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Die Bereitschaft und Fähigkeit, auf allen Organisationsebenen uneingeschränkt zu eskalieren, ist eine bedeutende Eigenschaft der Organisation und ihrer Kultur, die bewusst weiterentwickelt werden sollte, und zwar durch gezielte Schulungen, Kommunikationen der Führungsebene, Erwartungssetzung und den Einsatz von Mechanismen auf allen Organisationsebenen.

Implementierungsschritte

1. Definieren Sie Richtlinien, Standards und Erwartungen für Ihre Organisation.
    1. Sorgen Sie für eine breite Anwendung und Kenntnis der Richtlinien, Erwartungen und Standards.
2. Ermutigen, schulen und befähigen Sie die Mitarbeiter, damit sie frühzeitig und häufig eskalieren, wenn die Standards nicht eingehalten werden.
3. Bekräftigen Sie in der Organisation, dass die frühe und häufige Eskalation die bewährte Methode ist. Akzeptieren Sie im Unternehmen, dass sich Eskalationen zwar als unbegründet herausstellen können, es sich aber trotzdem insgesamt lohnt, wenn ein echter Vorfall dadurch verhindert wird.
    a. Entwickeln Sie einen Eskalationsmechanismus (wie ein Andron-Cord-System).
    b. Sorgen Sie für dokumentierte Verfahren, die definieren, wann und wie eine Eskalation erfolgen soll.
    c. Definieren Sie die Abfolge der Personen mit zunehmenden Befugnissen, um Maßnahmen zu ergreifen oder zu genehmigen, sowie die Kontaktinformationen der einzelnen Stakeholder.
4. Im Falle einer Eskalation sollte sie so lange fortgesetzt werden, bis das Teammitglied davon überzeugt ist, dass das Risiko durch entsprechende Maßnahmen der Führung gemindert wurde.
    a. Eskalationen sollten Folgendes beinhalten:
        i. Beschreibung der Situation und Art des Risikos
        ii. Kritikalität der Situation
        iii. Wer oder was betroffen ist
        iv. Umfang der Auswirkungen
        v. Dringlichkeit, falls eine Auswirkung eintritt
        vi. Vorgeschlagene Abhilfemaßnahmen und Risikominderungsplan
    b. Schützen Sie Mitarbeiter, die ein Problem eskalieren. Führen Sie eine Richtlinie ein, die Teammitglieder vor Konsequenzen schützt, wenn sie an einen ablehnend eingestellten Entscheidungsträger oder Stakeholder eskalieren. Schaffen Sie Mechanismen, um solche Szenarien zu erkennen, und leiten Sie entsprechende Maßnahmen ein.

5. Fördern Sie eine Kultur der kontinuierlichen Verbesserung durch Feedback-Schleifen in allen Bereichen der Organisation. Feedback-Schleifen fungieren als kleine Eskalationen an die verantwortlichen Personen und identifizieren Verbesserungsmöglichkeiten, auch wenn eine Eskalation nicht erforderlich ist. Eine Kultur der kontinuierlichen Verbesserung zwingt alle dazu, proaktiver zu werden.
6. Die Führung sollte regelmäßig an die Richtlinien, Standards und Mechanismen erinnern sowie an den Wunsch nach offener Eskalation und kontinuierlichen Feedback-Schleifen ohne Vergeltungsmaßnahmen jedweder Art.

Aufwand des Implementierungsplans: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP05 Mechanismen zum Anfordern von Ergänzungen, Änderungen und Ausnahmen sind vorhanden

Zugehörige Dokumente:

- Wie wird eine Kultur der kontinuierlichen Verbesserung und des Lernens von Andon und Eskalationssystemen geschaffen?
- Das Andon Cord (IT-Revolution)
- AWS-DevOps-Anleitung | Etablieren Sie klare Eskalationspfade und fördern Sie konstruktive Auseinandersetzungen

Zugehörige Videos:

- Jeff Bezos über Entscheidungsprozesse (und deren Beschleunigung)
- Das Toyota-Produktsystem: Produktionsstopp, ein Knopf und ein elektronisches Andon-Board
- Andon Cord in der LEAN-Fertigung

Zugehörige Beispiele:

- Arbeiten mit Eskalationsplänen im Incident Manager

OPS03-BP04 Die Kommunikation ist zeitnah, klar und umsetzbar

Die Führung ist für eine überzeugende und effektive Kommunikation zuständig, insbesondere wenn die Organisation vor der Einführung neuer Strategien, Technologien oder Arbeitsweisen steht. Führungskräfte sollten Erwartungen an alle Mitarbeiter stellen, damit sie auf die Unternehmensziele hinarbeiten können. Entwickeln Sie Kommunikationsmechanismen für die Bildung und Aufrechterhaltung des geforderten Bewusstseins in Teams, die für die Durchführung von Plänen verantwortlich sind, die von der Führung finanziert und unterstützt werden. Machen Sie sich die organisationsübergreifende Vielfalt zunutze und hören Sie sich verschiedene einzigartige Perspektiven aufmerksam an. Nutzen Sie diese Perspektiven, um Innovation zu fördern, Ihre Annahmen in Frage zu stellen und das Risiko einer Verzerrung durch automatische Bestätigung zu reduzieren. Stärken Sie Inklusion, Vielfalt und Zugehörigkeit innerhalb Ihrer Teams, um nützliche Perspektiven zu gewinnen.

Gewünschtes Ergebnis: Ihre Organisation entwirft Kommunikationsstrategien, um den Auswirkungen von Veränderungen auf das Unternehmen gerecht zu werden. Die Teams werden informiert und motiviert, weiter miteinander statt gegeneinander zu arbeiten. Einzelpersonen kennen die Bedeutung ihrer Rolle, um die angegebenen Ziele zu erreichen. E-Mail ist nur ein passiver Kommunikationsmechanismus und wird als solcher behandelt. Das Management verbringt Zeit mit seinen einzelnen Mitarbeitern, um ihnen ihre Verantwortung, die zu erledigenden Aufgaben und die Bedeutung ihrer Arbeit zur Gesamtmission zu vermitteln. Bei Bedarf binden Führungskräfte ihre Mitarbeiter an kleineren Veranstaltungsorten direkt ein, um Botschaften zu kommunizieren, und sie stellen sicher, dass diese Botschaften effektiv übermittelt werden. Die Organisation erfüllt oder übertrifft die Erwartungen der Führung mithilfe geeigneter Kommunikationsstrategien. Die Führung begrüßt und fördert unterschiedliche Meinungen innerhalb und zwischen Teams.

Typische Anti-Muster:

- Ihre Organisation hat einen Fünf-Jahres-Plan für die Migration aller Workloads in AWS. Der Business Case für die Cloud beinhaltet die Modernisierung von 25 % aller Workloads, um die Vorteile der Serverless-Technologie zu nutzen. Der CIO kommuniziert diese Strategie direkt unterstellten Mitarbeitern und erwartet, dass die Führungskräfte diese Präsentation ohne persönliche Gespräche an Manager, Bereichsleiter und einzelne Mitarbeiter weiterleiten. Der CIO zieht sich zurück und erwartet, dass seine Organisation die neue Strategie umsetzt.
- Die Führung bietet oder nutzt keine Feedback-Mechanismen, und die Erwartungslücke wächst, was dazu führt, dass einzelne Projekte ins Stocken geraten.

- Sie werden gebeten, eine Änderung an Ihren Sicherheitsgruppen vorzunehmen, ohne konkrete Informationen über die Änderung zu erhalten oder darüber, welche Auswirkungen sie auf alle Workloads haben könnte und bis wann sie umzusetzen ist. Der Manager leitet eine E-Mail vom VP von InfoSec weiter und fügt folgende Nachricht hinzu: "Make this happen."
- An Ihrer Migrationsstrategie wurden Änderungen vorgenommen, die die Anzahl der geplanten Modernisierungen von 25 auf 10 % reduzieren. Dies hat nachgelagerte Auswirkungen auf die Betriebsorganisation. Sie wurden nicht über diese strategische Änderung informiert und verfügen daher nicht über genügend qualifizierte Mitarbeiter, um einen größeren Lift-and-Shift-Aufwand von Workloads in AWS zu bewältigen.

Vorteile der Nutzung dieser bewährten Methode:

- Ihre Organisation ist über neue oder geänderte Strategien hinreichend informiert und die Mitarbeiter sind hochmotiviert, um sich gegenseitig dabei zu unterstützen, die von der Führung festgelegten Gesamtziele und Metriken zu erreichen.
- Es gibt Mechanismen und sie werden angewandt, um Teammitglieder rechtzeitig über bekannte Risiken und geplante Ereignisse zu informieren.
- Neue Arbeitsweisen (einschließlich Änderungen bzgl. Belegschaft, Organisation, Prozessen oder Technologien) werden zusammen mit den erforderlichen Fähigkeiten von der Organisation effektiver übernommen. Darüber hinaus erreicht Ihre Organisation schneller Geschäftsvorteile.
- Die Teammitglieder verfügen über die notwendigen Hintergrundinformationen zu den eingehenden Kommunikationen und können ihre Arbeit effektiver erledigen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Zur Implementierung dieser bewährten Methode müssen Sie mit Beteiligten aus der gesamten Organisation zusammenarbeiten, um Kommunikationsstandards zu vereinbaren. Machen Sie diese Standards in der Organisation bekannt. Bei allen wichtigen IT-Umstellungen kann ein etabliertes Planungsteam die Auswirkungen der Änderungen auf seine Mitarbeiter erfolgreicher bewältigen als eine Organisation, die diese Methode nicht anwendet. In größeren Organisationen können Veränderungen schwieriger umzusetzen sein, da es auf eine hohe Zustimmung aller einzelnen Mitarbeiter zu einer neuen Strategie ankommt. In Ermangelung eines solchen Umstellungsplanungsteams trägt die Führung zu 100 % die Verantwortung für eine effektive Kommunikation. Wenn Sie ein Umstellungsplanungsteam einrichten, weisen Sie die Teammitglieder

an, mit der gesamten Organisationsführung zusammenzuarbeiten, um eine effektive Kommunikation auf allen Ebenen zu definieren und zu gewährleisten.

Kundenbeispiel

AnyCompany Retail hat sich für den AWS Enterprise Support registriert und ist für seine Cloud-Betriebsabläufe auf andere Drittanbieter angewiesen. Das Unternehmen nutzt Chat und Chatops als zentrales Kommunikationsmedium für seine betrieblichen Aktivitäten. Warnmeldungen und andere Informationen ergehen über spezifische Kanäle. Wenn eine Maßnahme erforderlich ist, wird das erwartete Ergebnis klar formuliert, und in vielen Fällen gibt es ein Runbook oder Playbook dafür. Das Unternehmen verwendet einen Änderungskalender für die Planung größerer Änderungen an Produktionssystemen.

Implementierungsschritte

1. Richten Sie innerhalb der Organisation ein Kernteam ein, das für die Erstellung und Initiierung von Kommunikationsplänen für Änderungen verantwortlich ist, die auf mehreren Ebenen innerhalb der Organisation stattfinden.
2. Fordern Sie Eigenverantwortlichkeit, um ein hohes Maß an Übersicht zu fördern. Geben Sie den einzelnen Teams die Möglichkeit, unabhängig voneinander Innovationen zu entwickeln, und sorgen Sie für einen ausgewogenen Einsatz einheitlicher Mechanismen, die das richtige Maß an Einsicht und Zielgerichtetheit ermöglichen.
3. Arbeiten Sie mit allen Stakeholdern in Ihrer Organisation zusammen, um Kommunikationsstandards, -methoden und -pläne zu vereinbaren.
4. Stellen Sie sicher, dass das zentrale Kommunikationsteam mit der Organisations- und Programmleitung zusammenarbeitet, um im Namen der Führungskräfte Botschaften an die zuständigen Mitarbeiter zu verfassen.
5. Entwickeln Sie strategische Kommunikationsmechanismen, um Veränderungen mithilfe von Ankündigungen, gemeinsamen Kalendern, Besprechungen mit allen Mitarbeitern und persönlichen oder Einzelgesprächen zu bewältigen, sodass die Teammitglieder die richtigen Erwartungen bezüglich der zu ergreifenden Maßnahmen haben.
6. Geben Sie den erforderlichen Kontext, Details und die nötige Zeit (wenn möglich), um festzustellen, ob Maßnahmen erforderlich sind. Wenn Maßnahmen erforderlich sind, identifizieren Sie die erforderlichen Maßnahmen und deren Auswirkungen.
7. Implementieren Sie Tools, die eine taktische Kommunikation fördern, z. B. interne Chats, E-Mails und Wissensmanagement.

8. Implementieren Sie Mechanismen, um zu messen und zu überprüfen, ob mit allen Kommunikationen die gewünschten Ergebnisse erreicht werden.
9. Richten Sie eine Feedback-Schleife ein, die die Effektivität aller Kommunikationen misst, insbesondere wenn darin der Widerstand gegen Veränderungen in der Organisation thematisiert wird.
10. Ernennen Sie für alle AWS-Konten alternative Ansprechpartner für Abrechnung, Sicherheit und Betrieb. Idealerweise sollte es sich bei diesen Kontakten um E-Mail-Verteilerlisten und nicht um Einzelpersonen handeln.
11. Erstellen Sie einen Kommunikationsplan für die Eskalation und die umgekehrte Eskalation, um mit Ihren internen und externen Teams, einschließlich AWS Support und anderen Drittanbietern, zusammenzuarbeiten.
12. Initiieren Sie Kommunikationsstrategien und setzen Sie sie während der gesamten Laufzeit jedes Transformationsprogramms konsequent um.
13. Priorisieren Sie Maßnahmen, die nach Möglichkeit wiederholbar sind, um sie sicher und in großem Maßstab zu automatisieren.
14. Wenn Kommunikation in Szenarien mit automatisierten Maßnahmen erforderlich ist, sollte die Kommunikation hauptsächlich der Information der Teams oder Audits dienen oder Teil des Änderungsverwaltungsprozesses sein.
15. Analysieren Sie die Kommunikation Ihrer Warnsysteme auf Fehlalarme oder Warnmeldungen, die ständig generiert werden. Entfernen Sie diese Warnmeldungen oder ändern Sie sie so, dass sie nur ausgelöst werden, wenn menschliches Eingreifen erforderlich ist. Stellen Sie ein Runbook oder Playbook bereit, wenn eine Warnmeldung ausgelöst wird.
    a. Mit AWS Systems Manager-Dokumenten können Sie Runbooks oder Playbooks für Warnmeldung erstellen.
16. Es gibt Mechanismen zur Benachrichtigung über Risiken oder geplante Ereignisse auf eine klare und unterstützende Weise mit ausreichend Zeit für geeignete Maßnahmen. Verwenden Sie E-Mail-Listen oder Chat-Kanäle zum Senden von Benachrichtigungen vor geplanten Ereignissen.
    a. Mit AWS Chatbot können Sie innerhalb der Messaging-Plattform Ihrer Organisation Warnmeldungen senden und auf Ereignisse reagieren.
17. Stellen Sie eine zugängliche Informationsquelle bereit, der geplante Ereignisse zu entnehmen sind. Stellen Sie Benachrichtigungen zu geplanten Ereignissen vom gleichen System bereit.
    a. Mit AWS Systems Manager Change Calendar können Sie Änderungszeitfenster für anstehende Änderungen einrichten. Dadurch werden Teammitglieder benachrichtigt, wann Sie in sicherer Weise Änderungen vornehmen können.

18. Überwachen Sie Benachrichtigungen zu Schwachstellen und Patch-Informationen, um bestehende Schwachstellen und potenzielle Risiken im Zusammenhang mit den Komponenten Ihrer Workloads zu verstehen. Stellen Sie Benachrichtigungen für die Teammitglieder bereit, damit sie Maßnahmen ergreifen können.
    a. Sie können AWS Security Bulletins abonnieren, um zu Schwachstellen in AWS benachrichtigt zu werden.
19. Berücksichtigen unterschiedlicher Meinungen und Perspektiven: Ermutigen Sie alle anderen, sich zu Wort zu melden. Geben Sie unterrepräsentierten Gruppen die Möglichkeit, sich in die Kommunikation einzubringen. Rotieren Sie die Rollen und Zuständigkeiten in Meetings.
    a. Erweitern von Rollen und Zuständigkeiten: Bieten Sie Teammitgliedern Möglichkeiten, Rollen zu übernehmen, die ihnen fremd sind. Auf diese Weise können sie Erfahrung sammeln und neue Perspektiven durch die Rolle und den resultierenden Austausch mit neuen Teammitgliedern gewinnen, zu denen sie möglicherweise andernfalls keinen Kontakt hätten. Nicht zuletzt können sie die neue Rolle und die Teammitglieder mit ihren Erfahrungen und Perspektiven bereichern. Mit zunehmender Erfahrung werden Sie aufkommende Geschäftsmöglichkeiten oder neue Verbesserungsmöglichkeiten identifizieren. Rotieren Sie allgemeine Aufgaben zwischen den Mitgliedern innerhalb eines Teams, die normalerweise anderen Tätigkeiten nachgehen, damit sie deren Anforderungen und Auswirkungen verstehen.
    b. Bereitstellen einer sicheren und freundlichen Umgebung: Etablieren Sie Richtlinien und Kontrollen zum Schutz der geistigen und physischen Sicherheit der Teammitglieder in Ihrer Organisation. Die Teammitglieder müssen ohne Angst vor Vergeltungsmaßnahmen zusammenarbeiten können. Wenn sich Teammitglieder sicher und willkommen fühlen, ist die Wahrscheinlichkeit höher, dass sie engagiert und produktiv bleiben. Je vielfältiger Ihre Organisation ist, desto besser verstehen Sie die Personen, die Sie unterstützen, einschließlich Ihrer Kunden. Wenn Ihre Teammitglieder zufrieden sind, ihre Meinung sagen können und sich ernst genommen fühlen, steigt die Wahrscheinlichkeit, dass sie wertvolle Erkenntnisse mitteilen (z. B. Marketingmöglichkeiten, erforderliche Maßnahmen zur Barrierefreiheit, unerschlossene Marktsegmente, unbehandelte Risiken in Ihrer Umgebung).
    c. Ermöglichen einer umfassenden Beteiligung von Teammitgliedern: Stellen Sie die Ressourcen bereit, die Ihre Mitarbeiter zur umfassenden Beteiligung an allen arbeitsbezogenen Aktivitäten benötigen. Teammitglieder haben Fähigkeiten entwickelt, mit denen sie ihre täglichen Herausforderungen meistern. Diese einzigartigen Fähigkeiten können für Ihre Organisation von großem Vorteil sein. Wenn Sie die Teammitglieder mit den notwendigen Ressourcen ausstatten, können Sie den Nutzen ihrer Beiträge maximieren.

Ressourcen

Zugehörige bewährte Methoden:

- OPS03-BP01 Förderung durch die Geschäftsführung gewährleisten
- OPS07-BP03 Verwenden von Runbooks zur Durchführung von Verfahren
- OPS07-BP04 Verwenden von Playbooks zum Untersuchen von Problemen

Zugehörige Dokumente:

- AWS-Blogbeitrag | Eigenverantwortung und Befähigung sind der Schlüssel zu leistungsstarken agilen Organisationen
- AWS Executive Insights | Lernen Sie, Innovation statt Komplexität zu skalieren | Eigenverantwortliche Führungskräfte
- AWS-Sicherheitsberichte
- Open CVE
- AWS Support App in Slack zur Verwaltung von Support-Fällen
- Verwaltung von AWS-Ressourcen in Slack-Kanälen mit AWS Chatbot

Zugehörige Beispiele:

- Well-Architected Labs: Inventory and Patch Management (Level 100) (Well-Architected Labs: Bestands- und Patch-Verwaltung (Stufe 100))

Zugehörige Services:

- AWS Chatbot
- AWS Systems Manager Change Calendar
- AWS Systems Manager-Dokumente

OPS03-BP05 Experimentieren wird empfohlen

Experimente können Katalysatoren für die Umsetzung von Ideen in Produkte und Funktionen sein. Sie beschleunigen Lernprozesse und halten Teammitglieder interessiert und engagiert.

Team-Mitglieder sollten oft experimentieren, um Innovationen voranzubringen. Selbst nicht erwünschte Ergebnissen bieten den Vorteil, dass man dadurch weiß, wie man nicht vorgehen sollte. Teammitglieder werden nicht für erfolgreiche Experimente mit unerwünschten Ergebnissen bestraft.

Gewünschtes Ergebnis:

- Ihre Organisation ermutigt zum Experimentieren, um Innovationen voranzubringen.
- Experimente werden genutzt, um daraus zu lernen.

Typische Anti-Muster:

- Sie möchten einen A/B-Test durchführen, es gibt jedoch keinen Mechanismus für das Experiment. Sie stellen eine UI-Änderung bereit, ohne diese testen zu können. Dies beeinträchtigt den Kundenkomfort.
- Ihr Unternehmen verfügt nur über eine Staging- und eine Produktionsumgebung. Es gibt keine Sandbox-Umgebung zum Experimentieren mit neuen Funktionen oder Produkten, weshalb Sie in der Produktionsumgebung experimentieren müssen.

Vorteile der Nutzung dieser bewährten Methode:

- Experimente bringen Innovationen voran.
- Mithilfe von Experimenten können Sie schneller auf Feedback reagieren.
- Ihre Organisation entwickelt eine Lernkultur.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Experimente sollten in sicherer Weise durchgeführt werden. Nutzen Sie mehrere Umgebungen für Experimente, ohne dabei Produktionsressourcen in Gefahr zu bringen. Nutzen Sie A/B-Tests und Feature-Flags für Testexperimente. Geben Sie Teammitgliedern die Möglichkeit, Experimente in einer Sandbox-Umgebung durchzuführen.

Kundenbeispiel

AnyCompany Retail ermuntert seine Mitarbeiter zu Experimenten. Teammitglieder können 20 % ihrer wöchentlichen Arbeitszeit für Experimente oder zum Erlernen neuer Technologien nutzen. Es gibt

eine Sandbox-Umgebung zum Ausprobieren von Innovationen. Für neue Funktionen werden A/B-Tests verwendet, um sie mit realem Benutzerfeedback zu prüfen.

Implementierungsschritte

1. Arbeiten Sie mit Führungskräften aus dem gesamten Unternehmen zusammen, um Experimente zu unterstützen. Teammitglieder sollten aufgefordert werden, Experimente in sicherer Weise durchzuführen.
2. Stellen Sie Ihren Teammitgliedern eine Umgebung zur Verfügung, in der sie in sicherer Weise experimentieren können. Sie müssen Zugriff auf eine Umgebung haben, die der Produktionsumgebung stark ähnelt.
   a. Sie können ein separates AWS-Konto verwenden, um eine Sandbox-Umgebung für Experimente einzurichten. AWS Control Tower kann zur Bereitstellung solcher Konten verwendet werden.
3. Verwenden Sie Feature-Flags und A/B-Tests, um in sicherer Weise zu experimentieren und Benutzer-Feedback einzuholen.
   a. AWS AppConfig Feature Flags ermöglicht das Erstellen von Feature-Flags.
   b. Amazon CloudWatch Evidently kann für A/B-Tests für eine begrenzte Bereitstellung verwendet werden.
   c. Mit AWS Lambda-Versionen können Sie eine neue Version einer Funktion für Beta-Tests bereitstellen.

Grad des Aufwands für den Implementierungsplan: hoch. Die Bereitstellung einer Umgebung für Teammitglieder, in der sie in sicherer Weise experimentieren können, kann erhebliche Investitionen erfordern. Möglicherweise muss auch der Anwendungscode modifiziert werden, um Feature-Flags verwenden oder A/B-Tests unterstützen zu können.

Ressourcen

Zugehörige bewährte Methoden:

- OPS11-BP02 Durchführen von Analysen nach Vorfällen – Das Lernen aus Vorfällen ist zusammen mit Experimenten ein wichtiger Faktor für Innovationen.
- OPS11-BP03 Implementieren von Feedbackschleifen – Feedbackschleifen sind ein wichtiger Bestandteil von Experimenten.

Zugehörige Dokumente:

- An Inside Look at the Amazon Culture: Experimentation, Failure, and Customer Obsession (Ein Insiderblick auf die Kultur bei Amazon: Experimente, Fehler und absolute Kundenorientierung)
- Best practices for creating and managing sandbox accounts in AWS(Bewährte Methoden für das Erstellen und Verwalten von Sandbox-Konten in AWS)
- Create a Culture of Experimentation Enabled by the Cloud (Schaffen einer Experimente-Kultur mithilfe der Cloud)
- Enabling experimentation and innovation in the cloud at SulAmérica Seguros (Ermöglichen von Experimenten und Innovationen in der Cloud bei SulAmérica Seguros)
- Experiment More, Fail Less (Mehr Experimente, weniger Fehlschläge)
- Organizing Your AWS Environment Using Multiple Accounts - Sandbox OU (Organisieren der AWS-Umgebung mithilfe mehrerer Konten – Sandbox-OU)
- Using AWS AppConfig Feature Flags (Verwendung von AWS AppConfig-Feature-Flags)

Zugehörige Videos:

- AWS On Air ft. Amazon CloudWatch Evidently | AWS Events
- AWS On Air San Fran Summit 2022 ft. AWS AppConfig Feature Flags integration with Jira (AWS AppConfig-Feature-Flags-Integration mit Jira)
- AWS re:Invent 2022 - A deployment is not a release: Control your launches w/feature flags (BOA305-R) (AWS re:Invent 2022 – Eine Bereitstellung ist keine Freigabe: Produktstarts mit Feature-Flags kontrollieren (BOA305-R))
- Programmatically Create an AWS-Konto with AWS Control Tower(Ein AWS-Konto mit AWS Control Tower programmgesteuert erstellen)
- Set Up a Multi-Account AWS Environment that Uses Best Practices for AWS Organizations(Eine Multi-Konto-Umgebung in AWS einrichten, in der bewährte Methoden für AWS Organizations verwendet werden)

Zugehörige Beispiele:

- AWS Innovation Sandbox
- End-to-end Personalization 101 for E-Commerce (Einführung in die durchgehende Personalisierung für E-Commerce)

Zugehörige Services:

- Amazon CloudWatch Evidently
- AWS AppConfig
- AWS Control Tower

OPS03-BP06 Teammitglieder werden ermutigt, ihre Fähigkeiten zu pflegen und zu erweitern

Teams müssen ihre Fähigkeiten ausbauen, um neue Technologien nutzen und mit veränderten Anforderungen und Aufgaben Ihrer Workloads umgehen zu können. Neue Fähigkeiten im Umgang mit neuen Technologien erhöhen oftmals die Zufriedenheit der Teammitglieder und ermöglichen Innovationen. Unterstützen Sie Ihre Teammitglieder beim Erlangen und Bewahren von Branchenzertifizierungen, mit denen ihre wachsenden Fähigkeiten bestätigt und anerkannt werden. Führen Sie funktionsübergreifende Trainings durch, um den Wissenstransfer zu fördern und das Risiko signifikanter Auswirkungen zu reduzieren, wenn Sie qualifizierte und erfahrene Teammitglieder mit kritischem Wissen verlieren. Schaffen Sie spezielle strukturierte Lernzeiten.

AWS bietet Ressourcen, darunter das AWS Getting Started Resource Center, AWS Blogs, AWS Online Tech Talks, AWS-Veranstaltungen und Webinare sowie die AWS Well-Architected Labs, die Leitfäden, Beispiele und detaillierte Anleitungen zur Schulung Ihrer Teams bieten.

Ressourcen wie AWS Support, (AWS re:Post, AWS Support Center) und AWS-Documentation helfen dabei, technische Hindernisse zu beseitigen und den Betrieb zu verbessern. Bei Fragen können Sie sich über das AWS Support Center an den AWS Support wenden.

AWS stellt in der The Amazon Builders' Library auch bewährte Methoden und Muster vor, die wir durch den Betrieb von AWS gelernt haben, sowie im AWS-Blog und im offiziellen AWS-Podcast eine Vielzahl anderer nützlicher Lernmaterialien.

AWS Training und die Zertifizierung beinhalten kostenlose Schulungen in digitalen Kursen zum Selbststudium sowie rollen- und bereichsspezifische Lernpläne. Sie können sich auch für eine Schulung mit Kursleiter registrieren, um die AWS-Fähigkeiten Ihres Teams auszubauen.

Gewünschtes Ergebnis: Ihre Organisation evaluiert ständig Qualifikationslücken und schließt sie durch strukturierte Budget- und Investitionspläne. Die Teams ermutigen und unterstützen ihre Mitglieder durch Weiterbildungsaktivitäten wie den Erwerb führender Branchenzertifizierungen. Die Teams nutzen spezielle Programme zum Wissensaustausch wie informelle Schulungen,

Immersion Days, Hackathons und GameDays. Ihre Organisation hält ihre Wissenssysteme auf dem aktuellen Stand und relevant für die Schulung von Teammitgliedern, einschließlich Schulungen zur Einarbeitung neuer Mitarbeiter.

Typische Anti-Muster:

- Aufgrund eines fehlenden strukturierten Trainingsprogramms und Budgets entstehen in den Teams Unsicherheit und Zweifel, wenn sie versuchen, mit der technologischen Entwicklung Schritt zu halten, was letztlich zu einer erhöhten Personalabwanderung führt.
- Im Rahmen der Migration zu AWS weist Ihre Organisation Qualifikationslücken auf und die Teams verfügen über unterschiedlich starke Cloud-Kompetenzen. Aufgrund fehlender Fortbildungsprogramme sehen sich die Teams mit der veralteten und ineffizienten Verwaltung der Cloud-Umgebung überfordert, was zu einer Mehrbelastung der Mitarbeiter führt. Diese erschwerten Arbeitsbedingungen erhöhen die Unzufriedenheit der Mitarbeiter.

Vorteile der Einführung dieser bewährten Methode: Wenn Ihre Organisation bewusst in die Verbesserung der Fähigkeiten seiner Teams investiert, wird damit auch die Cloud-Einführung und -Optimierung beschleunigt und skaliert. Gezielte Lernprogramme fördern Innovationen und stärken die operativen Fähigkeiten der Teams, um auf Ereignisse vorbereitet zu sein. Teams investieren bewusst in die Implementierung und Weiterentwicklung von bewährten Methoden. Die Arbeitsmoral im Team ist hoch und die Teammitglieder sind stolz auf ihren Beitrag zum Unternehmen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Investieren Sie kontinuierlich in die berufliche Weiterentwicklung Ihrer Teams, um neue Technologien einzuführen, Innovationen voranzutreiben und mit den Veränderungen der Anforderungen und Verantwortlichkeiten Schritt zu halten, um Ihre Workloads zu unterstützen.

Implementierungsschritte

1. Verwendung strukturierter Cloud-Unterstützungsprogramme:AWS Skills Guild bietet beratende Schulungen an, um das Vertrauen in Cloud-Fähigkeiten zu stärken und eine Kultur des kontinuierlichen Lernens anzuregen.
2. Bereitstellung von Ressourcen für Weiterbildungen: Richten Sie eine spezielle strukturierte Lernzeit ein und stellen Sie Schulungsmaterialien und Übungsressourcen bereit. Unterstützen Sie die Teilnahme an Konferenzen und bei Branchenverbänden, die Möglichkeiten zum Lernen

von Lehrkräften und anderen Fachleuten bieten. Stellen Sie für Ihre Junior-Teammitglieder den Kontakt zu erfahreneren Teammitgliedern als Mentoren her oder ermöglichen Sie Junior-Teammitgliedern, ihnen bei der Arbeit zuzusehen, um sich mit ihren Methoden und Fähigkeiten vertraut zu machen. Ermutigen Sie dazu, auch etwas über Inhalte zu lernen, die nicht direkt mit der Arbeit zusammenhängen, um den Horizont zu erweitern.

3. Ermutigung zur Nutzung technischer Fachressourcen: Nutzen Sie Ressourcen wie AWS Re:Post, um Zugang zu kuratiertem Wissen und einer lebendigen Community zu erhalten.
4. Aufbau und Pflege eines aktuellen Wissensrepositorys: Verwenden Sie Plattformen für den Wissensaustausch wie Wikis und Runbooks. Erstellen Sie mit AWS re:POST Private Ihre eigene wiederverwendbare Informationsquelle mit Expertenwissen, um die Zusammenarbeit zu optimieren, die Produktivität zu verbessern und die Einarbeitung von Mitarbeitern zu beschleunigen.
5. Teamschulung und teamübergreifende Zusammenarbeit: Planen Sie die kontinuierlichen Weiterbildungsanforderungen Ihrer Teammitglieder mit ein. Schaffen Sie Gelegenheiten für die Teammitglieder, (vorübergehend oder dauerhaft) in anderen Teams zu arbeiten, damit sie untereinander Fähigkeiten und bewährte Methoden austauschen können, wovon letztendlich die gesamte Organisation profitiert.
6. Unterstützung beim Erlangen und Bewahren von Branchenzertifizierungen: Unterstützen Sie Ihre Teammitglieder bei der Erlangung und dem Erhalt von Branchenzertifizierungen, durch die das Gelernte bestätigt wird und die Erfolge anerkannt werden.

Aufwand für den Implementierungsplans: hoch

Ressourcen

Zugehörige bewährte Methoden:

- OPS03-BP01 Förderung durch die Geschäftsführung gewährleisten
- OPS11-BP04 Wissensmanagement

Zugehörige Dokumente:

- AWS Whitepaper | Framework zur Cloud-Einführung: Die Perspektive der Mitarbeiter
- Investition in kontinuierliches Lernen für eine erfolgreiche Zukunft Ihrer Organisation
- AWS Skills Guild
- AWS Training und -Zertifizierung

- AWS Support
- AWS re:Post
- AWS-Ressourcencenter für den Einstieg
- AWS-Blogs
- AWS Cloud-Compliance
- AWS-Dokumentation
- Der offizielle AWS-Podcast.
- AWS Online Tech Talks
- AWS-Veranstaltungen und -Webinare
- AWS Well-Architected Labs
- Die Amazon Builders’ Library

Zugehörige Videos:

- AWS re:Invent 2023 | Umschulung im Tempo der Cloud: Aus Mitarbeitern werden Unternehmer
- WS re:Invent 2023 | Aufbau einer Kultur der Neugier durch Gamification

OPS03-BP07 Teams mit entsprechenden Ressourcen ausstatten

Setzen Sie die richtige Anzahl kompetenter Teammitglieder ein und stellen Sie Tools und Ressourcen zur Verfügung, um Ihre Workload-Anforderungen zu erfüllen. Eine Überlastung der Teammitglieder erhöht das Risiko menschlicher Fehler. Investitionen in Tools und Ressourcen wie Automatisierung können die Effektivität Ihres Teams steigern und es dabei unterstützen, eine größere Anzahl von Workloads zu bewältigen, ohne zusätzliche Kapazitäten zu benötigen.

Gewünschtes Ergebnis:

- Sie haben Ihr Team personell angemessen ausgestattet, um die erforderlichen Fähigkeiten zu erwerben, um Workloads in AWS entsprechend Ihres Migrationsplans zu betreiben. Da sich Ihr Team im Laufe Ihres Migrationsprojekts vergrößert hat, hat es sich mit den AWS-Kerntechnologien vertraut gemacht, die das Unternehmen bei der Migration oder Modernisierung seiner Anwendungen verwenden möchte.
- Sie haben Ihren Personalplan sorgfältig abgestimmt, um Ressourcen mithilfe von Automatisierung und Workflows effizient zu nutzen. Ein kleineres Team kann jetzt im Auftrag der Anwendungsentwicklungsteams mehr Infrastruktur verwalten.

- Angesichts sich ändernder betrieblicher Prioritäten werden Personalengpässe proaktiv erkannt, um den Erfolg von Geschäftsinitiativen zu sichern.
- Betriebsmetriken, die auf operative Schwierigkeiten (wie Ermüdung des Bereitschaftsdienstes oder übermäßiges Telefonieren) hinweisen, werden überprüft, um eine Überforderung der Mitarbeiter zu vermeiden.

Typische Anti-Muster:

- Ihre Mitarbeiter erwerben keine neuen AWS-Fähigkeiten, während Sie Ihren mehrjährigen Cloud-Migrationsplan entwickeln, was die Unterstützung der Workloads riskiert und die Arbeitsmoral der Mitarbeiter herabsetzt.
- Ihre gesamte IT-Organisation stellt sich auf agile Arbeitsweisen um. Das Unternehmen priorisiert das Produktportfolio und legt Metriken dafür fest, welche Features zuerst entwickelt werden müssen. Ihr agiler Prozess erfordert nicht, dass Teams ihren Arbeitsplänen Story Points zuweisen. Daher ist es unmöglich zu wissen, welche Kapazitäten für den nächsten Arbeitsschritt erforderlich sind oder ob Sie über die dafür notwendigen Fähigkeiten verfügen.
- Sie lassen Ihre Workloads von einem AWS Partner migrieren, und Sie haben keinen Supportübergangsplan für Ihre Teams, sobald der Partner das Migrationsprojekt abgeschlossen hat. Ihre Teams haben Schwierigkeiten, die Workloads effizient und effektiv zu unterstützen.

Vorteile der Einführung dieser bewährten Methode:In Ihrer Organisation stehen Ihnen entsprechend qualifizierte Teammitglieder zur Verfügung, um die Workloads zu unterstützen. Die Ressourcenzuweisung kann an sich ändernde Prioritäten angepasst werden, ohne die Leistung zu beeinträchtigen. Somit können die Teams die Workloads effizient unterstützen und gleichzeitig mehr Zeit mit Innovationen für Kunden aufwenden, was wiederum die Mitarbeiterzufriedenheit erhöht.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Die Ressourcenplanung für Ihre Cloud-Migration sollte auf einer Organisationsebene erfolgen, die Ihrem Migrationsplan sowie dem gewünschten Betriebsmodell entspricht, das zur Unterstützung Ihrer neuen Cloud-Umgebung implementiert wird. Dies erfordert nicht zuletzt ein umfassendes Verständnis, welche Cloud-Technologien für die Geschäfts- und Anwendungsentwicklungsteams eingesetzt werden. Die Infrastruktur- und Betriebsleitung sorgt für eine Analyse von Qualifikationslücken, Schulungen und die Rollendefinition für Ingenieure, die die Cloud-Einführung leiten.

Implementierungsschritte

1. Definieren Sie Erfolgskriterien für den Erfolg des Teams anhand relevanter Betriebsmetriken wie der Mitarbeiterproduktivität (z. B. Kosten für die Unterstützung einer Workload oder Arbeitsstunden, die Mitarbeiter bei Vorfällen aufgewendet haben).
2. Definieren Sie Mechanismen zur Planung und Überprüfung der Kapazität von Ressourcen, um sicherzustellen, dass bei Bedarf ausreichend qualifizierte Ressourcen verfügbar sind und deren Zahl im Laufe der Zeit angepasst werden kann.
3. Schaffen Sie Mechanismen (z. B. das Senden einer monatlichen Umfrage an Teams), um arbeitsbezogene Herausforderungen zu verstehen, die sich auf Teams auswirken (z. B. zunehmende Verantwortlichkeiten, technologische Veränderungen, Personalabwanderung oder wachsende Anzahl unterstützter Kunden).
4. Verwenden Sie diese Mechanismen, um mit Teams in Kontakt zu treten und Trends zu erkennen, die zu Problemen bei der Mitarbeiterproduktivität beitragen können. Wenn sich äußere Faktoren negativ auf Ihre Teams auswirken, bewerten Sie die Ziele neu und passen Sie sie entsprechend an. Identifizieren Sie Hindernisse für den Fortschritt Ihrer Teams.
5. Prüfen Sie regelmäßig, ob Ihre derzeit vorhandenen Ressourcen noch ausreichen oder ob zusätzliche Ressourcen benötigt werden, und nehmen Sie entsprechende Anpassungen an den Support-Teams vor.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS03-BP06 Teammitglieder werden ermutigt, ihre Fähigkeiten zu pflegen und zu erweitern
- OPS09-BP03 Überprüfen der Betriebsmetriken und Priorisieren von Verbesserungen
- OPS10-BP01 Verwenden eines Prozesses für die Bewältigung von Ereignissen, Vorfällen und Problemen
- OPS10-BP07 Automatisieren von Reaktionen auf Ereignisse

Zugehörige Dokumente:

- AWS Cloud Adoption Framework: Die Perspektive der Mitarbeiter
- Auf dem Weg zu einem zukunftsfähigen Unternehmen

- Priorisieren der Fähigkeiten Ihrer Mitarbeiter, um das Geschäftswachstum voranzutreiben
- Leistungsstarke Organisation – das Zwei-Pizza-Team von Amazon
- Das Erfolgsrezept von Cloud-reifen Unternehmen

Vorbereitung

Zur Vorbereitung auf operative Exzellenz müssen Sie in Erfahrung bringen, mit welchen Workloads zu rechnen ist und wie diese wahrscheinlich ausfallen werden. Dann können Sie diese so gestalten, dass Sie Einblick in deren Status erhalten und entsprechende Verfahren zu deren Unterstützung entwerfen.

Zur Vorbereitung auf operative Exzellenz müssen Sie die folgenden Punkte berücksichtigen:

Themen

Implementieren von Beobachtbarkeit

Implementieren Sie Beobachtbarkeit in Ihren Workload, damit Sie seinen Zustand verstehen und datengesteuerte Entscheidungen auf der Grundlage von Geschäftsanforderungen treffen können.

Beobachtbarkeit geht über die einfache Überwachung hinaus und bietet ein umfassendes Verständnis der internen Funktionsweise eines Systems auf der Grundlage seiner externen Ergebnisse. Beobachtbarkeit basiert auf Metriken, Protokollen und Traces und liefert tiefgreifende Erkenntnisse zum Verhalten und zur Dynamik von Systemen. Mit effektiver Beobachtbarkeit können Teams Muster, Anomalien und Trends erkennen, sodass sie potenzielle Probleme proaktiv angehen und einen optimalen Systemzustand aufrechterhalten können.

Die Identifizierung von wichtigen Leistungskennzahlen (KPIs) ist entscheidend, um sicherzustellen, dass die Überwachungsaktivitäten und die Geschäftsziele aufeinander abgestimmt sind. Diese Abstimmung stellt sicher, dass Teams datengestützte Entscheidungen anhand von Metriken treffen, die wirklich wichtig sind, wodurch sowohl die Systemleistung als auch die Geschäftsergebnisse optimiert werden.

Darüber hinaus ermöglicht Beobachtbarkeit Unternehmen, proaktiv statt reaktiv zu handeln. Teams können die Ursache-Wirkung-Beziehungen innerhalb ihrer Systeme verstehen und Probleme vorhersagen und verhindern, anstatt nur auf sie zu reagieren. Da sich Workloads weiterentwickeln,

ist es wichtig, die Beobachtbarkeitsstrategie immer wieder neu aufzugreifen und zu verfeinern, um sicherzustellen, dass sie relevant und effektiv bleibt.

Bewährte Methoden

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS04-BP02 Implementieren einer Anwendungstelemetrie
- OPS04-BP03 Implementieren von Telemetrie für Benutzererfahrung
- OPS04-BP04 Implementieren einer Abhängigkeitstelemetrie
- OPS04-BP05 Implementieren der verteilten Nachverfolgung

OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen

Die Implementierung von Beobachtbarkeit in Ihrem Workload beginnt damit, seinen Status zu verstehen und datengestützte Entscheidungen auf der Grundlage der geschäftlichen Anforderungen zu treffen. Eine der wirksamsten Methoden zur Sicherung der Übereinstimmung von Überwachungsaktivitäten mit den Geschäftszielen ist die Definition und Überwachung von Leistungskennzahlen (KPIs).

Gewünschtes Ergebnis: Effiziente Beobachtbarkeitspraktiken, die eng an den Geschäftszielen ausgerichtet sind und sicherstellen, dass die Überwachungsanstrengungen stets greifbaren Geschäftsergebnissen dienen.

Typische Anti-Muster:

- Undefinierte KPIs: Das Arbeiten ohne klare KPIs kann dazu führen, dass zu viel oder zu wenig überwacht wird und wichtige Signale fehlen.
- Statische KPIs: KPIs werden nicht überarbeitet oder verfeinert, wenn sich der Workload oder die Geschäftsziele ändern.
- Fehlausrichtung: Konzentration auf technische Metriken, die nicht direkt mit Geschäftsergebnissen korrelieren oder schwieriger mit realen Problemen zu korrelieren sind.

Vorteile der Nutzung dieser bewährten Methode:

- Einfache Identifizierung von Problemen: Geschäfts-KPIs machen Probleme oft deutlicher sichtbar als technische Metriken. Ein Rückgang eines Geschäfts-KPIs kann ein Problem effektiver lokalisieren, als die Analyse zahlreicher technischer Metriken.

- Geschäftsausrichtung: Es wird sichergestellt, dass die Überwachungsaktivitäten die Geschäftsziele direkt unterstützen.
- Effizienz: Es erfolgt eine Priorisierung der Ressourcen für die Überwachung und die Konzentration auf wichtige Metriken.
- Proaktivität: Probleme werden erkannt und gelöst, bevor sie weitreichende Auswirkungen auf das Geschäft haben.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

So definieren Sie Workload-KPIs effektiv:

1. Beginnen Sie mit den Geschäftsergebnissen: Bevor Sie sich mit Metriken befassen, sollten Sie sich mit den gewünschten Geschäftsergebnissen vertraut machen. Sind es höhere Umsätze, mehr Benutzerinteraktionen oder schnellere Reaktionszeiten?
2. Stimmen Sie technische Metriken auf Geschäftsziele ab: Nicht alle technischen Metriken wirken sich direkt auf die Geschäftsergebnisse aus. Identifizieren Sie diejenigen, die dies tun. Oft ist es jedoch einfacher, ein Problem anhand eines Geschäfts-KPI zu identifizieren.
3. Verwenden Sie Amazon CloudWatch: Nutzen Sie CloudWatch, um Metriken zu definieren und zu überwachen, die Ihre KPIs repräsentieren.
4. Überprüfen und aktualisieren Sie die KPIs regelmäßig: Sorgen Sie dafür, dass Ihre KPIs relevant bleiben, während sich Ihr Workload und Ihr Unternehmen weiterentwickeln.
5. Beziehen Sie Stakeholder ein: Beziehen Sie sowohl IT- als auch Business-Teams in die Definition und Überprüfung von KPIs ein.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- the section called “OPS04-BP02 Implementieren einer Anwendungstelemetrie”
- the section called “OPS04-BP03 Implementieren von Telemetrie für Benutzererfahrung”
- the section called “OPS04-BP04 Implementieren einer Abhängigkeitstelemetrie”

- the section called “OPS04-BP05 Implementieren der verteilten Nachverfolgung”

Zugehörige Dokumente:

- AWS Observability Best Practices (Bewährte Methoden zur Beobachtbarkeit für AWS)
- CloudWatch User Guide (CloudWatch-Benutzerhandbuch)
- AWS Observability Skill Builder Course (Skill-Builder-Kurs zur Beobachtbarkeit in AWS)

Zugehörige Videos:

- Developing an observability strategy (Entwicklung einer Beobachtbarkeitsstrategie)

Zugehörige Beispiele:

- Workshop zur Beobachtbarkeit

OPS04-BP02 Implementieren einer Anwendungstelemetrie

Anwendungstelemetrie dient als Grundlage für die Beobachtbarkeit Ihres Workloads. Die ausgegebene Telemetrie muss unbedingt umsetzbare Erkenntnisse zum Status Ihrer Anwendung und zum Erreichen sowohl technischer als auch geschäftlicher Ergebnisse liefern. Ob es um Fehlerbehebung, die Messung der Auswirkungen einer neuen Funktion oder die zuverlässige Ausrichtung auf wichtige Leistungsindikatoren (KPIs) geht – Anwendungstelemetrie liefert Informationen darüber, wie Sie Ihren Workload aufbauen, betreiben und weiterentwickeln können.

Metriken, Protokolle und Traces bilden die drei wichtigsten Säulen der Beobachtbarkeit. Sie dienen als Diagnosetools, die den Status Ihrer Anwendung beschreiben. Im Laufe der Zeit helfen sie bei der Erstellung von Baselines und der Identifizierung von Anomalien. Um sicherzustellen, dass die Überwachungsaktivitäten und die Geschäftsziele aufeinander abgestimmt sind, ist jedoch die Definition und Überwachung von wichtigen Key Performance Indicators (KPIs) entscheidend. Oft ist es leichter, Probleme anhand von Geschäfts-KPIs zu identifizieren als nur anhand von technischen Metriken.

Andere Telemetriearten, wie Real User Monitoring (RUM) und synthetische Transaktionen, ergänzen diese primären Datenquellen. RUM liefert Echtzeit-Erkenntnisse zu Benutzerinteraktionen, während synthetische Transaktionen potenzielles Benutzerverhalten simulieren und so helfen, Engpässe zu erkennen, bevor echte Benutzer darauf stoßen.

Gewünschtes Ergebnis: Sie erzielen umsetzbare Erkenntnisse zur Leistung Ihres Workloads. Diese Erkenntnisse ermöglichen es Ihnen, proaktive Entscheidungen zur Leistungsoptimierung zu treffen, eine höhere Workload-Stabilität zu erreichen, CI/CD-Prozesse zu rationalisieren und Ressourcen effektiv zu nutzen.

Typische Anti-Muster:

- Unvollständige Beobachtbarkeit: Wenn die Beobachtbarkeit nicht auf jeder Ebene des Workloads berücksichtigt wird, führt dies zu blinden Flecken, die wichtige Erkenntnisse über Systemleistung und Verhalten verschleiern können.
- Fragmentierte Datenansicht: Wenn Daten über mehrere Tools und Systeme verteilt sind, wird es schwierig, einen ganzheitlichen Überblick über den Zustand und die Leistung Ihrer Workloads zu behalten.
- Von Benutzern gemeldete Probleme: Ein Zeichen dafür, dass eine proaktive Problemerkennung durch Telemetrie und Überwachung von Geschäfts-KPIs fehlt.

Vorteile der Nutzung dieser bewährten Methode:

- Fundierte Entscheidungen: Mit Erkenntnissen aus Telemetrie und Geschäfts-KPIs können Sie datengestützte Entscheidungen treffen.
- Verbesserte betriebliche Effizienz: Datengesteuerte Ressourcennutzung führt zu Kosteneffektivität.
- Verbesserte Workload-Stabilität: Schnellere Erkennung und Lösung von Problemen führt zu einer verbesserten Verfügbarkeit.
- Optimierte CI/CD-Prozesse: Erkenntnisse aus Telemetriedaten erleichtern die Verfeinerung von Prozessen und sichern die Codebereitstellung.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Verwenden Sie AWS-Services wie Amazon CloudWatch und AWS X-Ray, um Anwendungstelemetrie für Ihren Workload zu implementieren. Amazon CloudWatch bietet eine umfassende Suite von Überwachungstools, mit denen Sie Ihre Ressourcen und Anwendungen in AWS und On-Premises beobachten können. Der Service erfasst, verfolgt und analysiert Metriken, konsolidiert und überwacht Protokolldaten und reagiert auf Änderungen in Ihren Ressourcen, wodurch Sie besser verstehen, wie Ihr Workload funktioniert. Gleichzeitig können Sie mit AWS X-Ray Ihre Anwendungen verfolgen, analysieren und debuggen, um ein umfassendes Verständnis des Verhaltens Ihrer Workloads

zu entwickeln. Mit Features wie Service-Maps, Latenzverteilungen und Trace-Zeitplänen liefert AWS X-Ray Ihnen Erkenntnisse zur Leistung Ihres Workloads und zu den Schwachstellen, die ihn beeinträchtigen.

Implementierungsschritte

1. Identifizieren Sie, welche Daten erfasst werden sollen: Ermitteln Sie die wichtigsten Metriken, Protokolle und Traces, die aussagekräftige Erkenntnisse zu Zustand, Leistung und Verhalten Ihres Workloads bieten.
2. Bereitstellen des CloudWatch Agents: Der CloudWatch-Agent ist maßgeblich an der Beschaffung von System- und Anwendungsmetriken und Protokollen von Ihrem Workload und der zugrunde liegenden Infrastruktur beteiligt. Der CloudWatch-Agent kann auch verwendet werden, um OpenTelemetry- oder X-Ray-Traces zu erfassen und an X-Ray zu senden.
3. Implementieren Sie eine Anomalieerkennung für Protokolle und Metriken: Verwenden Sie die CloudWatch Logs-Anomalieerkennung und die CloudWatch Erkennung von Metrikanomalien, um ungewöhnliche Aktivitäten im Betrieb Ihrer Anwendung automatisch zu identifizieren. Diese Tools verwenden Machine-Learning-Algorithmen, um Anomalien zu erkennen und sie zu melden. Dadurch werden Ihre Überwachungsfunktionen verbessert und die Reaktionszeit bei potenziellen Störungen oder Sicherheitsbedrohungen verkürzt. Richten Sie diese Features ein, um den Zustand und die Sicherheit von Anwendungen proaktiv zu verwalten.
4. Schützen Sie vertrauliche Protokolldaten: Verwenden Sie den Amazon CloudWatch Logs Datenschutz, um vertrauliche Informationen in Ihren Protokollen zu maskieren. Dieses Feature trägt zur Wahrung von Datenschutz und Compliance bei, indem sensible Daten automatisch erkannt und maskiert werden, bevor auf sie zugegriffen wird. Implementieren Sie Datenmaskierung, um sensible Daten wie persönlich identifizierbare Informationen (PII) sicher zu handhaben und zu schützen.
5. Definieren und überwachen von Geschäfts-KPIs: Richten Sie benutzerdefinierte Metriken ein, die auf Ihre Geschäftsergebnisse abgestimmt sind.
6. Instrumentieren Ihrer Anwendung mit AWS X-Ray: Neben der Bereitstellung des CloudWatch-Agenten ist es wichtig, Ihre Anwendung so zu instrumentieren, dass sie Trace-Daten ausgibt. Dieser Prozess kann weitere Erkenntnisse zum Verhalten und zur Leistung Ihres Workloads liefern.
7. Standardisieren der Datenerfassung in Ihrer gesamten Anwendung: Standardisieren Sie die Datenerfassungspraktiken in Ihrer gesamten Anwendung. Einheitlichkeit hilft bei der Korrelation und Analyse von Daten und liefert einen umfassenden Überblick über das Verhalten Ihrer Anwendung.

8. Implementieren von kontoübergreifender Beobachtbarkeit: Verbessern Sie die Effizienz der Überwachung mehrerer Konten AWS-Konten mit Amazon CloudWatch kontoübergreifender Beobachtbarkeit. Mit diesem Feature können Sie Metriken, Protokolle und Alarme aus verschiedenen Konten in einer einzigen Ansicht konsolidieren, was die Verwaltung vereinfacht und die Reaktionszeiten bei identifizierten Problemen in der gesamten AWS-Umgebung der Organisation verbessert.
9. Analysieren und Nutzen von Daten: Sobald die Datenerfassung und Normalisierung abgeschlossen sind, verwenden Sie sie Amazon CloudWatch für Metriken- und Protokollanalysen sowie AWS X-Ray für Trace-Analysen. Eine solche Analyse kann wichtige Erkenntnisse über den Zustand, die Leistung und das Verhalten Ihrer Workload liefern und so Ihren Entscheidungsprozess beeinflussen.

Aufwand für den Implementierungsplan: hoch

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Definieren von Workload-KPIs
- OPS04-BP03 Implementieren von Telemetrie für Benutzeraktivitäten
- OPS04-BP04 Implementieren einer Abhängigkeitstelemetrie
- OPS04-BP05 Implementieren einer Transaktionsverfolgung

Zugehörige Dokumente:

- Bewährte Methoden zur Beobachtbarkeit für AWS
- CloudWatch-Benutzerhandbuch
- AWS X-Ray-Entwicklerhandbuch
- Instrumentieren verteilter Systeme für Einblicke in die Betriebsabläufe
- Skill-Builder-Kurs zur Beobachtbarkeit in AWS
- Neuerungen bei Amazon CloudWatch
- Neuerungen bei AWS X-Ray

Zugehörige Videos:

- AWS re:Invent 2022 – Bewährte Überwachungsmethoden bei Amazon
- AWS re:Invent 2022 – Entwicklung einer Überwachungsstrategie

Zugehörige Beispiele:

- Workshop zur Beobachtbarkeit
- AWS-Lösungsbibliothek: Anwendungsüberwachung mit Amazon CloudWatch

OPS04-BP03 Implementieren von Telemetrie für Benutzererfahrung

Ein entscheidender Erfolgsfaktor besteht darin, tiefe Einblicke in die Erfahrung Ihrer Kunden und deren Interaktionen mit Ihrer Anwendung zu gewinnen. Zwei leistungsstarke Tools, die diesem Zweck dienen, sind Real User Monitoring (RUM, Reale Benutzerüberwachung) und synthetische Transaktionen. RUM liefert Daten zu echten Benutzerinteraktionen, die ein wahrheitsgetreues Bild der Benutzerzufriedenheit vermitteln. Synthetische Transaktionen hingegen simulieren Benutzerinteraktionen und helfen Ihnen dadurch, potenzielle Probleme zu erkennen, noch bevor sie sich auf echte Benutzer auswirken.

Gewünschtes Ergebnis: Eine ganzheitliche Ansicht des Kundenerlebnisses, die proaktive Erkennung von Problemen und die Optimierung der Benutzerinteraktionen, um nahtlos digitale Erfahrungen zu ermöglichen.

Typische Anti-Muster:

- Anwendungen ohne RUM:
  - Verzögerte Problemerkennung: Ohne RUM werden Sie möglicherweise erst dann auf Leistungsengpässe oder -probleme aufmerksam, wenn sich Benutzer beschweren. Dieser reaktive Ansatz kann bei Ihren Kunden zu Unzufriedenheit führen.
  - Fehlende Einblicke in die Benutzererfahrung: Wenn Sie RUM nicht verwenden, lassen Sie wichtige Daten ungenutzt, die zeigen, wie echte Benutzer mit Ihrer Anwendung interagieren, wodurch Ihre Möglichkeiten zur Optimierung der Benutzererfahrung eingeschränkt bleiben.
- Anwendungen ohne synthetische Transaktionen:
  - Fehlende Grenzfälle: Synthetische Transaktionen helfen Ihnen dabei, Pfade und Funktionen zu testen, die von den meisten Benutzern möglicherweise nicht häufig verwendet werden, aber für bestimmte Geschäftsfunktionen von entscheidender Bedeutung sind. Ohne sie könnten mögliche Fehler bei diesen Pfaden und Funktionen unbemerkt bleiben.

- Ausbleibende Überprüfung auf Probleme bei inaktiver Anwendung: Regelmäßige synthetische Tests können Situationen simulieren, in denen echte Benutzer nicht aktiv mit Ihrer Anwendung interagieren, wodurch sichergestellt wird, dass das System immer korrekt funktioniert.

Vorteile der Nutzung dieser bewährten Methode:

- Proaktive Problemerkennung: Identifizieren und beheben Sie potenzielle Probleme, bevor sie sich auf echte Benutzer auswirken.
- Optimierte Benutzererfahrung: Kontinuierliches Feedback von RUM hilft Ihnen dabei, die allgemeine Benutzererfahrung zu verfeinern und zu verbessern.
- Erkenntnisse zur Geräte- und Browserleistung: Verstehen Sie, wie gut Ihre Anwendung auf verschiedenen Geräten und Browsern funktioniert, um weitere Optimierungen zu ermöglichen.
- Validierte Geschäftsabläufe: Regelmäßige synthetische Transaktionen stellen sicher, dass Kernfunktionen und kritische Pfade stets betriebsbereit und effizient bleiben.
- Verbesserte Anwendungsleistung: Nutzen Sie Erkenntnisse aus echten Benutzerdaten, um die Reaktionsfähigkeit und Zuverlässigkeit Ihrer Anwendungen zu verbessern.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Um RUM und synthetische Transaktionen für die Telemetrie von Benutzeraktivitäten zu nutzen, bietet AWS Ihnen Services wie Amazon CloudWatch RUM und Amazon CloudWatch Synthetics. In Verbindung mit Daten zur Benutzeraktivität bieten Metriken, Protokolle und Traces einen umfassenden Überblick über den Betriebsstatus der Anwendung und die Benutzererfahrung zugleich.

Implementierungsschritte

1. Amazon CloudWatch RUM bereitstellen: Integrieren Sie Ihre Anwendung in CloudWatch RUM, um echte Benutzerdaten zu erfassen, zu analysieren und zu präsentieren.
   a. Verwenden Sie die CloudWatch RUM-JavaScript-Bibliothek, um RUM in Ihre Anwendung zu integrieren.
   b. Richten Sie Dashboards ein, um echte Benutzerdaten zu visualisieren und zu überwachen.
2. CloudWatch Synthetics konfigurieren: Erstellen Sie Canaries oder skriptbasierte Routinen, die Benutzerinteraktionen mit Ihrer Anwendung simulieren.
   a. Definieren Sie kritische Anwendungsworkflows und -pfade.

   b. Entwerfen Sie Canaries mit CloudWatch Synthetics-Skripten, um Benutzerinteraktionen für diese Pfade zu simulieren.
   c. Planen und überwachen Sie Canaries so, dass sie in bestimmten Intervallen ausgeführt werden, und sorgen Sie so für einheitliche Leistungsprüfungen.
3. Daten analysieren und Erkenntnisse umsetzen: Nutzen Sie Daten aus RUM und synthetischen Transaktionen, um Erkenntnisse zu gewinnen und korrigierende Maßnahmen zu ergreifen, wenn Anomalien festgestellt werden. Verwenden Sie CloudWatch-Dashboards und Alarme, um auf dem Laufenden zu bleiben.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS04-BP02 Implementieren einer Anwendungstelemetrie
- OPS04-BP04 Implementieren einer Abhängigkeitstelemetrie
- OPS04-BP05 Implementieren der verteilten Nachverfolgung

Zugehörige Dokumente:

- Leitfaden zu Amazon CloudWatch RUM
- Leitfaden zu Amazon CloudWatch Synthetics

Zugehörige Videos:

- Optimize applications through end user insights with Amazon CloudWatch RUM (Optimierung von Anwendungen durch Endbenutzereinblicke mit Amazon CloudWatch RUM)
- AWS on Air ft. Real-User Monitoring for Amazon CloudWatch (AWS on Air mit RUM für Amazon CloudWatch)

Zugehörige Beispiele:

- Workshop zur Beobachtbarkeit

- Git-Repository für den Amazon CloudWatch RUM-Web-Client
- Verwenden von Amazon CloudWatch Synthetics zur Messung der Seitenladezeit

OPS04-BP04 Implementieren einer Abhängigkeitstelemetrie

Die Abhängigkeitstelemetrie ist für die Überwachung des Status und der Leistung der externen Services und Komponenten, auf die Ihr Workload angewiesen ist, unerlässlich. Sie liefert wertvolle Erkenntnisse zu Erreichbarkeit, Timeouts und anderen kritischen Ereignissen im Zusammenhang mit Abhängigkeiten wie DNS, Datenbanken oder APIs von Drittanbietern. Wenn Sie Ihre Anwendung so instrumentieren, dass sie Metriken, Protokolle und Traces zu diesen Abhängigkeiten ausgibt, gewinnen Sie ein besseres Verständnis von potenziellen Engpässen, Leistungsproblemen oder Ausfällen, die sich auf Ihren Workload auswirken könnten.

Gewünschtes Ergebnis: Die Abhängigkeiten, auf die Ihr Workload angewiesen ist, funktionieren erwartungsgemäß, sodass Sie Probleme proaktiv angehen und eine optimale Workload-Leistung gewährleisten können.

Typische Anti-Muster:

- Nichtbeachtung externer Abhängigkeiten: Sich nur auf interne Anwendungsmetriken konzentrieren und dabei Metriken im Zusammenhang mit externen Abhängigkeiten außer Acht lassen.
- Mangelnde proaktive Überwachung: warten, bis Probleme auftreten, statt den Status und die Leistung von Abhängigkeiten kontinuierlich zu überwachen.
- Isolierte Überwachung: Einsatz mehrerer, unterschiedlicher Überwachungstools, was zu fragmentierten und inkonsistenten Ansichten bezüglich des Überwachungsstatus führen kann.

Vorteile der Nutzung dieser bewährten Methode:

- Verbesserte Zuverlässigkeit der Workloads: Indem sichergestellt wird, dass externe Abhängigkeiten kontinuierlich verfügbar sind und optimal funktionieren.
- Schnellere Problemerkennung und -lösung: Proaktives Identifizieren und Beheben von Problemen mit Abhängigkeiten, bevor sie sich auf den Workload auswirken.
- Umfassender Überblick: Erhalt eines ganzheitlichen Überblicks über interne und externe Komponenten, die den Workload-Status beeinflussen.
- Verbesserte Skalierbarkeit der Workloads: Verständnis der Skalierbarkeitsgrenzen und Leistungsmerkmale externer Abhängigkeiten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Implementieren Sie die Abhängigkeitstelemetrie, indem Sie zunächst die Services, Infrastrukturen und Prozesse identifizieren, von denen Ihr Workload abhängt. Quantifizieren Sie, wie gute Bedingungen aussehen, wenn diese Abhängigkeiten wie erwartet funktionieren, und bestimmen Sie dann, welche Daten zum Messen dieser Bedingungen benötigt werden. Mit diesen Informationen können Sie Dashboards und Warnmeldungen erstellen, die Ihren Operations-Teams Erkenntnisse zum Status dieser Abhängigkeiten liefern. Verwenden Sie AWS-Tools, um die Auswirkungen zu ermitteln und zu quantifizieren, wenn Abhängigkeiten nicht die gewünschten Resultate zeigen. Überarbeiten Sie Ihre Strategie kontinuierlich, um Änderungen der Prioritäten, Ziele und gewonnenen Erkenntnisse Rechnung zu tragen.

Implementierungsschritte

So implementieren Sie die Abhängigkeitstelemetrie auf effiziente Weise:

1. Identifizieren von externen Abhängigkeiten: Arbeiten Sie mit Stakeholdern zusammen, um die externen Abhängigkeiten zu ermitteln, von denen Ihr Workload abhängt. Zu externen Abhängigkeiten zählen Services wie externe Datenbanken, APIs von Drittanbietern, Netzwerkverbindungsrouten zu anderen Umgebungen und DNS-Services. Der erste Schritt zu einer effektiven Abhängigkeitstelemetrie besteht darin, auf ganzer Ebene zu verstehen, welche diese Abhängigkeiten sind.
2. Entwicklung einer Überwachungsstrategie: Sobald Sie sich ein klares Bild von Ihren externen Abhängigkeiten verschafft haben, entwerfen Sie eine darauf zugeschnittene Überwachungsstrategie. Dazu müssen Sie die Wichtigkeit jeder Abhängigkeit, ihr erwartetes Verhalten und alle damit verbundenen Service Level Agreements oder -Ziele verstehen. Richten Sie proaktive Warnmeldungen ein, die Sie über Statusänderungen oder Leistungsabweichungen informieren.
3. Netzwerküberwachung verwenden: Verwenden Sie Internet Monitor und Network Monitor, die umfassende Einblicke in die globalen Internet- und Netzwerkbedingungen bieten. Diese Tools helfen Ihnen dabei, Ausfälle, Unterbrechungen oder Leistungseinbußen, die sich auf Ihre externen Abhängigkeiten auswirken, zu verstehen und darauf zu reagieren.
4. Informiert bleiben mit dem AWS Health Dashboard: Dieses Dashboard stellt Warnmeldungen bereit und empfiehlt Abhilfemaßnahmen, wenn in AWS Ereignisse eintreten, die möglicherweise Ihre Services betreffen.

   a. Überwachen Sie AWS Health-Ereignisse mithilfe von Amazon EventBridge-Regeln oder integrieren Sie sie programmgesteuert in die AWS Health API, um Aktionen zu automatisieren, wenn Sie AWS Health-Ereignisse erhalten. Dies können allgemeine Aktionen sein, z. B. das Senden aller geplanten Lebenszyklus-Ereignisnachrichten an eine Chat-Oberfläche, oder spezifische Aktionen, wie das Initiieren eines Workflows in einem IT-Servicemanagement-Tool.
   b. Wenn Sie AWS Organizations verwenden, aggregieren Sie AWS Health-Ereignisse kontoübergreifend.
5. Instrumentieren Ihrer Anwendung mit AWS X-Ray: AWS X-Ray bietet Einblicke in die Leistung von Anwendungen und ihren zugrunde liegenden Abhängigkeiten. Verfolgen Sie Anfragen von Anfang bis Ende nach, um Engpässe oder Ausfälle bei den externen Services oder Komponenten zu identifizieren, auf die sich Ihre Anwendung stützt.
6. Verwendung von Amazon DevOps Guru: Dieser Machine-Learning-gestützte Service identifiziert operative Probleme, prognostiziert das Auftreten kritischer Probleme und empfiehlt spezifische Maßnahmen. Dadurch ist er von unschätzbarem Wert, wenn es darum geht, Erkenntnisse zu Abhängigkeiten zu gewinnen und festzustellen, dass sie nicht die Ursache von operativen Problemen sind.
7. Regelmäßige Überwachung: Überwachen Sie kontinuierlich alle Metriken und Protokolle, die sich auf externe Abhängigkeiten beziehen. Richten Sie Warnmeldungen ein, die Sie über unerwartetes Verhalten oder Leistungseinbußen informieren.
8. Validierung nach Änderungen: Überprüfen Sie nach jeder Aktualisierung oder Änderung einer externen Abhängigkeit deren Leistung und Ausrichtung auf die Anforderungen Ihrer Anwendung.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Definieren von Workload-KPIs
- OPS04-BP02 Implementieren einer Anwendungstelemetrie
- OPS04-BP03 Implementieren von Telemetrie für Benutzeraktivitäten
- OPS04-BP05 Implementieren einer Transaktionsverfolgung
- OP08-BP04 Erstellen umsetzbarer Warnmeldungen

Zugehörige Dokumente:

- Amazon Personalize AWS Health Dashboard – Benutzerhandbuch
- AWS Internet Monitor – Benutzerhandbuch
- AWS X-Ray-Entwicklerhandbuch
- AWS DevOps Guru-Benutzerhandbuch

Zugehörige Videos:

- Wie sich Internetprobleme auf die Leistung von Apps auswirken
- Einführung in Amazon DevOps Guru
- Verwaltung von Ereignissen im Ressourcenlebenszyklus im großen Maßstab mit AWS Health

Zugehörige Beispiele:

- Operative Erkenntnisse gewinnen mit AIOps und Amazon DevOps Guru
- AWS Health Aware
- Verwenden von tagbasierter Filterung zur Verwaltung von AWS Health Überwachung und Warnmeldungen im großen Maßstab

OPS04-BP05 Implementieren der verteilten Nachverfolgung

Die verteilte Nachverfolgung bietet eine Möglichkeit, Anfragen zu überwachen und zu visualisieren, während sie verschiedene Komponenten eines verteilten Systems durchlaufen. Durch die Erfassung von Trace-Daten aus mehreren Quellen und deren Analyse in einer zentralen Ansicht können Teams besser verstehen, wie Anfragen ablaufen, wo Engpässe bestehen und worauf Optimierungsbemühungen abzielen sollten.

Gewünschtes Ergebnis: Sie verschaffen sich einen ganzheitlichen Überblick über die Anfragen, die durch Ihr verteiltes System fließen, und ermöglichen so präzises Debugging, optimierte Leistung und verbesserte Benutzererfahrungen.

Typische Anti-Muster:

- Inkonsistente Instrumentierung: Nicht alle Services in einem verteilten System sind für die Nachverfolgung instrumentiert.
- Latenz wird ignoriert: Sie konzentrieren sich nur auf Fehler und berücksichtigen nicht die Latenz oder allmähliche Leistungseinbußen.

Vorteile der Nutzung dieser bewährten Methode:

- Umfassender Systemüberblick: Visualisierung des gesamten Anfragenverlaufs, vom Eingang bis zum Ausgang.
- Verbessertes Debugging: Schnelle Identifizierung von Fehlern oder Leistungsproblemen.
- Verbessertes Benutzererlebnis: Überwachung und Optimierung auf der Grundlage von tatsächlichen Benutzerdaten, um sicherzustellen, dass das System den realen Anforderungen entspricht.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Identifizieren Sie zunächst alle Elemente Ihres Workloads, für die eine Instrumentierung erforderlich ist. Sobald alle Komponenten berücksichtigt sind, können Sie Tools wie AWS X-Ray und OpenTelemetry nutzen, um Trace-Daten für die Analyse mit Tools wie X-Ray und Amazon CloudWatch ServiceLens Map zu erfassen. Nehmen Sie regelmäßig an Besprechungen mit Entwicklern teil und ergänzen Sie diese Diskussionen mit Tools wie Amazon DevOps Guru, X-Ray Analytics und X-Ray Insights, um tiefere Erkenntnisse zu gewinnen. Richten Sie Warnmeldungen anhand von Trace-Daten ein, damit Sie benachrichtigt werden, wenn die im Workload-Überwachungsplan definierten Ergebnisse gefährdet sind.

Implementierungsschritte

So implementieren Sie die verteilte Nachverfolgung auf effektive Weise:

1. Nutzen Sie AWS X-Ray: Integrieren Sie X-Ray in Ihre Anwendung, um Erkenntnisse zu ihrem Verhalten zu gewinnen, ihre Leistung zu verstehen und Engpässe zu lokalisieren. Nutzen Sie X-Ray Insights für die automatische Trace-Analyse.
2. Instrumentieren Sie Ihre Services: Stellen Sie sicher, dass jeder Service, jede AWS Lambda-Funktion und jede EC2-Instance,Trace-Daten sendet. Je mehr Services Sie instrumentieren, desto klarer wird die Gesamtansicht.
3. Integrieren Sie CloudWatch Real User Monitoring und synthetische Überwachung: Integrieren Sie Real User Monitoring (RUM) und synthetische Überwachung mit X-Ray. Auf diese Weise können reale Benutzererfahrungen erfasst und Benutzerinteraktionen simuliert werden, um potenzielle Probleme zu identifizieren.
4. Nutzen Sie den CloudWatch Agent: Der Agent kann Traces entweder von X-Ray oder von OpenTelemetry senden, wodurch die Tiefe der gewonnenen Erkenntnisse verbessert wird.

5. Verwenden Sie Amazon DevOps Guru: DevOps Guru verwendet Daten von X-Ray, CloudWatch, AWS Config und AWS CloudTrail, um umsetzbare Empfehlungen zu liefern.
6. Analysieren Sie Traces: Überprüfen Sie die Trace-Daten regelmäßig, um Muster, Anomalien oder Engpässe zu erkennen, die sich auf die Leistung Ihrer Anwendung auswirken könnten.
7. Richten Sie Benachrichtigungen ein: Konfigurieren Sie Alarme in CloudWatch für ungewöhnliche Muster oder längere Latenzen und ermöglichen Sie dadurch eine proaktive Problembehebung.
8. Kontinuierliche Verbesserung: Überarbeiten Sie Ihre Tracing-Strategie, wenn Services hinzugefügt oder geändert werden, um alle relevanten Datenpunkte zu erfassen.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS04-BP02 Implementieren einer Anwendungstelemetrie
- OPS04-BP03 Implementieren von Telemetrie für Benutzererfahrung
- OPS04-BP04 Implementieren einer Abhängigkeitstelemetrie

Zugehörige Dokumente:

- AWS X-Ray-Entwicklerhandbuch
- Amazon CloudWatch-Benutzerhandbuch für Kundendienstmitarbeiter
- Amazon DevOps Guru-Benutzerhandbuch

Zugehörige Videos:

- Use AWS X-Ray Insights (Nutzung von AWS X-Ray-Erkenntnissen)
- AWS on Air ft. Observability: Amazon CloudWatch and AWS X-Ray (AWS on Air mit Beobachtbarkeit: Amazon CloudWatch und AWS X-Ray)

Zugehörige Beispiele:

- Instrumentierung Ihrer Anwendung mit AWS X-Ray

Design für den Betrieb

Verwenden Sie Strategien, die die Übertragung von Änderungen auf die Produktionsumgebung verbessern und Faktorwechsel, schnelles Feedback zur Qualität sowie eine schnelle Fehlerbehebung ermöglichen. Dadurch fließen nützliche Änderungen schneller in die Produktion ein und es treten bei der Bereitstellung weniger Probleme auf. Zudem können Probleme, die durch Bereitstellungsaktivitäten verursacht werden, schnell aufgespürt und gelöst werden.

In AWS können Sie sämtliche Workloads (Anwendungen, Infrastruktur, Richtlinien, Governance und Betrieb) als Code einsehen. Alles kann in Code definiert und mittels Code aktualisiert werden. Das bedeutet, dass Sie bei jedem Element Ihres Stacks die gleiche technischen Vorgehensweise wie bei Anwendungscode anwenden können.

Bewährte Methoden

- OPS05-BP01 Verwendung einer Versionskontrolle
- OPS05-BP02 Testen und Validieren von Änderungen
- OPS05-BP03 Einsatz von Systemen zur Konfigurationsverwaltung
- OPS05-BP04 Einsatz von Systemen zur Build- und Bereitstellungsverwaltung.
- OPS05-BP05 Durchführen der Patch-Verwaltung
- OPS05-BP06 Gemeinsame Design-Standards
- OPS05-BP07 Implementieren von Verfahren zur Verbesserung der Codequalität
- OPS05-BP08 Verwenden mehrerer Umgebungen
- OPS05-BP09 Häufige, kleine, reversible Änderungen vornehmen
- OPS05-BP10 Vollständige Automatisierung von Integration und Bereitstellung

OPS05-BP01 Verwendung einer Versionskontrolle

Aktivieren Sie die Verfolgung von Änderungen und Releases mithilfe einer Versionskontrolle.

Viele AWS-Services bieten Versionskontrollfunktionen. Verwenden Sie ein Revisions- oder Quellcodeverwaltungssystem wie AWS CodeCommit, um Code und andere Artefakte zu verwalten, z. B. versionsgesteuerte AWS CloudFormation -Vorlagen Ihrer Infrastruktur.

Gewünschtes Ergebnis: Ihre Teams arbeiten gemeinsam am Code. Bei der Zusammenführung ist der Code einheitlich und es gehen keine Änderungen verloren. Fehler können durch korrekte Versionierung leicht behoben werden.

Typische Anti-Muster:

- Sie haben Ihren Code auf Ihrer Workstation entwickelt und gespeichert. Es ist ein Speicherfehler bei der Workstation aufgetreten, der nicht rückgängig gemacht werden kann, und Sie haben den Code verloren.
- Nachdem Sie den vorhandenen Code mit Ihren Änderungen überschrieben haben, starten Sie Ihre Anwendung neu, doch sie funktioniert nicht mehr. Sie können die Änderung nicht rückgängig machen.
- Sie arbeiten an einer Berichtsdatei, deshalb ist sie für alle anderen schreibgeschützt, doch ein anderer Benutzer möchte sie bearbeiten. Der Benutzer kontaktiert Sie und bittet darum, die Arbeit daran zu beenden, damit er seine Aufgabe erledigen kann.
- Ihr Forschungsteam arbeitet an einer detaillierten Analyse, die Ihre zukünftige Arbeit prägt. Jemand hat versehentlich seine Einkaufsliste über den endgültigen Bericht gespeichert. Sie können die Änderung nicht rückgängig machen und müssen den Bericht neu erstellen.

Vorteile der Nutzung dieser bewährten Methode: Durch die Verwendung von Versionskontrollfunktionen können Sie problemlos auf einen bekanntermaßen funktionierenden Status bzw. frühere Versionen zurücksetzen und so das Risiko von verlorenen Assets begrenzen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Bewahren Sie Ressourcen in Repositorys mit Versionskontrolle auf. Dies ermöglicht die Nachvollziehung von Änderungen, die Bereitstellung neuer Versionen, die Erkennung von Änderungen an bestehenden Versionen und die Rückkehr zu vorherigen Versionen (zum Beispiel bei einem Fehler die Zurücksetzung auf einen bekanntermaßen funktionierenden Zustand). Integrieren Sie die Versionskontrollfunktionen Ihrer Konfigurationsverwaltungssysteme in Ihre Verfahren.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP04 Einsatz von Systemen zur Build- und Bereitstellungsverwaltung.

Zugehörige Dokumente:

- Was ist AWS CodeCommit?

Zugehörige Videos:

- Einführung in AWS CodeCommit

OPS05-BP02 Testen und Validieren von Änderungen

Jede eingesetzte Änderung muss getestet werden, um Fehler in der Produktion zu vermeiden. Diese bewährte Methode konzentriert sich auf das Testen von Änderungen von der Versionskontrolle bis zur Erstellung von Artefakten. Neben Änderungen am Anwendungscode sollten die Tests auch die Infrastruktur, die Konfiguration, die Sicherheitskontrollen und die Betriebsverfahren umfassen. Es gibt viele Formen des Testens, von Tests der Einheiten bis hin zur Softwarekomponentenanalyse (SCA). Wenn Tests im Softwareintegrations- und -bereitstellungsprozess weiter nach links verschoben werden, führt dies zu einer höheren Gewissheit der Artefaktqualität.

Ihr Unternehmen muss Teststandards für alle Software-Artefakte entwickeln. Automatisierte Tests verringern den Arbeitsaufwand und vermeiden manuelle Testfehler. In einigen Fällen können aber auch manuelle Tests notwendig sein. Entwickler müssen Zugang zu automatisierten Testergebnissen haben, um Feedback-Schleifen zur Verbesserung der Softwarequalität zu schaffen.

Gewünschtes Ergebnis: Ihre Softwareänderungen werden vor der Bereitstellung getestet. Die Entwickler haben Zugang zu den Testergebnissen und den Validierungen. Ihre Organisation hat einen Teststandard, der für alle Softwareänderungen gilt.

Typische Anti-Muster:

- Sie stellen eine neue Softwareänderung ohne jegliche Tests bereit. Sie wird in der Produktion nicht ausgeführt, was zu einem Ausfall führt.
- Es werden neue Sicherheitsgruppen mit AWS CloudFormation eingesetzt, ohne in einer Vorproduktionsumgebung getestet zu werden. Durch die Sicherheitsgruppen ist Ihre App für Ihre Kunden unerreichbar.
- Eine Methode wurde geändert, aber es gibt keine Tests der Einheiten. Die Software läuft nicht, wenn sie in der Produktion eingesetzt wird.

Vorteile der Nutzung dieser bewährten Methode: Die Fehlerquote von Änderungen bei Softwarebereitstellungen wird reduziert. Die Qualität der Software wird verbessert. Die Entwickler haben ein größeres Bewusstsein für die Lebensfähigkeit ihres Codes. Sicherheitsrichtlinien können zuverlässig eingeführt werden, um die Compliance des Unternehmens zu unterstützen.

Infrastrukturänderungen, wie automatische Aktualisierungen der Skalierungsrichtlinien, werden im Voraus getestet, um den Anforderungen des Datenverkehrs gerecht zu werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Alle Änderungen, vom Anwendungscode bis zur Infrastruktur, werden im Rahmen Ihrer kontinuierlichen Integrationspraxis getestet. Die Testergebnisse werden veröffentlicht, damit die Entwickler schnelles Feedback erhalten. Ihre Organisation hat einen Teststandard, den alle Änderungen erfüllen müssen.

Nutzen Sie die Leistungsfähigkeit generativer KI mit Amazon Q Developer, um die Produktivität und Codequalität von Entwicklern zu verbessern. Amazon Q Developer umfasst die Generierung von Codevorschlägen (basierend auf großen Sprachmodellen), die Erstellung von Komponententests (einschließlich Randbedingungen) und Verbesserungen der Codesicherheit durch die Erkennung und Behebung von Sicherheitsschwachstellen.

Kundenbeispiel

Als Teil der kontinuierlichen Integrationspipeline führt AnyCompany Retail verschiedene Arten von Tests für alle Software-Artefakte durch. Sie praktizieren eine testgesteuerte Entwicklung, sodass die gesamte Software über Tests von Einheiten verfügt. Sobald das Artefakt erstellt ist, führen sie End-to-End-Tests durch. Nach Abschluss dieser ersten Testrunde führen sie einen statischen Anwendungssicherheitsscan durch, bei dem nach bekannten Schwachstellen gesucht wird. Die Entwickler erhalten Meldungen, sobald die einzelnen Prüfpunkte durchlaufen wurden. Sobald alle Tests abgeschlossen wurden, wird der Software-Artefakt in einem Artefakt-Repository gespeichert.

Implementierungsschritte

1. Arbeiten Sie mit den Beteiligten in Ihrem Unternehmen zusammen, um einen Teststandard für Software-Artefakte zu entwickeln. Welche Standardtests sollten alle Artefakte bestehen? Gibt es Compliance- oder Governance-Anforderungen, die bei der Testabdeckung berücksichtigt werden müssen? Müssen Sie die Qualität des Codes testen? Wer muss informiert werden, sobald die Tests abgeschlossen sind?
    1. Die AWS Deployment Pipeline Reference Architecture enthält eine maßgebliche Liste von Testtypen, die als Teil einer Integrationspipeline an Software-Artefakten durchgeführt werden können.

2. Instrumentieren Sie Ihre Anwendung mit den erforderlichen Tests auf der Grundlage Ihres Software-Teststandards. Jeder Testreihe sollte in weniger als zehn Minuten abgeschlossen sein. Tests sollten im Rahmen einer Integrationspipeline durchgeführt werden.
   a. Verwenden Sie Amazon Q Developer, ein generatives KI-Tool, mit dem Sie Komponententestfälle (einschließlich Randbedingungen) erstellen, Funktionen mithilfe von Code und Kommentaren generieren und bekannte Algorithmen implementieren können.
   b. Verwenden Sie Amazon CodeGuru Reviewer, Ihren Anwendungscode auf Fehler zu prüfen.
   c. Mithilfe von AWS CodeBuild können Sie Tests auf Software-Artefakten durchführen.
   d. AWS CodePipeline kann Ihre Softwaretest in eine Pipeline orchestrieren.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP01 Verwendung einer Versionskontrolle
- OPS05-BP06 Gemeinsame Design-Standards
- OPS05-BP07 Implementieren von Verfahren zur Verbesserung der Codequalität
- OPS05-BP10 Vollständige Automatisierung von Integration und Bereitstellung

Zugehörige Dokumente:

- Einführung eines testgesteuerten Entwicklungsansatzes
- Beschleunigen Ihres Softwareentwicklungszyklus mit Amazon Q
- Amazon Q Developer, jetzt allgemein verfügbar, enthält eine Vorschau auf neue Funktionen, mit denen das Entwicklererlebnis neu gestaltet werden kann
- Der ultimative Spickzettel für die Verwendung von Amazon Q Developer in Ihrer IDE
- Shift-Left-Workload, Nutzung von KI für die Testerstellung
- Amazon Q Developer Center
- 10 Methoden für eine schnellere Entwicklung von Anwendungen mit Amazon CodeWhisperer
- Ein Blick über die Codeabdeckung hinaus mit Amazon CodeWhisperer
- Bewährte Methoden für Prompt-Engineering mit Amazon CodeWhisperer
- Automatisierte AWS CloudFormation-Testpipeline mit TaskCat und CodePipeline

- Erstellen einer End-to-End-AWS-DevSecOps-CI/CD-Pipeline mit Open-Source-SCA-, -SAST- und -DAST-Tools
- Erste Schritte beim Testen von Serverless-Anwendungen
- Meine CI/CD-Pipeline ist mein Release Captain
- Durchführung von Continuous Integration und Continuous Delivery in AWS – Whitepaper

Zugehörige Videos:

- Implementieren einer API mit dem Amazon Q Developer-Agenten für Softwareentwicklung
- Installation, Konfiguration und Verwendung von Amazon Q Developer mit JetBrains-IDEs (Anleitung)
- Beherrschung der Kunst von Amazon CodeWhisperer – YouTube-Playlist
- AWS re:Invent 2020 – Testbare Infrastruktur: Integrationstests auf AWS
- AWS Summit ANZ 2021 – Vorantreiben einer „Test-First“-Strategie mit CDK und testgesteuerter Entwicklung
- Testen Ihrer Infrastruktur as Code mit AWS CDK

Zugehörige Ressourcen:

- Erstellen von Anwendungen mit generativer KI mit Amazon CodeWhisperer
- Amazon CodeWhisperer-Workshop
- Referenzarchitektur für AWS-Bereitstellungs-Pipelines – Anwendung
- AWS Kubernetes DevSecOps Pipeline
- Richtlinie als Code – Workshop – Testgesteuerte Entwicklung
- Tests von Einheiten für eine Node.js-Anwendung aus GitHub mithilfe von AWS CodeBuild
- Serverspec für die testgesteuerte Entwicklung von Infrastrukturcode verwenden

Zugehörige Services:

- Amazon Q Developer
- Amazon CodeGuru Reviewer
- AWS CodeBuild

- AWS CodePipeline

OPS05-BP03 Einsatz von Systemen zur Konfigurationsverwaltung

Verwenden Sie Systeme zur Konfigurationsverwaltung, um Änderungen vorzunehmen und zu verfolgen. Diese Systeme reduzieren Fehler aufgrund von manuellen Prozessen und verringern den Testaufwand.

Bei der statischen Konfigurationsverwaltung werden Werte festgelegt, wenn eine Ressource initialisiert wird, die erwartungsgemäß während der Lebensdauer der Ressource konsistent bleibt. Einige Beispiele sind die Konfiguration eines Web- oder Anwendungsservers auf einer Instance oder die Definition der Konfiguration eines AWS-Service innerhalb der AWS Management Console oder durch die AWS CLI.

Bei der dynamischen Konfigurationsverwaltung werden bei der Initialisierung Werte festgelegt, die sich während der Lebensdauer einer Ressource ändern können oder voraussichtlich ändern werden. So können Sie zum Beispiel durch eine Konfigurationsänderung eine Funktion in Ihrem Code aktivieren oder während eines Vorfalls den Detaillierungsgrad des Protokolls ändern, um mehr Daten zu erfassen, und dann nach dem Vorfall wieder zum Ursprungswert zurückkehren, um unnötige Protokolle und damit verbundene Kosten zu vermeiden.

In AWS können Sie AWS Config zur kontinuierlichen Überwachung Ihrer AWS-Ressourcenkonfigurationen über Konten und Regionen hinweg verwenden. So können Sie den Konfigurationsverlauf besser verfolgen, nachvollziehen, wie sich eine Konfigurationsänderung auf andere Ressourcen auswirkt, und sie im Hinblick auf die erwarteten oder gewünschten Konfigurationen mithilfe von AWS-Config-Regeln und AWS Config Conformance Packs prüfen.

Wenn Sie dynamische Konfigurationen in Ihren Anwendungen haben, die auf Amazon EC2-Instances, AWS Lambda, Containern, Mobilfunkanwendungen oder IoT-Geräten ausgeführt werden, können Sie AWS AppConfig nutzen, um sie in Ihren Umgebungen zu konfigurieren, zu validieren, bereitzustellen und zu überwachen.

In AWS können Sie CI/CD-Pipelines (Continuous Integration/Continuous Deployment) unter Verwendung von Services wie den AWS Developer Tools erstellen (Beispiel: AWS CodeCommit, AWS CodeBuild, AWS CodePipeline, AWS CodeDeployund AWS CodeStar).

Gewünschtes Ergebnis: Sie konfigurieren, validieren und implementieren als Teil Ihrer CI/CD-Pipeline (Continuous Integration, Continuous Delivery). Sie überwachen, um zu überprüfen, ob

die Konfigurationen korrekt sind. Dadurch werden die Auswirkungen auf Endbenutzer und Kunden minimiert.

Typische Anti-Muster:

- Sie aktualisieren die Konfigurationen aller Webserver manuell und eine Reihe von Servern reagiert aufgrund von Updatefehlern nicht mehr.
- Sie aktualisieren Ihre Anwendungsserver mehrere Stunden lang auf manuelle Weise. Die Inkonsistenz der Konfiguration während der Änderung führt zu unerwarteten Verhaltensweisen.
- Jemand hat Ihre Sicherheitsgruppen aktualisiert und auf Ihre Webserver kann nicht mehr zugegriffen werden. Sie wissen nicht, was geändert wurde, und verbringen viel Zeit mit der Suche nach dem Problem – die Zeit bis zur Wiederherstellung nimmt zu.
- Sie übertragen eine Vorproduktionskonfiguration ohne Validierung über CI/CD in die Produktion. Sie setzen Benutzer und Kunden falschen Daten und Services aus.

Vorteile der Nutzung dieser bewährten Methode: Die Einführung von Konfigurationsverwaltungssystemen reduziert den Aufwand für die Durchführung und Nachverfolgung von Änderungen sowie die Häufigkeit der durch manuelle Verfahren verursachten Fehler. Konfigurationsverwaltungssysteme liefern Garantien in Bezug auf Governance, Compliance und regulatorische Anforderungen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Konfigurationsverwaltungssysteme werden verwendet, um Änderungen an Anwendungs- und Umgebungskonfigurationen zu verfolgen und zu implementieren. Konfigurationsmanagementsysteme werden auch eingesetzt, um Fehler zu reduzieren, die durch manuelle Prozesse verursacht werden, Konfigurationsänderungen wiederholbar und überprüfbar zu machen und den Aufwand zu reduzieren.

Implementierungsschritte

1. Identifizieren Sie die Verantwortlichen der Konfiguration.
   a. Informieren Sie die Verantwortlichen der Konfigurationen über alle Compliance-, Governance- oder regulatorischen Anforderungen.
2. Identifizieren Sie Konfigurationselemente und Leistungen.
   a. Konfigurationselemente sind alle Anwendungs- und Umgebungskonfigurationen, die von einer Bereitstellung innerhalb Ihrer CI/CD-Pipeline betroffen sind.

b. Zu den Leistungen gehören Erfolgskriterien, Validierung und was überwacht werden muss.

3. Wählen Sie Tools für die Konfigurationsverwaltung basierend auf Ihren Geschäftsanforderungen und Ihrer Bereitstellungspipeline aus.
4. Ziehen Sie für signifikante Konfigurationsänderungen gewichtete Bereitstellungen wie Canary-Bereitstellungen in Betracht, um die Auswirkungen falscher Konfigurationen zu minimieren.
5. Integrieren Sie Ihre Konfigurationsverwaltung in Ihre CI/CD-Pipeline.
6. Bestätigen Sie alle übermittelten Änderungen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS06-BP01 Einkalkulieren nicht erfolgreicher Änderungen
- OPS06-BP02 Testbereitstellungen
- OPS06-BP03 Einsetzen sicherer Bereitstellungsstrategien
- OPS06-BP04 Automatisieren von Tests und Rollback

Zugehörige Dokumente:

- AWS Control Tower
- Landing Zone Accelerator in AWS
- AWS Config
- Was ist AWS Config?
- AWS AppConfig
- Was ist AWS CloudFormation?
- AWS Developer Tools

Zugehörige Videos:

- AWS re:Invent 2022 - Proactive governance and compliance for AWS workloads (AWS re:Invent 2022 – Proaktive Governance und Compliance für AWS-Workloads)
- AWS re:Invent 2020: Achieve compliance as code using AWS Config (AWS re:Invent 2020: Mit AWS Config Compliance als Code erzielen)

- Manage and Deploy Application Configurations with AWS AppConfig (Verwaltung und Bereitstellung von Anwendungskonfigurationen mit AWS AppConfig)

OPS05-BP04 Einsatz von Systemen zur Build- und Bereitstellungsverwaltung.

Verwenden Sie Systeme zur Build- und Bereitstellungsverwaltung. Diese Systeme reduzieren Fehler aufgrund von manuellen Prozessen und verringern den Testaufwand.

In AWS können Sie CI/CD-Pipelines (Continuous Integration/Continuous Deployment) unter Verwendung von Services wie den AWS Developer Tools nutzen (z. B. AWS CodeCommit, AWS CodeBuild, AWS CodePipeline, AWS CodeDeployund AWS CodeStar).

Gewünschtes Ergebnis: Ihre Systeme zur Build- und Bereitstellungsverwaltung unterstützen das Continuous Integration Continuous Delivery (CI/CD)-System Ihrer Organisation, das Funktionen zur Automatisierung sicherer Rollouts mit den richtigen Konfigurationen bietet.

Typische Anti-Muster:

- Nachdem Sie Ihren Code auf Ihrem Entwicklungssystem kompiliert haben, kopieren Sie die ausführbare Datei auf Ihre Produktionssysteme und sie kann nicht gestartet werden. Die lokalen Protokolldateien zeigen an, dass die Ausführung aufgrund fehlender Abhängigkeiten fehlgeschlagen ist.
- Sie erstellen Ihre Anwendung erfolgreich mit neuen Funktionen in Ihrer Entwicklungsumgebung und stellen den Code der Quality Assurance (QA, Qualitätsprüfung) zur Verfügung. Die QA-Prüfung schlägt fehl, da statische Komponenten fehlen.
- Am Freitag haben Sie Ihre Anwendung nach großem Aufwand manuell in Ihrer Entwicklungsumgebung erstellt, einschließlich der neu geschriebenen Funktionen. Am Montag können Sie die Schritte, mit denen Sie Ihre Anwendung erfolgreich erstellen konnten, nicht wiederholen.
- Sie führen die Tests durch, die Sie für den neuen Release erstellt haben. Sie verbringen die nächste Woche damit, eine Testumgebung einzurichten und alle vorhandenen Integrationstests durchzuführen, gefolgt von den Leistungstests. Der neue Code bewirkt eine inakzeptable Leistungsbeeinträchtigung und muss neu entwickelt und dann erneut getestet werden.

Vorteile der Nutzung dieser bewährten Methode: Mithilfe von Mechanismen zur Verwaltung von Erstellungs- und Bereitstellungsaktivitäten reduzieren Sie den Aufwand für wiederholte Aufgaben,

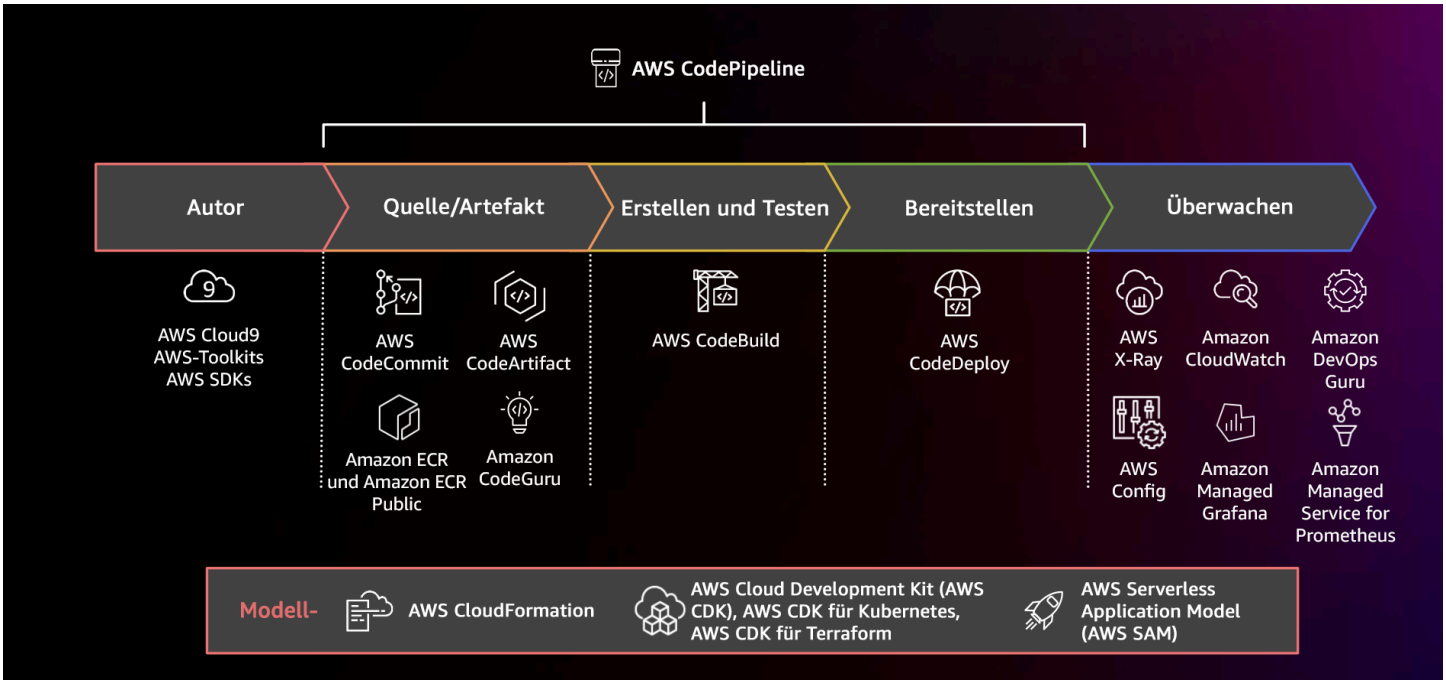
verschaffen Ihren Teammitgliedern die Zeit, sich auf ihre wichtigen Aufgaben zu konzentrieren, und begrenzen die Entstehung von Fehlern durch manuelle Verfahren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Systeme zur Build- und Bereitstellungsverwaltung werden verwendet, um Änderungen nachzuverfolgen und zu implementieren, Fehler zu reduzieren, die durch manuelle Prozesse verursacht werden, und den Aufwand für sichere Implementierungen zu minimieren. Nutzen Sie eine vollständig automatisierte Integrations- und Bereitstellungs-Pipeline vom Einchecken des Codes über das Testen und die Bereitstellung bis hin zur Validierung. Dies reduziert die Vorlaufzeit, senkt die Kosten, ermöglicht häufigere Änderungen, minimiert den Aufwand und verbessert die Zusammenarbeit.

Implementierungsschritte



Diagramm, das eine CI/CD-Pipeline mit AWS CodePipeline und zugehörigen Services zeigt

1. Nutzen Sie AWS CodeCommit zur Versionskontrolle und zum Speichern und Verwalten von Ressourcen (wie Dokumente, Quellcode und Binärdateien).
2. Nutzen Sie CodeBuild, um den Quellcode zu kompilieren, Komponententests auszuführen und Artefakte zu erzeugen, die sofort bereitgestellt werden können.

3. Nutzen Sie CodeDeploy als Bereitstellungsservice, der Anwendungsbereitstellungen für Amazon EC2-Instances, On-Premises-Instances, AWS Lambda-Serverless-Funktionenoder Amazon ECSautomatisiert.
4. Überwachen Sie Ihre Bereitstellungen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS06-BP04 Automatisieren von Tests und Rollback

Zugehörige Dokumente:

- AWS Developer Tools (AWS-Entwicklertools)
- Was ist AWS CodeCommit?
- Was ist AWS CodeBuild?
- AWS CodeBuild
- Was ist AWS CodeDeploy?

Zugehörige Videos:

- AWS re:Invent 2022 - AWS Well-Architected best practices for DevOps on AWS (AWS re:Invent 2022 – AWS Well-Architected Best Practices für DevOps in AWS)

OPS05-BP05 Durchführen der Patch-Verwaltung

Führen Sie eine Patch-Verwaltung durch, um Funktionen zu erhalten, Probleme zu beheben und die Konformität mit der Governance zu gewährleisten. Automatisieren Sie die Patch-Verwaltung, um Fehler aufgrund manueller Prozesse zu reduzieren, zu skalieren und den Aufwand für die Installation von Patches zu verringern.

Patch- und Schwachstellenmanagement sind Teil Ihrer Vorteile- und Risikomanagement-Aktivitäten. Es ist vorzuziehen, unveränderliche Infrastrukturen zu haben und Workloads in verifizierten bekannten guten Zuständen bereitzustellen. Wenn dies nicht realisierbar ist, ist das Patchen die verbleibende Option.

Amazon EC2 Image Builder stellt Pipelines zur Aktualisierung von Machine Images bereit. Als Teil der Patch-Verwaltung nutzen Amazon Machine Images (AMIs) eine AMI-Image-Pipeline oder Container-Images eine Docker-Image-Pipeline,während AWS Lambda Muster für benutzerdefinierte Lambda-Laufzeiten und zusätzliche Bibliotheken bietet, um Sicherheitslücken zu beseitigen.

Sie sollten Updates für Amazon Machine Images für Linux- oder Windows Server-Images mit Amazon EC2 Image Builderverwalten. Sie können Amazon Elastic Container Registry (Amazon ECR) mit Ihrer bestehenden Pipeline zur Verwaltung von Amazon ECS-Images und von Amazon EKS-Images nutzen. Lambda beinhaltet Versionsmanagementfunktionen.

Patches sollten nicht auf Produktionssystemen ohne erste Tests in einer sicheren Umgebung durchgeführt werden. Patches sollten nur angewendet werden, wenn sie ein betriebliches oder geschäftliches Ergebnis unterstützen. In AWS können Sie AWS Systems Manager Patch Manager verwenden, um das Patchen verwalteter Systeme zu automatisieren und die Aktivitäten mithilfe von Systems Manager-Wartungsfenstern zu planen.

Gewünschtes Ergebnis: Ihre AMI und Container-Images sind gepatcht, aktuell und startbereit. Sie können den Status aller bereitgestellten Images nachverfolgen und wissen, dass die Patches konform sind. Sie können über den aktuellen Status berichten und verfügen über ein Verfahren, mit dem Sie Ihre Compliance-Anforderungen erfüllen können.

Typische Anti-Muster:

- Sie erhalten den Auftrag, alle neuen Sicherheits-Patches innerhalb von zwei Stunden anzuwenden, was zu mehreren Ausfällen aufgrund der Anwendungsinkompatibilität mit bestimmten Patches führt.
- Eine ungepatchte Bibliothek hat unbeabsichtigte Folgen, weil unbekannte Personen Schwachstellen darin ausnutzen, um auf Ihren Workload zuzugreifen.
- Sie patchen die Entwicklerumgebungen automatisch, ohne die Entwickler zu benachrichtigen. Sie erhalten mehrere Beschwerden von den Entwicklern, dass ihre Umgebung nicht mehr wie erwartet funktioniert.
- Sie haben die kommerziell im Handel erhältliche Software auf einer persistenten Instance nicht gepatcht. Als ein Problem mit der Software auftritt und Sie sich an den Anbieter wenden, werden Sie darüber informiert, dass die Version nicht unterstützt wird und Sie bestimmte Patches installieren müssen, um Unterstützung zu erhalten.
- Ein kürzlich veröffentlichter Patch für Ihre verwendete Verschlüsselungssoftware bietet signifikante Leistungsverbesserungen. Ihr ungepatchtes System weist Leistungsprobleme auf, die bestehen bleiben, weil es nicht gepatcht ist.

- Sie werden über eine Zero-Day-Schwachstelle informiert, die eine Notfalllösung erfordert, und Sie müssen alle Ihre Umgebungen manuell patchen.

Vorteile der Nutzung dieser bewährten Methode: Durch die Einrichtung eines Patch-Verwaltungsprozesses, einschließlich Ihrer Patching-Kriterien und Bereitstellungsmethodik für Ihre Umgebungen, können Sie die Patch-Ebenen skalieren und Berichte darüber erstellen. Das gibt Ihnen Sicherheit in Bezug auf Sicherheitspatches und gewährleistet einen klaren Überblick über den Status bekannter Problemlösungen. Dies wiederum fördert die Übernahme der gewünschten Merkmale und Funktionen, das Entfernen von Problemen und die kontinuierliche Compliance. Implementieren Sie Verwaltungssysteme und Automatisierung für Patches, um den Aufwand für die Bereitstellung von Patches zu reduzieren und Fehler zu begrenzen, die durch manuelle Prozesse verursacht werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Installieren Sie auf Ihren Systemen Patches zur Behebung von Problemen, zur Erlangung der gewünschten Funktionen oder Fähigkeiten sowie zur kontinuierlichen Einhaltung der Governance-Richtlinien und der Anforderungen des Lieferantensupport. Nehmen Sie in unveränderlichen Systemen eine Bereitstellung mit einer geeigneten Patch-Gruppe vor, um das gewünschte Ergebnis zu erzielen. Automatisieren Sie den Mechanismus der Patch-Verwaltung, um die Patch-Zeit zu verkürzen, Fehler aufgrund von manuellen Prozessen zu vermeiden und den Aufwand für die Installation von Patches zu verringern.

Implementierungsschritte

Für Amazon EC2 Image Builder:

1. Wenn Sie Amazon EC2 Image Builder verwenden, geben Sie die Pipeline-Details an:
   a. Erstellen Sie eine Image-Pipeline und geben Sie ihr einen Namen.
   b. Definieren Sie den Pipeline-Zeitplan und die Zeitzone.
   c. Konfigurieren Sie alle Abhängigkeiten.
2. Wählen Sie ein Rezept:
   a. Wählen Sie ein vorhandenes Rezept aus oder erstellen Sie ein neues.
   b. Wählen Sie den Image-Typ aus.
   c. Geben Sie Ihrem Rezept einen Namen und eine Versionsnummer.
   d. Wählen Sie Ihr Basis-Image aus.

e. Fügen Sie Build-Komponenten zur Zielregistrierung hinzu.

3. Optional: Definieren Sie Ihre Infrastrukturkonfiguration.
4. Optional: Definieren Sie die Konfigurationseinstellungen.
5. Überprüfen Sie die Einstellungen.
6. Achten Sie regelmäßig auf die Rezepthygiene.

Für Systems Manager Patch Manager:

1. Erstellen Sie eine Patch-Baseline.
2. Wählen Sie eine Methode für Pfadoperationen aus.
3. Aktivieren Sie Compliance-Berichte und -Scans.

Ressourcen

Zugehörige bewährte Methoden:

- OPS06-BP04 Automatisieren von Tests und Rollback

Zugehörige Dokumente:

- Was ist Amazon EC2 Image Builder?
- Create an image pipeline using the Amazon EC2 Image Builder (Erstellen einer Image-Pipeline mit dem Amazon EC2 Image Builder)
- Create a container image pipeline (Erstellen einer Container-Image-Pipeline)
- AWS Systems Manager Patch Manager
- Working with Patch Manager (Arbeiten mit Patch Manager)
- Working with patch compliance reports (Arbeiten mit Patch-Compliance-Berichten)
- AWS Developer Tools

Zugehörige Videos:

- CI/CD für Serverless Anwendungen in AWS
- Design mit Blick auf die Ops

Zugehörige Beispiele:

- Well-Architected Labs: Bestands- und Patch-Verwaltung
- Anleitungen zu AWS Systems Manager Patch Manager

OPS05-BP06 Gemeinsame Design-Standards

Tauschen Sie teamübergreifend bewährte Methoden aus, um das Bewusstsein zu schärfen und den Nutzen der Entwicklungsarbeit zu maximieren. Dokumentieren Sie sie und halten Sie sie auf dem neuesten Stand, wenn sich Ihre Architektur weiterentwickelt. Wenn gemeinsame Standards in Ihrem Unternehmen durchgesetzt werden, ist es wichtig, dass Mechanismen vorhanden sind, um Ergänzungen, Änderungen und Ausnahmen von Standards abzubilden. Ohne diese Option werden Standards zu einer Einschränkung der Innovation.

Gewünschtes Ergebnis: Designstandards werden von allen Teams in Ihren Organisationen gemeinsam genutzt. Sie werden dokumentiert und mit der Entwicklung bewährter Methoden auf dem neuesten Stand gehalten.

Typische Anti-Muster:

- Zwei Entwicklerteams haben jeweils einen Service zur Authentifizierung von Benutzern erstellt. Ihre Benutzer müssen für jeden Teil des Systems, auf den sie zugreifen möchten, eigene Anmeldeinformationen verwenden.
- Jedes Team verwaltet seine eigene Infrastruktur. Eine neue Compliance-Anforderung erzwingt eine Änderung Ihrer Infrastruktur. Jedes Team implementiert sie auf andere Weise.

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung gemeinsamer Standards unterstützt die Umsetzung bewährter Methoden und maximiert den Nutzen der Entwicklungsarbeit. Die Dokumentation und Aktualisierung von Designstandards hält Ihre Organisation auf dem neuesten Stand bezüglich der bewährten Methoden und der Anforderungen an die Sicherheit und Compliance.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Nutzen Sie bewährte Methoden, Designstandards, Checklisten, Arbeitsverfahren, Leitlinien und Governance-Anforderungen in allen Teams. Verwenden Sie Verfahren zur Anforderung von

Änderungen, Ergänzungen und Ausnahmen von Designstandards, um Verbesserungen und Innovationen zu unterstützen. Stellen Sie sicher, dass die Teams über die veröffentlichten Inhalte informiert sind. Verwenden Sie ein System, um die Designstandards auf dem neuesten Stand zu halten, wenn neue bewährte Methoden eingeführt werden.

Kundenbeispiel

AnyCompany Retail verfügt über ein funktionsübergreifendes Architekturteam, das Softwarearchitekturmuster erstellt. Dieses Team entwickelt die Architektur mit integrierter Compliance und Governance. Teams, die diese gemeinsamen Standards anwenden, profitieren davon, dass Compliance und Governance bereits integriert sind. Sie können schnell auf dem Designstandard aufbauen. Das Architekturteam trifft sich vierteljährlich, um die Architekturmuster zu bewerten und sie gegebenenfalls zu aktualisieren.

Implementierungsschritte

1. Bestimmen Sie ein funktionsübergreifendes Team, das für die Entwicklung und Aktualisierung der Designstandards zuständig ist. Dieses Team sollte mit Stakeholdern in Ihrer gesamten Organisation zusammenarbeiten, um Designstandards, Arbeitsverfahren, Checklisten, Leitlinien und Governance-Anforderungen zu entwickeln. Dokumentieren Sie die Designstandards und geben Sie sie innerhalb Ihrer Organisation weiter.
   a. Mit AWS Service Catalog können Sie Portfolios erstellen, die Designstandards als Infrastructure-as-Code abbilden. Sie können Portfolios über Konten hinweg gemeinsam nutzen.
2. Verwenden Sie ein System, um die Designstandards auf dem neuesten Stand zu halten, wenn neue bewährte Methoden eingeführt werden.
3. Wenn Designstandards zentral durchgesetzt werden, sollten Sie über ein Verfahren verfügen, um Änderungen, Aktualisierungen und Ausnahmen anzufordern.

Aufwand für den Implementierungsplan: Mittel. Die Entwicklung eines Prozesses zur Erstellung und gemeinsamen Nutzung von Designstandards kann die Koordination und Zusammenarbeit mit Stakeholdern in Ihrer gesamten Organisation erforderlich machen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP03 Bewerten der Governance-Anforderungen - Governance-Anforderungen beeinflussen Designstandards.

- OPS01-BP04 Bewerten der Compliance-Anforderungen - Compliance ist ein wichtiger Faktor bei der Erstellung von Designstandards.
- OPS07-BP02 Sicherstellen einer konsistenten Prüfung der betrieblichen Bereitschaft - Checklisten für die operative Einsatzbereitschaft sind ein Mechanismus zur Umsetzung von Designstandards bei der Gestaltung Ihres Workloads.
- OPS11-BP01 Implementieren eines Prozesses für die kontinuierliche Verbesserung - Die Aktualisierung von Designstandards ist ein Teil der kontinuierlichen Verbesserung.
- OPS11-BP04 Wissensmanagement - Als Teil Ihres Wissensmanagements sollten Sie Designstandards dokumentieren und weitergeben.

Zugehörige Dokumente:

- Automate AWS Backups with AWS Service Catalog (Automatisieren von AWS Backups mit AWS Service Catalog)
- AWS Service Catalog Account Factory-Enhanced (Erweiterte Nutzung von AWS Service Catalog Account Factory)
- How Expedia Group built Database as a Service (DBaaS) offering using AWS Service Catalog (So hat die Expedia Gruppe mit AWS Service Catalog ein Database-as-a-Service-Angebot (DBaaS) entwickelt)
- Maintain visibility over the use of cloud architecture patterns (Überblick über die Nutzung von Cloud-Architekturmustern)
- Simplify sharing your AWS Service Catalog portfolios in an AWS Organizations setup (Vereinfachen der gemeinsamen Nutzung Ihrer AWS Service Catalog-Portfolios in einem AWS Organizations-Setup)

Zugehörige Videos:

- AWS Service Catalog – Getting Started (AWS Service Catalog – Erste Schritte)
- AWS re:Invent 2020: Manage your AWS Service Catalog portfolios like an expert (AWS re:Invent 2020: Verwalten Ihrer AWS Service Catalog-Portfolios wie ein Experte)

Zugehörige Beispiele:

- AWS Service Catalog Reference Architecture (AWS Service Catalog-Referenzarchitektur)
- AWS Service Catalog-Workshop

Zugehörige Services:

- Mit AWS Service Catalog

OPS05-BP07 Implementieren von Verfahren zur Verbesserung der Codequalität

Implementieren Sie Verfahren zur Verbesserung der Codequalität und Minimierung von Fehlern. Einige Beispiele sind die testbasierte Entwicklung, Code-Reviews, die Einführung von Standards und Pair-Programming. Integrieren Sie diese Verfahren in Ihren Continuous-Integration- und delivery-Prozess.

Gewünschtes Ergebnis: Ihre Organisation setzt bewährte Methoden wie Code-Reviews oder Pair-Programming ein, um die Codequalität zu verbessern. Entwickler und operative Mitarbeiter nutzen bewährte Methoden zur Codequalität als Teil des Softwareentwicklungslebenszyklus.

Typische Anti-Muster:

- Sie führen ohne Code-Review Commits zum Main-Branch Ihrer Anwendung durch. Die Änderung wird automatisch in der Produktion bereitgestellt und verursacht einen Ausfall.
- Eine neue Anwendung wird ohne Unit-, End-to-End- oder Integrationstests entwickelt. Es gibt keine Möglichkeit, die Anwendung vor der Bereitstellung zu testen.
- Ihre Teams nehmen manuelle Änderungen in der Produktion vor, um Fehler zu beheben. Die Änderungen durchlaufen keine Tests oder Code-Reviews und werden nicht durch kontinuierliche Integrations- und Bereitstellungsprozesse erfasst oder protokolliert.

Vorteile der Nutzung dieser bewährten Methode: Durch die Einführung von Methoden zur Verbesserung der Codequalität können Sie dazu beitragen, Probleme in der Produktion zu minimieren. Die Codequalität erleichtert die Anwendung von bewährten Methoden wie Paarprogrammierung, Codeüberprüfungen und Implementierung von KI-Produktivitätstools.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Implementieren Sie Verfahren zur Verbesserung der Codequalität, um vor der Bereitstellung Fehler zu minimieren. Nutzen Sie Verfahren wie die testbasierte Entwicklung, Code-Reviews und Pair-Programming, um die Qualität Ihrer Entwicklung zu verbessern.

Nutzen Sie die Leistungsfähigkeit generativer KI mit Amazon Q Developer, um die Produktivität und Codequalität von Entwicklern zu verbessern. Amazon Q Developer umfasst die Generierung von Codevorschlägen (basierend auf großen Sprachmodellen), die Erstellung von Komponententests (einschließlich Randbedingungen) und Verbesserungen der Codesicherheit durch die Erkennung und Behebung von Sicherheitsschwachstellen.

Kundenbeispiel

AnyCompany Retail wendet verschiedene Verfahren an, um die Codequalität zu verbessern. Die testbasierte Entwicklung ist der Standard für die Entwicklung von Anwendungen. Bei einigen neuen Funktionen arbeiten die Entwickler während eines Sprints zusammen. Jede Pull-Anforderung wird von einem erfahrenen Entwickler überprüft, bevor sie integriert und bereitgestellt wird.

Implementierungsschritte

1. Setzen Sie bei Ihrem kontinuierlichen Integrations- und Bereitstellungsprozess auf Code-Qualitätsverfahren wie die testbasierte Entwicklung, Code-Reviews und Pair-Programming. Nutzen Sie diese Techniken, um die Softwarequalität zu verbessern.
   a. Verwenden Sie Amazon Q Developer, ein generatives KI-Tool, mit dem Sie Komponententestfälle (einschließlich Randbedingungen) erstellen, Funktionen mithilfe von Code und Kommentaren generieren, bekannte Algorithmen implementieren, Verstöße gegen Sicherheitsrichtlinien und Sicherheitsschwachstellen in Ihrem Code erkennen, Secrets erkennen, Infrastruktur as Code (IaC) scannen, Code dokumentieren und Codebibliotheken von Drittanbietern schneller erlernen können.
   b. Amazon CodeGuru Reviewer kann Machine-Learning-Programmierempfehlungen für Java- und Python-Code bereitstellen.
   c. Mit AWS Cloud9 können Sie gemeinsame Entwicklungsumgebungen schaffen, in denen Sie gemeinsam an der Codeentwicklung arbeiten können.

Aufwand des Implementierungsplans: mittel. Es gibt viele Möglichkeiten zur Umsetzung dieser bewährten Methode. Es kann jedoch schwierig sein, die Akzeptanz im Unternehmen zu erreichen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP02 Testen und Validieren von Änderungen
- OPS05-BP06 Gemeinsame Design-Standards

Zugehörige Dokumente:

- Einführung eines testgesteuerten Entwicklungsansatzes
- Beschleunigen Ihres Softwareentwicklungszyklus mit Amazon Q
- Amazon Q Developer, jetzt allgemein verfügbar, enthält eine Vorschau auf neue Funktionen, mit denen das Entwicklererlebnis neu gestaltet werden kann
- Der ultimative Spickzettel für die Verwendung von Amazon Q Developer in Ihrer IDE
- Shift-Left-Workload, Nutzung von KI für die Testerstellung
- Amazon Q Developer Center
- 10 Methoden für eine schnellere Entwicklung von Anwendungen mit Amazon CodeWhisperer
- Ein Blick über die Codeabdeckung hinaus mit Amazon CodeWhisperer
- Bewährte Methoden für Prompt-Engineering mit Amazon CodeWhisperer
- Leitfaden für agile Software
- Meine CI/CD-Pipeline ist mein Release Captain
- Automatisieren von Code-Reviews mit Amazon CodeGuru Reviewer
- Einführung eines testgesteuerten Entwicklungsansatzes
- So entwickelt DevFactory bessere Anwendungen mit Amazon CodeGuru
- Über Pair-Programming
- RENGA Inc. automatisiert Code-Reviews mit Amazon CodeGuru
- Die Kunst der agilen Entwicklung: Testbasierte Entwicklung
- Warum Code-Reviews wichtig sind (und tatsächlich Zeit sparen!)

Zugehörige Videos:

- Implementieren einer API mit dem Amazon Q Developer-Agenten für Softwareentwicklung
- Installation, Konfiguration und Verwendung von Amazon Q Developer mit JetBrains-IDEs (Anleitung)
- Beherrschung der Kunst von Amazon CodeWhisperer – YouTube-Playlist
- AWS re:Invent 2020: Kontinuierliche Verbesserung der Codequalität mit Amazon CodeGuru
- AWS Summit ANZ 2021 – Vorantreiben einer „Test-First“-Strategie mit CDK und testgesteuerter Entwicklung

Zugehörige Services:

- Amazon Q Developer
- Amazon CodeGuru Reviewer
- Amazon CodeGuru Profiler
- AWS Cloud9

OPS05-BP08 Verwenden mehrerer Umgebungen

Verwenden Sie mehrere Umgebungen, um Ihren Workload auszuprobieren, zu entwickeln und zu testen. Verwenden Sie zunehmende Kontrollstufen, wenn Umgebungen sich der Produktion nähern, um sicherzustellen, dass Ihr Workload bei der Bereitstellung wie beabsichtigt funktioniert.

Gewünschtes Ergebnis: Sie verfügen über mehrere Umgebungen, die Ihre Compliance- und Governance-Anforderungen widerspiegeln. Auf Ihrem Weg zur Produktion testen und promoten Sie Code in Umgebungen.

Typische Anti-Muster:

- Sie führen die Entwicklung in einer gemeinsamen Entwicklungsumgebung durch und ein weiterer Entwickler überschreibt Ihre Codeänderungen.
- Die restriktiven Sicherheitskontrollen Ihrer gemeinsamen Entwicklungsumgebung verhindern, dass Sie mit neuen Services und Funktionen experimentieren können.
- Sie führen Belastungstests auf Ihren Produktionssystemen durch und verursachen einen Ausfall für Ihre Benutzer.
- In der Produktion ist ein kritischer Fehler aufgetreten, der zum Verlust von Daten geführt hat. In Ihrer Produktionsumgebung versuchen Sie, die Bedingungen, die zum Datenverlust geführt haben, nachzustellen, damit Sie die Ursache feststellen und beseitigen können. Um einen weiteren Datenverlust während des Testens zu verhindern, müssen Sie die Anwendung für Ihre Benutzer deaktivieren.
- Sie betreiben einen Mehrmandanten-Service und können eine Kundenanfrage nach einer eigenen Umgebung nicht erfüllen.
- Möglicherweise testen Sie nicht immer, aber wenn Sie dies tun, testen Sie in Ihrer Produktionsumgebung.
- Sie glauben, dass die Einfachheit einer einzelnen Umgebung die Auswirkungen von Änderungen innerhalb der Umgebung ausgleicht.

Vorteile der Nutzung dieser bewährten Methode: Sie können gleichzeitig mehrere Entwicklungs-, Test- und Produktionsumgebungen unterstützen, ohne Konflikte zwischen Entwicklern oder User-Communities zu erzeugen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Verwenden Sie mehrere Umgebungen und stellen Sie den Entwicklern Sandbox-Umgebungen mit weniger Kontrollen zur Verfügung, in denen sie experimentieren können. Richten Sie individuelle Entwicklungsumgebungen ein, damit parallele Arbeit möglich ist. Dadurch steigern Sie die Agilität der Entwicklung. Implementieren Sie strengere Kontrollen erst in den Umgebungen, die kurz vor der Produktionsaufnahme stehen, damit Entwickler Innovationen schaffen können. Nutzen Sie die Infrastruktur als Code sowie Konfigurationsverwaltungssysteme, um Umgebungen bereitzustellen, die mit den in der Produktion vorhandenen Kontrollen einheitlich konfiguriert sind. Auf diese Weise können Sie sicherstellen, dass die Systeme bei der Bereitstellung wie erwartet funktionieren. Wenn Umgebungen nicht in Gebrauch sind, schalten Sie sie ab, um Kosten für ungenutzte Ressourcen zu vermeiden (z. B. Entwicklungssysteme am Abend und am Wochenende). Stellen Sie beim Belastungstest produktionsgleiche Umgebungen bereit, um die Gültigkeit der Ergebnisse zu verbessern.

Ressourcen

Zugehörige Dokumente:

- Instance Scheduler on AWS (Instance Scheduler in AWS)
- Was ist AWS CloudFormation?

OPS05-BP09 Häufige, kleine, reversible Änderungen vornehmen

Häufige, kleine und reversible Änderungen verringern den Umfang und die Auswirkung einer Änderung. In Verbindung mit Change-Management-Systemen, Systemen zur Konfigurationsverwaltung und Build- und Liefersystemen reduzieren häufige, kleine und reversible Änderungen den Umfang und die Auswirkungen einer Änderung. Dies macht die Fehlersuche effizienter und ermöglicht eine schnellere Korrektur, da die Möglichkeit besteht, Änderungen zurückzusetzen.

Typische Anti-Muster:

- Sie stellen vierteljährlich eine neue Version Ihrer Anwendung mit einem Änderungsfenster bereit, was bedeutet, dass ein zentraler Dienst ausgeschaltet wird.
- Sie nehmen häufig Änderungen an Ihrem Datenbankschema vor, ohne Änderungen in Ihren Managementsystemen nachzuverfolgen.
- Sie führen direkte manuelle Updates durch, überschreiben damit bestehende Installationen und Konfigurationen und haben keinen klaren Rollback-Plan.

Vorteile der Nutzung dieser bewährten Methode: Sie profitieren schneller von den Entwicklungsarbeiten, wenn Sie häufig kleine Änderungen bereitstellen. Wenn die Änderungen klein sind, ist es viel einfacher zu erkennen, ob sie unbeabsichtigte Folgen haben, und sie lassen sich leichter rückgängig machen. Wenn die Änderungen rückgängig gemacht werden können, ist die Implementierung mit geringeren Risiken verbunden, da die Wiederherstellung einfacher ist. Der Änderungsprozess hat ein geringeres Risiko und die Auswirkungen einer fehlgeschlagenen Änderung werden reduziert.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

Implementierungsleitfaden

Machen Sie häufige, kleine und reversible Änderungen und verringern Sie dadurch den Umfang und die Auswirkung einer Änderung. Dies erleichtert die Fehlersuche, trägt zur Beschleunigung der Fehlerbehebung bei und bietet die Möglichkeit, eine Änderung zurückzusetzen. Außerdem profitiert Ihr Unternehmen schneller von neuen Entwicklungen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP03 Einsatz von Systemen zur Konfigurationsverwaltung
- OPS05-BP04 Einsatz von Systemen zur Build- und Bereitstellungsverwaltung.
- OPS06-BP04 Automatisieren von Tests und Rollback

Zugehörige Dokumente:

- Implementieren von Microservices in AWS
- Microservices – Beobachtbarkeit

OPS05-BP10 Vollständige Automatisierung von Integration und Bereitstellung

Automatisieren Sie den Aufbau, die Bereitstellung und die Tests des Workloads. Dadurch werden Fehler aufgrund von manuellen Prozessen und der Aufwand für die Bereitstellung von Änderungen verringert.

Wenden Sie Metadaten mithilfe von Ressourcen-Tags und AWS Resource Groups nach einer konsistenten Markierungsstrategie an, um die Identifizierung Ihrer Ressourcen zu erleichtern. Versehen Sie Ihre Ressourcen mit Tags für Organisation, Kostenkalkulation, Zugriffssteuerung und Zielrichtung der Ausführung von automatisierten Betriebsaktivitäten.

Gewünschtes Ergebnis: Entwickler verwenden Tools, um Code bereitzustellen und bis zur Produktion zu unterstützen. Entwickler müssen sich nicht bei der AWS Management Console anmelden, um Updates bereitzustellen. Es gibt einen vollständigen Audit Trail für Änderungen und Konfigurationen, der die Governance- und Compliance-Anforderungen erfüllt. Prozesse sind wiederholbar und teamübergreifend standardisiert. Entwickler sind in der Lage, sich auf die Entwicklung und Code-Pushs zu konzentrieren und so die Produktivität zu steigern.

Typische Anti-Muster:

- Am Freitag schließen Sie die Erstellung des neuen Codes für Ihren Funktionszweig ab. Am Montag, nach dem Ausführen Ihrer Skripts für die Codequalitätstests und einzelnen Komponententests, überprüfen Sie Ihren Code für den nächsten geplanten Release.
- Sie erhalten die Aufgabe, eine Korrektur für ein kritisches Problem zu schreiben, das sich auf eine große Anzahl von Kunden in der Produktion auswirkt. Nachdem Sie die Korrektur getestet haben, übergeben Sie Ihren Code und fordern beim Änderungsmanagement die Bereitstellungsgenehmigung zur Produktion an.
- Als Entwickler melden Sie sich bei der AWS Management Console an, um eine neue Entwicklungsumgebung mit nicht standardmäßigen Methoden und Systemen zu erstellen.

Vorteile der Nutzung dieser bewährten Methode: Durch die Implementierung automatisierter Build- und Bereitstellungsverwaltungssysteme reduzieren Sie Fehler aus manuellen Prozessen und den Aufwand für die Bereitstellung von Änderungen, sodass sich Ihre Teammitglieder besser auf die Wertschöpfung konzentrieren können. Sie erhöhen die Liefergeschwindigkeit auf Ihrem Weg zur Produktion.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

Implementierungsleitfaden

Verwenden Sie Systeme zur Build- und Bereitstellungsverwaltung für die Verfolgung und Implementierung von Änderungen, die Reduzierung von Fehlern, die durch manuelle Prozesse entstehen, sowie zur Verringerung des Aufwands. Nutzen Sie eine vollständig automatisierte Integrations- und Bereitstellungs-Pipeline vom Einchecken des Codes über das Testen und die Bereitstellung bis hin zur Validierung. Dies reduziert die Vorlaufzeit, fördert häufigere Änderungen, reduziert den Aufwand, beschleunigt die Markteinführung, führt zu einer höheren Produktivität und erhöht die Sicherheit Ihres Codes bis hin zur Produktion.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP03 Einsatz von Systemen zur Konfigurationsverwaltung
- OPS05-BP04 Einsatz von Systemen zur Build- und Bereitstellungsverwaltung.

Zugehörige Dokumente:

- Was ist AWS CodeBuild?
- Was ist AWS CodeDeploy?

Zugehörige Videos:

- AWS re\:Invent 2022 - AWS Well-Architected best practices for DevOps on AWS (AWS re\:Invent 2022 – AWS Well-Architected Best Practices für DevOps in AWS)

Bereitstellungsrisiken abschwächen

Verwenden Sie Ansätze, die ein schnelles Feedback zur Qualität liefern und eine umgehende Wiederherstellung des vorherigen Zustands nach Änderungen ermöglichen, die nicht zu den gewünschten Ergebnissen führen. Mit diesen Verfahren können Sie die Auswirkung von Problemen eindämmen, die durch die Bereitstellung von Änderungen entstehen.

Das Design Ihres Workloads sollte beinhalten, wie es bereitgestellt, aktualisiert und betrieben werden soll. Sie werden technische Methoden implementieren möchten, die auf die Reduzierung von Mängeln sowie auf schnelle und sichere Fehlerbehebungen ausgerichtet sind.

Bewährte Methoden

- OPS06-BP01 Einkalkulieren nicht erfolgreicher Änderungen
- OPS06-BP02 Testbereitstellungen
- OPS06-BP03 Einsetzen sicherer Bereitstellungsstrategien
- OPS06-BP04 Automatisieren von Tests und Rollback

OPS06-BP01 Einkalkulieren nicht erfolgreicher Änderungen

Planen Sie Maßnahmen für die Rückkehr zu einem bekanntermaßen funktionierenden Zustand oder die Korrektur in der Produktionsumgebung ein, falls bei der Bereitstellung ein nicht erwünschtes Ergebnis auftritt. Eine Richtlinie zur Festlegung eines solchen Plans hilft allen Teams, Strategien zum Umgang mit fehlgeschlagenen Änderungen zu entwickeln. Einige Beispiele für Strategien sind Bereitstellungs- und Rollback-Schritte, Änderungsrichtlinien, Feature-Flags sowie die Isolierung und Verlagerung von Datenverkehr. Ein einzelner Release kann mehrere zusammengehörige Komponentenänderungen enthalten. Die Strategie sollte die Möglichkeit bieten, dem Ausfall einer Komponentenänderung standzuhalten oder sich danach zu regenerieren.

Gewünschtes Ergebnis: Sie haben einen detaillierten Wiederherstellungsplan für Ihre Änderung erstellt, falls diese nicht erfolgreich sein sollte. Darüber hinaus haben Sie die Größe Ihres Releases reduziert, um die potenziellen Auswirkungen auf andere Workload-Komponenten zu minimieren. Infolgedessen haben Sie die Auswirkungen auf Ihr Unternehmen verringert, indem Sie die potenziellen Ausfallzeiten aufgrund einer fehlgeschlagenen Änderung reduziert und die Flexibilität und Effizienz der Wiederherstellungszeiten erhöht haben.

Typische Anti-Muster:

- Sie haben Code bereitgestellt und Ihre Anwendung ist instabil geworden, aber es befinden sich aktive Benutzer im System. Sie müssen entscheiden, ob Sie die Änderung rückgängig machen und Auswirkungen auf die aktiven Benutzer in Kauf nehmen möchten, oder ob Sie die Änderung erst später rückgängig machen möchten, wodurch möglicherweise trotzdem Auswirkungen auf die Benutzer entstehen könnten.
- Nachdem Sie eine Routineänderung vorgenommen haben, kann auf Ihre neuen Umgebungen zugegriffen werden, aber eines Ihrer Subnetze ist nicht mehr erreichbar. Sie müssen entscheiden, ob Sie die gesamte Änderung rückgängig machen oder versuchen, die Nichtverfügbarkeit des Subnetzes zu beheben. Während Sie diese Entscheidung abwägen, bleibt das Subnetz nicht erreichbar.

- Ihre Systeme sind nicht so konzipiert, dass sie mit kleineren Releases aktualisiert werden können. Daher haben Sie Schwierigkeiten, die Bulk-Änderungen während einer fehlgeschlagenen Bereitstellung rückgängig zu machen.
- Sie verwenden nicht Infrastructure as Code (IaC) und Sie haben manuelle Aktualisierungen an Ihrer Infrastruktur vorgenommen, die zu einer unerwünschten Konfiguration geführt haben. Sie sind nicht in der Lage, die manuellen Änderungen effektiv zu verfolgen und rückgängig zu machen.
- Da Sie die erhöhte Häufigkeit Ihrer Bereitstellungen nicht gemessen haben, hat Ihr Team keinen Anreiz, den Umfang seiner Änderungen zu reduzieren und seine Rollback-Pläne für jede Änderung zu verbessern. Dies führt zu höheren Risiken und höheren Ausfallraten.
- Sie messen nicht die Gesamtdauer eines Ausfalls, der durch erfolglose Änderungen verursacht wird. Ihr Team ist nicht in der Lage, den Bereitstellungsprozess und die Effektivität des Wiederherstellungsplans zu priorisieren und zu verbessern.

Vorteile der Nutzung dieser bewährten Methode: Ein Plan zur Wiederherstellung nach erfolglosen Änderungen minimiert die mittlere Wiederherstellungszeit (MTTR) und reduziert die Auswirkungen auf Ihr Unternehmen.

Risikostufe bei fehlender Befolgung dieser Best Practice: Hoch

Implementierungsleitfaden

Mithilfe einer konsistenten, dokumentierten Richtlinie und Praxis, die von den Release-Teams angewendet wird, kann ein Unternehmen planen, was bei nicht erfolgreichen Änderungen passieren soll. Unter bestimmten Umständen sollte die Richtlinie ein Forward-Fixing berücksichtigen. In allen Fällen sollte ein Fix-Forward- oder Rollback-Plan vor der Bereitstellung in der Live-Produktion gut dokumentiert und getestet werden, um die benötigte Zeit zum Rückgängigmachen einer Änderung zu minimieren.

Implementierungsschritte

1. Dokumentieren Sie die Richtlinien, nach denen Teams über wirksame Pläne verfügen müssen, wie Änderungen innerhalb eines bestimmten Zeitraums rückgängig gemacht werden können.
   a. In den Richtlinien sollte festgelegt sein, wann eine Fix-Forward-Situation zulässig ist.
   b. Fordern Sie einen dokumentierten Rollback-Plan, auf den alle Beteiligten zugreifen können.
   c. Geben Sie die Anforderungen für das Rollback an (z. B. wenn festgestellt wird, dass nicht autorisierte Änderungen vorgenommen wurden).

2. Analysieren Sie den Grad der Auswirkungen aller Änderungen für jede Komponente eines Workloads.
   a. Ermöglichen Sie die Standardisierung, Vorlagenerstellung und Vorautorisierung wiederholbarer Änderungen, sofern sie einem konsistenten Workflow folgen, der Änderungsrichtlinien durchsetzt.
   b. Reduzieren Sie die potenziellen Auswirkungen jeder Änderung, indem Sie den Umfang der Änderung verringern, damit die Wiederherstellung weniger Zeit in Anspruch nimmt und weniger Auswirkungen auf das Unternehmen hat.
   c. Stellen Sie sicher, dass die Rollback-Verfahren den Code in einen bekannt funktionierenden Zustand zurückversetzen, um Zwischenfälle nach Möglichkeit zu vermeiden.
3. Integrieren Sie Tools und Workflows, um Ihre Richtlinien programmgesteuert durchzusetzen.
4. Machen Sie Daten zu Änderungen für andere Workload-Besitzer sichtbar, um die Diagnose bei fehlgeschlagenen Änderungen, für die kein Rollback möglich ist, zu beschleunigen.
   a. Messen Sie den Erfolg dieser Methode anhand sichtbarer Änderungsdaten und identifizieren Sie iterative Verbesserungen.
5. Verwenden Sie Überwachungstools, um den Erfolg oder Misserfolg einer Bereitstellung zu überprüfen und so die Entscheidungsfindung beim Rollback zu beschleunigen.
6. Messen Sie die Dauer des Ausfalls bei einer erfolglosen Änderung, um Ihre Wiederherstellungspläne kontinuierlich zu verbessern.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS06-BP04 Automatisieren von Tests und Rollback

Zugehörige Dokumente:

- AWS Builders' Library | Gewährleistung der Rollback-Sicherheit bei Bereitstellungen
- AWS Whitepaper | Änderungsmanagement in der Cloud

Zugehörige Videos:

- re:Invent 2019 | Amazon’s approach to high-availability deployment (re:Invent 2019 | Der Amazon-Ansatz für die Hochverfügbarkeitsbereitstellung)

OPS06-BP02 Testbereitstellungen

Testen Sie Release-Verfahren in der Vorproduktion, indem Sie dieselbe Bereitstellungskonfiguration, dieselben Sicherheitskontrollen, Schritte und Verfahren wie in der Produktion verwenden. Stellen Sie sicher, dass alle bereitgestellten Schritte wie erwartet abgeschlossen wurden, z. B. das Überprüfen von Dateien, Konfigurationen und Services. Testen Sie alle Änderungen darüber hinaus mit Funktions-, Integrations- und Auslastungstests sowie Überwachungsverfahren, z. B. Zustandsprüfungen. Durch diese Tests können Sie Bereitstellungsprobleme frühzeitig erkennen und haben die Möglichkeit, sie vor der Produktion einzuplanen und zu beheben.

Sie können temporäre parallele Umgebungen erstellen, um jede Änderung zu testen. Automatisieren Sie die Bereitstellung der Testumgebungen mithilfe von Infrastructure as Code (IaC), um den Arbeitsaufwand zu reduzieren und Stabilität, Konsistenz und schnellere Funktionsbereitstellung zu gewährleisten.

Gewünschtes Ergebnis: Ihr Unternehmen führt eine testgestützte Entwicklungskultur ein, die Testbereitstellungen einschließt. Dadurch wird sichergestellt, dass sich die Teams darauf konzentrieren, Werte für das Unternehmen zu schaffen, anstatt Releases zu verwalten. Die Teams werden bei der Identifizierung von Bereitstellungsrisiken frühzeitig einbezogen, um die geeigneten Maßnahmen zur Risikominderung festzulegen.

Typische Anti-Muster:

- Während Produktionseinführungen führen ungetestete Bereitstellungen häufig zu Problemen, die eine Fehlerbehebung und Eskalation erfordern.
- Ihr Release enthält Infrastructure as Code (IaC), wodurch vorhandene Ressourcen aktualisiert werden. Sie sind sich nicht sicher, ob IaC erfolgreich ausgeführt wird oder ob es Auswirkungen auf die Ressourcen gibt.
- Sie stellen eine neue Funktion für Ihre Anwendung bereit. Sie funktioniert nicht wie beabsichtigt und dies fällt erst auf, wenn sie von betroffenen Benutzern gemeldet wird.
- Sie aktualisieren Ihre Zertifikate. Sie installieren versehentlich die Zertifikate für die falschen Komponenten, was unentdeckt bleibt und Auswirkungen auf Website-Benutzer hat, da keine sichere Verbindung zur Website hergestellt werden kann.

Vorteile der Nutzung dieser bewährten Methode: Durch umfangreiche Tests der Bereitstellungsverfahren und der durch sie eingeführten Änderungen in der Vorproduktion werden die potenziellen Auswirkungen der Bereitstellungsschritte auf die Produktion minimiert. Dies erhöht das Vertrauen bei der Produktionseinführung und minimiert den Support während des Betriebs, ohne die bereitgestellten Änderungen zu verlangsamen.

Risikostufe bei fehlender Befolgung dieser Best Practice: Hoch

Implementierungsleitfaden

Das Testen Ihres Bereitstellungsprozesses ist genauso wichtig wie das Testen der Änderungen, die sich aus der Bereitstellung ergeben. Dies kann erreicht werden, indem Sie Ihre Bereitstellungsschritte in einer Vorproduktionsumgebung testen, die die Produktion so genau wie möglich widerspiegelt. Häufig auftretende Probleme, z. B. unvollständige oder falsche Bereitstellungsschritte oder Fehlkonfigurationen, können so vor der Bereitstellung in der Produktionsumgebung erkannt werden. Darüber hinaus können Sie Ihre Wiederherstellungsschritte testen.

Kundenbeispiel

Im Rahmen seiner CI/CD-Pipeline (Continuous Integration and Continuous Delivery) führt AnyCompany Retail die definierten Schritte durch, die zur Veröffentlichung von Infrastruktur- und Softwareupdates für seine Kunden in einer produktionsähnlichen Umgebung erforderlich sind. Die Pipeline besteht aus Vorabprüfungen zur Erkennung von Abweichungen (Erkennung von Änderungen an Ressourcen, die außerhalb von IaC vorgenommen wurden) bei Ressourcen vor der Bereitstellung sowie zur Validierung der Aktionen, die von IaC bei der Initiierung ausgeführt werden. Vor der erneuten Registrierung beim Load Balancer werden Bereitstellungsschritte validiert und z. B. sichergestellt, dass bestimmte Dateien und Konfigurationen vorhanden sind und Services ausgeführt werden und korrekt auf Zustandsprüfungen auf dem lokalen Host reagieren. Darüber hinaus führen alle Änderungen zu einer Reihe automatisierter Tests wie Funktions-, Sicherheits-, Regressions-, Integrations- und Auslastungstests.

Implementierungsschritte

1. Führen Sie Prüfungen vor der Installation durch, um die Vorproduktionsumgebung in der Produktionsumgebung zu spiegeln.
   a. Mit der Abweichungserkennung können Sie erkennen, wann Ressourcen außerhalb von AWS CloudFormation geändert wurden.

   b. Verwenden Sie Änderungssätze, um zu überprüfen, ob die Absicht einer Stack-Aktualisierung mit den Aktionen übereinstimmt, die von AWS CloudFormation bei der Initiierung des Änderungssatzes ausgeführt werden.
2. Dadurch wird ein manueller Genehmigungsschritt in AWS CodePipeline ausgelöst, um die Bereitstellung in der Vorproduktionsumgebung zu autorisieren.
3. Verwenden Sie Bereitstellungskonfigurationen wie AWS CodeDeploy-AppSpec- Dateien zur Definition der Bereitstellungs- und Validierungsschritte.
4. Wo zutreffend, integrieren Sie AWS CodeDeploy in andere AWS-Services oder integrieren Sie AWS CodeDeploy in Produkte und Services von Partnern.
5. Überwachen Sie Bereitstellungen mithilfe von Ereignisbenachrichtigungen von Amazon CloudWatch, AWS CloudTrail und Amazon SNS.
6. Führen Sie nach der Bereitstellung automatisierte Tests durch, einschließlich Funktions-, Sicherheits-, Regressions-, Integrations- und Auslastungstests.
7. Behandlung von Problemen bei der Bereitstellung.
8. Eine erfolgreiche Validierung der zuvor genannten Schritte sollte einen manuellen Genehmigungsworkflow initiieren, um die Bereitstellung in der Produktion zu autorisieren.

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP02 Testen und Validieren von Änderungen

Zugehörige Dokumente:

- AWS Builders' Library | Automatisierung sicherer, vollautomatischer Bereitstellungen | Testbereitstellungen
- AWS-Whitepaper | Durchführung von dauerhafter Integration/dauerhafter Bereitstellung in AWS
- The Story of Apollo – Amazon's Deployment Engine (Apollo – die Bereitstellungs-Engine von Amazon)
- Vorgehensweise für den lokalen Test und lokales Debugging von AWS CodeDeploy vor der Auslieferung Ihres Codes

- Integrating Network Connectivity Testing with Infrastructure Deployment (Integration von Netzwerkkonnektivitätstests in die Bereitstellung der Infrastruktur)

Zugehörige Videos:

- re:Invent 2020 | Testing software and systems at Amazon (re:Invent 2020 | Testen von Software und Systemen bei Amazon)

Zugehörige Beispiele:

- Tutorial | Bereitstellen eines Amazon ECS-Services mit einem Validierungstest

OPS06-BP03 Einsetzen sicherer Bereitstellungsstrategien

Sichere Produktionseinführungen steuern den Fluss vorteilhafter Änderungen mit dem Ziel, die von den Kunden wahrgenommenen Auswirkungen dieser Änderungen zu minimieren. Die Sicherheitskontrollen bieten Prüfmechanismen, um die gewünschten Ergebnisse zu validieren und den Umfang der Auswirkungen von Fehlern zu begrenzen, die durch die Änderungen oder durch Fehler bei der Bereitstellung verursacht werden. Zu sicheren Rollouts können Strategien wie Feature-Flags, One-Box, Rolling (Canary-Releases), Immutable, Aufteilung des Datenverkehrs und Blau/Grün-Bereitstellungen gehören.

Gewünschtes Ergebnis: Ihr Unternehmen verwendet ein CI/CD-System (Continuous integration and continuous delivery, kontinuierliche Integration und kontinuierliche Bereitstellung), das Funktionen zur Automatisierung sicherer Rollouts bietet. Die Teams müssen angemessene sichere Rollout-Strategien anwenden.

Typische Anti-Muster:

- Sie stellen eine nicht erfolgreiche Änderung für die gesamte Produktion gleichzeitig bereit. Infolgedessen sind alle Kunden gleichzeitig betroffen.
- Ein Fehler, der bei einer gleichzeitigen Bereitstellung in allen Systemen auftritt, erfordert ein Notfall-Release. Die Korrektur für alle Kunden dauert mehrere Tage.
- Die Verwaltung der Produktionseinführung erfordert die Planung und Beteiligung mehrerer Teams. Dies schränkt Ihre Fähigkeit ein, Features für Ihre Kunden häufig zu aktualisieren.
- Sie führen eine veränderbare Bereitstellung durch, indem Sie Ihre vorhandenen Systeme ändern. Nachdem Sie festgestellt haben, dass die Änderung nicht erfolgreich war, müssen Sie die

Systeme erneut ändern, um die alte Version wiederherzustellen, was die Wiederherstellungsdauer verlängert.

Vorteile der Nutzung dieser bewährten Methode: Automatisierte Bereitstellungen sorgen für ein ausgewogenes Verhältnis zwischen der Geschwindigkeit der Bereitstellungen und der konsistenten Bereitstellung nützlicher Änderungen für die Kunden. Die Begrenzung der Auswirkungen verhindert kostspielige Bereitstellungsfehler und maximiert die Fähigkeit der Teams, effizient auf Ausfälle zu reagieren.

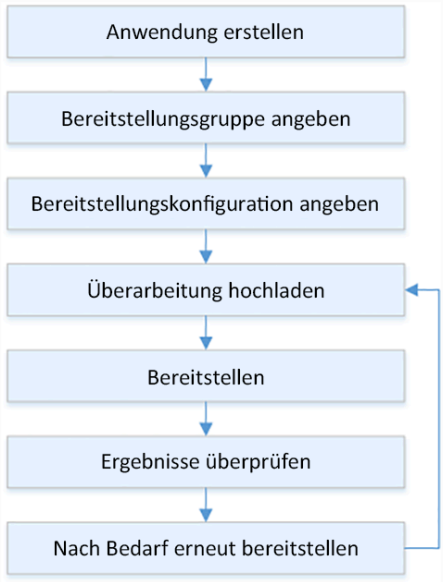
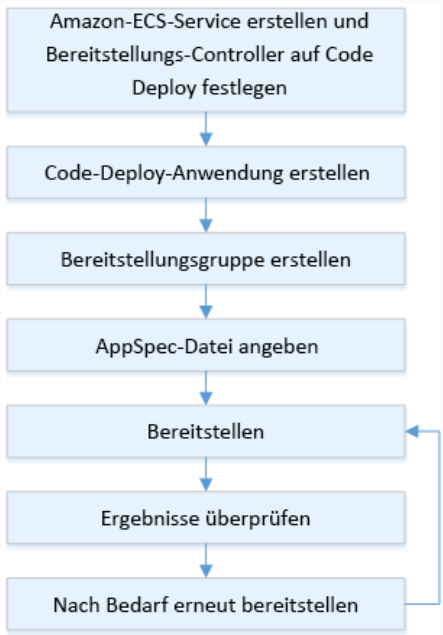
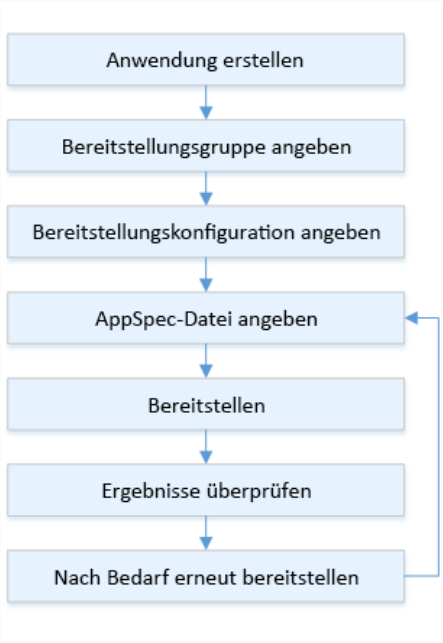
Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Ausfälle bei der kontinuierlichen Bereitstellung können zu einer verringerten Serviceverfügbarkeit und schlechten Kundenerfahrungen führen. Um die Anzahl erfolgreicher Implementierungen zu maximieren, sollten Sie im gesamten Release-Prozess Sicherheitskontrollen zur Minimierung von Bereitstellungsfehlern implementieren. Das Ziel sollte dabei sein, dass keine Bereitstellungsfehler auftreten.

Kundenbeispiel

AnyCompany Retail möchte Bereitstellungen mit minimalen bis gar keinen Ausfallzeiten erreichen, d. h. es soll während der Bereitstellung keine spürbaren Auswirkungen für die Benutzer geben. Um dies zu erreichen, hat das Unternehmen Bereitstellungsmuster festgelegt, z. B. fortlaufende und Blau/Grün-Bereitstellung (siehe nachfolgendes Workflow-Diagramm). Alle Teams übernehmen eines oder mehrere dieser Muster in ihre CI/CD-Pipeline.

CodeDeploy-Workflow für Amazon EC2	CodeDeploy-Workflow für Amazon ECS	CodeDeploy-Workflow für Lambda
		

Implementierungsschritte

1. Verwenden Sie einen Genehmigungsworkflow, um die Reihenfolge der Produktionseinführungsschritte nach der Beförderung zur Produktion einzuleiten.
2. Verwenden Sie ein automatisiertes Bereitstellungssystem wie AWS CodeDeploy. AWS CodeDeploy- Bereitstellungsoptionen schließen lokale Bereitstellungen für EC2/On-Premises und Blau/Grün-Bereitstellungen für EC2/On-Premises ein, AWS Lambda und Amazon ECS (siehe vorhergehendes Workflow-Diagramm).
   a. Wo zutreffend, integrieren Sie AWS CodeDeploy in andere AWS-Services oder integrieren Sie AWS CodeDeploy in Produkte und Services von Partnern.
3. Verwenden Sie Blau/Grün-Bereitstellungen für Datenbanken wie Amazon Aurora und Amazon RDS.
4. Überwachen Sie Bereitstellungen mithilfe von Ereignisbenachrichtigungen von Amazon CloudWatch, AWS CloudTrail und Amazon Simple Notification Service (Amazon SNS).
5. Führen Sie nach der Bereitstellung automatisierte Tests durch, einschließlich Funktions-, Sicherheits-, Regressions-, Integrations- und Auslastungstests.
6. Behandlung von Problemen bei der Bereitstellung.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP02 Testen und Validieren von Änderungen
- OPS05-BP09 Häufige, kleine, reversible Änderungen vornehmen
- OPS05-BP10 Vollständige Automatisierung von Integration und Bereitstellung

Zugehörige Dokumente:

- AWS Builders' Library | Automatisierung sicherer, vollautomatischer Bereitstellungen | Produktionsbereitstellungen
- AWS Builders' Library | Meine CI/CD-Pipeline ist mein Release Captain | Sichere, automatische Produktionseinführungen
- AWS-Whitepaper | Durchführung von dauerhafter Integration/dauerhafter Bereitstellung in AWS | Bereitstellungsmethoden
- AWS CodeDeploy-Benutzerhandbuch
- Arbeiten mit Bereitstellungskonfigurationen in AWS CodeDeploy
- Einrichten einer API Gateway-Canary-Bereitstellung als Release
- Amazon ECS-Bereitstellungstypen
- Vollständig verwaltete Blau/Grün-Bereitstellungen in Amazon Aurora und Amazon RDS
- Blau/Grün-Bereitstellungen mit AWS Elastic Beanstalk

Zugehörige Videos:

- re:Invent 2020 | Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon
- re:Invent 2019 | Der Amazon-Ansatz für die Hochverfügbarkeitsbereitstellung

Zugehörige Beispiele:

- Testen einer Blau/Grün-Bereitstellung in AWS CodeDeploy
- Workshop | Erstellen von CI/CD-Pipelines für Lambda-Canary-Bereitstellungen mit AWS CDK

- Workshop | Blau/Grün- und Canary-Bereitstellungen für EKS und ECS
- Workshop | Erstellen einer kontenübergreifenden CI/CD-Pipeline

OPS06-BP04 Automatisieren von Tests und Rollback

Um die Geschwindigkeit, Zuverlässigkeit und Sicherheit Ihres Bereitstellungsprozesses zu erhöhen, sollten Sie eine Strategie für automatisierte Test- und Rollback-Funktionen in Vorproduktions- und Produktionsumgebungen entwickeln. Automatisieren Sie Tests bei der Bereitstellung in der Produktion, um Interaktionen zwischen Mensch und System zu simulieren und die bereitgestellten Änderungen zu überprüfen. Automatisieren Sie das Rollback, um schnell zu einem als funktionierend bekannten Zustand zurückkehren zu können. Das Rollback sollte unter vordefinierten Bedingungen automatisch eingeleitet werden, z. B. wenn das gewünschte Ergebnis einer Änderung nicht erreicht wird oder wenn der automatisierte Test fehlschlägt. Die Automatisierung dieser beiden Aktivitäten verbessert Ihre Erfolgsquote bei Bereitstellungen, minimiert die Wiederherstellungszeit und reduziert die potenziellen Auswirkungen auf das Unternehmen.

Gewünschtes Ergebnis: Ihre automatisierten Tests und Rollback-Strategien sind in Ihre CI/CD-Pipeline (Continuous Integration and Continuous Delivery, kontinuierliche Integration und kontinuierliche Bereitstellung) integriert. Ihre Überwachung kann Validierungen anhand Ihrer Erfolgskriterien ausführen und bei einem Fehler ein automatisches Rollback einleiten. Dadurch werden die Auswirkungen auf Endbenutzer und Kunden minimiert. Wenn beispielsweise alle Testergebnisse den Anforderungen entsprechen, übertragen Sie Ihren Code in die Produktionsumgebung, wo automatisierte Regressionstests unter Verwendung derselben Testfälle eingeleitet werden. Wenn die Ergebnisse der Regressionstests nicht den Erwartungen entsprechen, wird im Pipeline-Workflow ein automatisiertes Rollback eingeleitet.

Typische Anti-Muster:

- Ihre Systeme sind nicht so konzipiert, dass sie mit kleineren Releases aktualisiert werden können. Daher haben Sie Schwierigkeiten, die Bulk-Änderungen während einer fehlgeschlagenen Bereitstellung rückgängig zu machen.
- Ihr Bereitstellungsprozess besteht aus einer Reihe manueller Schritte. Nachdem Sie Änderungen an Ihrem Workload bereitgestellt haben, beginnen Sie mit den Tests nach der Bereitstellung. Danach bemerken Sie, dass Ihr Workload nicht mehr funktioniert und die Verbindung der Kunden getrennt wird. Sie starten das Rollback zur vorherigen Version. All diese manuellen Schritte verzögern die allgemeine Systemwiederherstellung und wirken sich nachhaltig auf Ihre Kunden aus.

- Sie haben Zeit dafür aufgewendet, automatisierte Testfälle für Funktionen zu entwickeln, die in Ihrer Anwendung nicht häufig verwendet werden. Dadurch amortisiert sich die Investition in Ihre automatisierten Testfunktionen nur schlecht.
- Ihre Version besteht aus Anwendungs-, Infrastruktur-, Patch- und Konfigurations-Updates, die voneinander unabhängig sind. Sie haben jedoch nur eine CI/CD-Pipeline, die alle Änderungen gleichzeitig bereitstellt. Ein Fehler in einer Komponente zwingt Sie, alle Änderungen rückgängig zu machen, wodurch Ihr Rollback komplex und ineffizient wird.
- Ihr Team schließt die Programmierarbeiten im ersten Sprint ab und beginnt mit dem zweiten Sprint, aber Ihr Plan sieht Tests erst im dritten Sprint vor. Deshalb haben automatisierte Tests Fehler aus dem ersten Sprint aufgedeckt, die behoben werden müssen, bevor mit dem Testen der Ergebnisse von Sprint zwei begonnen werden kann. Der gesamte Release verzögert sich, wodurch der Wert Ihrer automatisierten Tests erheblich verringert wird.
- Ihre automatisierten Regressionstestfälle für die Produktionsversion sind abgeschlossen, aber Sie überwachen den Zustand der Workloads nicht. Da Sie nicht sehen können, ob der Dienst neu gestartet wurde oder nicht, sind Sie sich nicht sicher, ob ein Rollback erforderlich ist oder bereits stattgefunden hat.

Vorteile der Nutzung dieser bewährten Methode: Automatisierte Tests erhöhen die Transparenz Ihres Testprozesses und Ihre Fähigkeit, mehr Funktionen in kürzerer Zeit abzudecken. Durch das Testen und Validieren von Änderungen in der Produktionsphase können Sie Probleme sofort identifizieren. Die Verbesserung der Konsistenz mit automatisierten Testtools ermöglicht eine bessere Fehlererkennung. Durch das automatische Rollback zur vorherigen Version werden die Auswirkungen für Ihre Kunden minimiert. Ein automatisiertes Rollback sorgt letztendlich für mehr Vertrauen in Ihre Bereitstellungsfunktionen, da es die Auswirkungen auf Ihr Unternehmen verringert. Insgesamt verkürzen diese Funktionen die Zeit bis zur Lieferung und stellen gleichzeitig die Qualität sicher.

Risikostufe bei fehlender Befolgung dieser Best Practice: Mittel

Implementierungsleitfaden

Automatisieren Sie die Tests von bereitgestellten Umgebungen, um schneller die gewünschten Ergebnisse zu erreichen. Automatisieren Sie den Rollback zu einem bekanntermaßen funktionierenden vorherigen Zustand, wenn die zuvor definierten Ergebnisse nicht erzielt werden. So können Sie die Wiederherstellungszeit minimieren und verringern Fehler, die durch manuelle Prozesse entstehen. Integrieren Sie Testtools in Ihren Pipeline-Workflow, um manuelle Eingaben konsistent zu testen und zu minimieren. Priorisieren Sie die Automatisierung von Testfällen, z. B.

Tests, die die größten Risiken minimieren und die bei jeder Änderung häufig durchgeführt werden müssen. Automatisieren Sie außerdem das Rollback auf Grundlage bestimmter Bedingungen, die in Ihrem Testplan vordefiniert sind.

Implementierungsschritte

1. Richten Sie einen Testlebenszyklus für Ihren Entwicklungslebenszyklus ein, in dem jede Phase des Testprozesses definiert wird. Dies reicht von der Anforderungsplanung über die Testfallentwicklung, die Toolkonfiguration, das automatisierte Testen bis hin zum Abschluss des Testfalls.
   a. Erstellen Sie anhand Ihrer gesamten Teststrategie einen Workload-spezifischen Testansatz.
   b. Ziehen Sie eine Strategie für kontinuierliche Tests während des gesamten Entwicklungszyklus in Erwägung.
2. Wählen Sie in Abhängigkeit von Ihren Geschäftsanforderungen und Pipeline-Investitionen automatisierte Tools für Tests und Rollbacks aus.
3. Entscheiden Sie, welche Testfälle Sie automatisieren möchten und welche manuell durchgeführt werden sollen. Dies kann auf Grundlage des geschäftlichen Nutzens der getesteten Funktion definiert werden. Informieren Sie alle Teammitglieder über diesen Plan und legen Sie fest, wer für die Durchführung manueller Tests verantwortlich ist.
   a. Wenden Sie automatisierte Testfunktionen auf bestimmte Testfälle an, die für die Automatisierung sinnvoll sind, z. B. wiederholbare oder häufig ausgeführte Fälle, Fälle, die sich wiederholende Aufgaben erfordern, oder solche, die für mehrere Konfigurationen erforderlich sind.
   b. Definieren Sie Skripts für die Testautomatisierung sowie die Erfolgskriterien im Automatisierungstool, sodass eine kontinuierliche Workflow-Automatisierung initiiert werden kann, wenn bei bestimmten Fällen Fehler auftreten.
   c. Definieren Sie spezifische Fehlerkriterien für das automatisierte Rollback.
4. Priorisieren Sie die Testautomatisierung, um konsistente Ergebnisse mit einer gründlichen Testfallentwicklung zu erzielen, bei der Komplexität und menschliche Interaktion ein höheres Ausfallrisiko darstellen.
5. Integrieren Sie Ihre automatisierten Test- und Rollback-Tools in Ihre CI/CD-Pipeline.
   a. Entwickeln Sie klare Erfolgskriterien für Ihre Änderungen.
   b. Überwachen und beobachten Sie Ihre Umgebung, um diese Kriterien zu erkennen und Änderungen automatisch rückgängig zu machen, wenn bestimmte Rollback-Kriterien erfüllt werden.

6. Führen Sie verschiedene Arten automatisierter Produktionstests durch, z. B.:
   a. A/B-Tests zur Anzeige von Ergebnissen im Vergleich zur aktuellen Version zwischen zwei Benutzertestgruppen.
   b. Canary-Tests, mit denen Sie Ihre Änderung für eine Untergruppe von Benutzern bereitstellen können, bevor Sie sie für alle freigeben.
   c. Testen mit Feature-Flags, wobei jeweils eine einzelne Funktion der neuen Version außerhalb der Anwendung ein- und ausgeschaltet werden kann, sodass alle neuen Funktionen einzeln validiert werden können.
   d. Regressionstests zur Überprüfung neuer Funktionen mit bestehenden, miteinander verbundenen Komponenten.
7. Überwachen Sie die betrieblichen Aspekte der Anwendung, Transaktionen und Interaktionen mit anderen Anwendungen und Komponenten. Entwickeln Sie Berichte, um den Erfolg von Änderungen nach Workload aufzuzeigen, sodass Sie erkennen können, welche Teile der Automatisierung und des Workflows weiter optimiert werden können.
   a. Entwickeln Sie Testergebnisberichte, anhand derer Sie schnell entscheiden können, ob Rollback-Verfahren eingeleitet werden sollten oder nicht.
   b. Implementieren Sie eine Strategie, die ein automatisiertes Rollback auf Grundlage vordefinierter Fehlerbedingungen ermöglicht, die sich aus einer oder mehreren Ihrer Testmethoden ergeben.
8. Entwickeln Sie Ihre automatisierten Testfälle so, dass sie bei zukünftigen wiederholbaren Änderungen wiederverwendet werden können.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS06-BP01 Einkalkulieren nicht erfolgreicher Änderungen
- OPS06-BP02 Testbereitstellungen

Zugehörige Dokumente:

- AWS Builders' Library | Gewährleistung der Rollback-Sicherheit bei Bereitstellungen
- Erneutes Bereitstellen und Zurücksetzen einer Bereitstellung mit AWS CodeDeploy
- 8 bewährte Methoden beim Automatisieren von Bereitstellungen mit AWS CloudFormation

Zugehörige Beispiele:

- Serverless-Tests für UI mit Selenium, AWS Lambda, AWS Fargate (Fargate) und AWS Developer Tools

Zugehörige Videos:

- re:Invent 2020 | Hands-off: Automating continuous delivery pipelines at Amazon (re:Invent 2020 | Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon)
- re:Invent 2019 | Amazon’s approach to high-availability deployment (re:Invent 2019 | Der Amazon-Ansatz für die Hochverfügbarkeitsbereitstellung)

Operative Bereitschaft und Änderungsverwaltung

Bewerten Sie die operative Bereitschaft Ihres Workloads, der Prozesse und Verfahren sowie Ihrer Mitarbeiter, damit Sie die operativen Risiken im Zusammenhang mit Ihrem Workload genau kennen. Verwalten Sie den Änderungsfluss in Ihre Umgebungen.

Sie sollten einen konsistenten Prozess (inklusive manueller und automatisierter Checklisten) anwenden, damit Sie wissen, wann Sie bereit sind, Ihren Workload oder eine Änderung live zu schalten. Auf diese Weise können Sie auch alle Bereiche finden, um die Sie sich kümmern müssen. Ihre routinemäßigen Aktivitäten werden Sie in Runbooks notieren und Playbooks werden Ihnen bei der Lösung von Problemen helfen. Verwenden Sie einen Mechanismus zur Verwaltung von Änderungen, der die Erzielung eines geschäftlichen Nutzens unterstützt und dazu beiträgt, mit den Änderungen verbundene Risiken zu mindern.

Bewährte Methoden

- OPS07-BP01 Sicherstellen des Know-hows der Mitarbeiter
- OPS07-BP02 Sicherstellen einer konsistenten Prüfung der betrieblichen Bereitschaft
- OPS07-BP03 Verwenden von Runbooks zur Durchführung von Verfahren
- OPS07-BP04 Verwenden von Playbooks zum Untersuchen von Problemen
- OPS07-BP05 Treffen fundierter Entscheidungen für die Bereitstellung von Systemen und Änderungen
- OPS07-BP06 Aktivieren von Supportplänen für Produktions-Workloads

OPS07-BP01 Sicherstellen des Know-hows der Mitarbeiter

Nutzen Sie ein System, mit dem Sie validieren können, dass Sie über eine angemessene Anzahl von trainierten Mitarbeitern verfügen, um den Workload zu unterstützen. Sie müssen für die Plattform und die Services, die Ihren Workload ausmachen, trainiert sein. Vermitteln Sie ihnen das für den Betrieb des Workloads erforderliche Wissen. Sie müssen über genügend geschulte Mitarbeiter verfügen, um den normalen Betrieb des Workloads zu unterstützen und auftretende Probleme zu beheben. Sorgen Sie für genügend Mitarbeiter, sodass Sie Bereitschaftsdienste und Urlaubsvertretungen abwechseln können, um Burnouts zu vermeiden.

Gewünschtes Ergebnis:

- Es gibt genügend trainierte Mitarbeiter, um den Workload im Rahmen des Verfügbarkeitszeitraums zu unterstützen.
- Sie trainieren Ihre Mitarbeiter für die Software und Services, die Ihren Workload ausmachen.

Typische Anti-Muster:

- Bereitstellen eines Workloads ohne Teammitglieder, die für den Betrieb der Plattform und der genutzten Services trainiert sind.
- Sie haben nicht genug Mitarbeiter, um wechselnde Bereitschaftsdienste oder Urlaubszeiten abzubilden.

Vorteile der Nutzung dieser bewährten Methode:

- Wenn Sie über qualifizierte Teammitglieder verfügen, können sie Ihren Workload effektiv unterstützen.
- Mit einer ausreichenden Anzahl von Teammitgliedern können Sie den Workload und die Rotation der Bereitschaftsdienste unterstützen und gleichzeitig das Risiko eines Burnouts verringern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Validieren Sie, ob ausreichend trainierte Mitarbeiter für den Support des Workloads vorhanden sind. Vergewissern Sie sich, dass Sie über genügend Teammitglieder verfügen, um die normalen operativen Aktivitäten, einschließlich Einsatzbereitschaftsdienste, abzudecken.

Kundenbeispiel

AnyCompany Retail sorgt dafür, dass die Teams für den Workload angemessen besetzt und trainiert sind. Es gibt genügend Ingenieure, um wechselnde Bereitschaftsdienste zu unterstützen. Die Mitarbeiter erhalten Training, um die Software und die Workload-Plattform zu nutzen. Sie werden außerdem ermutigt, Zertifizierungen zu erwerben. Es gibt so viele Mitarbeiter, dass Urlaub möglich ist, ohne dass der Workload und die rotierenden Bereitschaftsdienste unterbrochen werden müssen.

Implementierungsschritte

1. Weisen Sie eine ausreichende Anzahl von Mitarbeitern für den Betrieb und den Support Ihres Workloads zu – einschließlich der Bereitschaftsdienste.
2. Trainieren Sie die Mitarbeiter im Umgang mit der Software und den Plattformen, die Ihren Workload ausmachen.
   a. Bei AWS Training und Zertifizierung finden Sie eine Bibliothek mit Kursen zu AWS. Es gibt kostenlose und kostenpflichtige Kurse – online und vor Ort.
   b. AWS hostet Veranstaltungen und Webinare, bei denen Sie von AWS Experten lernen.
3. Bewerten Sie regelmäßig die Größe und die Fähigkeiten des Teams, wenn sich die operativen Bedingungen und der Workload verändern. Passen Sie die Größe und Fähigkeiten des Teams an die operativen Anforderungen an.

Grad des Aufwands für den Implementierungsplan: hoch Das Einstellen und Trainieren eines Teams zur Unterstützung eines Workloads kann einen erheblichen Aufwand darstellen, bietet aber langfristig einen bedeutenden Nutzen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS11-BP04 Wissensmanagement - Die Teammitglieder müssen über die notwendigen Informationen verfügen, um den Workload zu betreiben und zu unterstützen. Der Schlüssel dazu ist das Wissensmanagement.

Zugehörige Dokumente:

- AWS-Veranstaltungen und -Webinare
- AWS Training und Zertifizierung

OPS07-BP02 Sicherstellen einer konsistenten Prüfung der betrieblichen Bereitschaft

Verwenden Sie Operational Readiness Reviews (ORRs, Überprüfungen der Einsatzbereitschaft), um zu prüfen, ob Sie Ihren Workload betreiben können. ORR ist ein bei Amazon entwickelter Mechanismus zur Prüfung, ob Teams ihre Workloads in sicherer Weise betreiben können. ORR bezeichnet einen Prüfungs- und Inspektionsprozess anhand einer Checkliste mit Anforderungen. Dies ist ein Self-Service-Vorgang, mit dem Teams ihre Workloads zertifizieren. ORRs beinhalten bewährte Methoden aus unseren jahrelangen Erfahrungen bei der Erstellung von Software.

Eine ORR-Checkliste besteht aus Architekturempfehlungen, betrieblichen Prozessen, Ereignismanagement und Freigabequalität. Unser Correction of Error (CoE)-Prozess ist dafür eine sehr wichtige Grundlage. Ihre eigene Analyse nach einem Vorfall sollte die Weiterentwicklung Ihrer eigenen ORR unterstützen. Bei einer ORR geht es nicht nur um die Umsetzung bewährter Methoden, sondern auch darum, das erneute Auftreten von Ereignissen zu verhindern. Schließlich können auch Sicherheit, Governance und Compliance zu einer ORR gehören.

Führen Sie eine ORR durch, bevor ein Workload zur allgemeinen Verfügbarkeit gestartet wird, und anschließend während des gesamten Softwareentwicklungslebenszyklus. Die Durchführung der ORR vor dem Start verbessert Ihre Fähigkeit zum sicheren Betrieb des Workloads. Führen Sie die ORR auf dem Workload regelmäßig erneut durch, um Abweichungen von bewährten Methoden zu erkennen. Sie können ORR-Checklisten für neue Serviceeinführungen oder für regelmäßige Prüfungen haben. So bleiben Sie hinsichtlich der neuen bewährten Methoden auf dem Laufenden und können Erfahrungen aus Analysen nach Vorfällen einarbeiten. Wenn Sie mit der Cloud immer vertrauter werden, können Sie ORR-Anforderungen als Standardelemente in Ihre Architektur einbauen.

Gewünschtes Ergebnis: Sie haben eine ORR-Checkliste mit bewährten Methoden für Ihre Organisation. ORRs werden vor dem Start von Workloads durchgeführt. ORR werden im Laufe des Workloadlebenszyklus regelmäßig durchgeführt.

Typische Anti-Muster:

- Sie starten einen Workload, ohne zu wissen, ob Sie diesen betreiben können.
- Governance- und Sicherheitsanforderungen gehören nicht zur Zertifizierung eines Workloads für den Start.
- Workloads werden nicht regelmäßig erneut bewertet.
- Workloads werden gestartet, ohne dass erforderliche Verfahren eingerichtet sind.

- Sie erleben die Wiederholung von Ausfällen mit der gleichen Ursache bei mehreren Workloads.

Vorteile der Nutzung dieser bewährten Methode:

- Ihre Workloads beinhalten bewährte Methoden für Architektur, Prozess und Management.
- Erkenntnisse werden in Ihren ORR-Prozess integriert.
- Workloads werden gestartet, wenn erforderliche Verfahren eingerichtet sind.
- ORRs werden über den gesamten Softwarelebenszyklus Ihrer Workloads hinweg ausgeführt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Eine ORR ist zweierlei: ein Verfahren und eine Checkliste. Ihr ORR-Verfahren sollte von ihrer Organisation übernommen und von der Unternehmensleitung unterstützt werden. ORRs müssen mindestens durchgeführt werden, bevor Workloads zur allgemeinen Verfügbarkeit gestartet werden. Führen Sie die ORR während des gesamten Lebenszyklus der Softwareentwicklung durch, um ihn bei bewährten Methoden oder neuen Anforderungen aktuell zu halten. Die ORR-Checkliste sollte Konfigurationselemente, Sicherheits- und Governance-Elemente sowie bewährte Methoden aus Ihrer Organisation enthalten. Mit der Zeit können Sie Services wie AWS Config, AWS Security Hubund AWS Control Tower Guardrailsverwenden, um bewährte Methoden aus der ORR in den Integritätsschutz für die automatische Erkennung optimaler Verfahrensweisen aufzunehmen.

Kundenbeispiel

Nach mehreren Produktionsvorfällen entschied sich AnyCompany Retail, einen ORR-Prozess zu implementieren. Das Unternehmen erstellte eine Checkliste mit bewährten Methoden sowie Governance- und Compliance-Anforderungen und Erfahrungen aus früheren Ausfällen. Für neue Workloads werden vor dem Start ORRs durchgeführt. Für jeden Workload wird eine jährliche ORR mit einer Teilmenge der bewährten Methoden durchgeführt, um neue bewährte Methoden und Anforderungen umzusetzen, die der ORR-Checkliste hinzugefügt werden. Mit der Zeit verwendete AnyCompany Retail AWS Config zur Aufdeckung einer bewährter Methoden, was den ORR-Prozess beschleunigte.

Implementierungsschritte

Weitere Informationen zu ORRs finden Sie im Whitepaper zur Überprüfung der betrieblichen Bereitschaft (ORR). Hier finden Sie ausführliche Informationen zur Geschichte des ORR-Verfahrens,

zum Aufbau Ihrer eigenen ORR-Praxis und zur Erstellung Ihrer ORR-Checkliste. Die folgenden Schritte sind eine verkürzte Version dieses Dokuments. Für ein vertieftes Verständnis des ORR-Konzepts und der Erstellung eigener ORRs empfehlen wir, das Whitepaper zu lesen.

1. Bringen Sie die wichtigsten Beteiligten zusammen, darunter auch Vertreter aus den Bereichen Sicherheit, Operations und Entwicklung.
2. Lassen Sie alle Beteiligten mindestens eine Anforderung beisteuern. Versuchen Sie für den ersten Durchgang die Anzahl der Elemente auf höchstens dreißig zu beschränken.
   - Anhang B: Beispielfragen für ORRs aus dem ORR-Whitepaper enthält Beispielfragen, die Ihnen beim Start helfen können.
3. Fassen Sie Ihre Anforderungen in einer Tabelle zusammen.
   - Sie können Fokusbereiche in AWS Well-Architected Tool verwenden, um Ihre ORR zu entwickeln und an Ihre Konten und die AWS-Organisation weiterzugeben.
4. Identifizieren Sie einen Workload für die ORR. Ideal ist dafür ein Pre-Launch-Workload oder ein interner Workload.
5. Gehen Sie die ORR-Checkliste durch und notieren Sie alle Erkenntnisse. Diese sind möglicherweise nicht OK, wenn eine Behebung stattfindet. Fügen Sie alle Erkenntnisse ohne Behebung Ihrer Liste hinzu und implementieren Sie die Behebungen vor dem Start.
6. Fügen Sie Ihrer ORR-Checkliste stets weitere bewährte Methoden und Anforderungen hinzu.

AWS Support-Kunden mit Enterprise Support können den Operational Readiness Review Workshop bei ihrem Technical Account Manager anfordern. Der Workshop ist eine interaktive „Working Backwards“- Sitzung zur Entwicklung Ihrer eigenen ORR-Checkliste.

Aufwand für den Implementierungsplan: Hoch. Die Einführung einer ORR-Praxis in Ihrer Organisation erfordert die Unterstützung durch Führungskräfte und alle Beteiligten. Erstellen und aktualisieren Sie die Checkliste mit Beiträgen aus der gesamten Organisation.

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP03 Bewerten der Governance-Anforderungen – Governance-Anforderungen passen perfekt zu einer ORR-Checkliste
- OPS01-BP04 Bewerten der Compliance-Anforderungen – Compliance-Anforderungen werden manchmal auf ORR-Checklisten berücksichtigt. Ansonsten sind sie ein separater Prozess.

- OPS03-BP07 Teams mit entsprechenden Ressourcen ausstatten – Die Team-Kapazität ist ein guter Kandidat für eine ORR-Anforderung.
- OPS06-BP01 Einkalkulieren nicht erfolgreicher Änderungen – Vor dem Start Ihres Workloads muss ein Rollback- oder Rollforward-Plan eingerichtet werden.
- OPS07-BP01 Sicherstellen des Know-hows der Mitarbeiter – Zur Unterstützung eines Workloads benötigen Sie das erforderliche Personal.
- SEC01-BP03 Identifizieren und Validieren von Kontrollzielen – Sicherheitskontrollziele sind hervorragende ORR-Anforderungen.
- REL13-BP01 Definieren von Wiederherstellungszielen bei Ausfällen und Datenverlusten – Notfallwiederherstellungspläne sind eine gute ORR-Anforderung.
- COST02-BP01 Entwickeln von Richtlinien auf Basis Ihrer Organisationsanforderungen – Kostenmanagementrichtlinien sind für Ihre ORR-Checkliste gut geeignet.

Zugehörige Dokumente:

- AWS Control Tower - Integritätsschutz in AWS Control Tower
- AWS Well-Architected Tool - Fokusbereiche
- Operational Readiness Review Template von Adrian Hornsby
- Whitepaper zur Überprüfung der betrieblichen Bereitschaft (ORR)

Zugehörige Videos:

- AWS Supports You | Building an Effective Operational Readiness Review (ORR) (AWS Supports You | Entwickeln einer effektiven Überprüfung der betrieblichen Bereitschaft (ORR))

Zugehörige Beispiele:

- Sample Operational Readiness Review (ORR)-Fokusbereich

Zugehörige Services:

- AWS Config
- AWS Control Tower
- AWS Security Hub

- AWS Well-Architected Tool

OPS07-BP03 Verwenden von Runbooks zur Durchführung von Verfahren

Ein Runbook ist ein dokumentierter Prozess für das Erreichen eines bestimmten Ergebnisses. Runbooks bestehen aus einer Reihe von Schritten, die befolgt werden sollen, um ein Ergebnis zu erzielen. Runbooks werden schon seit den frühen Tagen der Luftfahrt verwendet. Im Cloud-Bereich werden Runbooks verwendet, um die Risiken zu reduzieren und die gewünschten Ergebnisse zu erzielen. In der einfachsten Form ist ein Runbook eine Checkliste für die Durchführung einer Aufgabe.

Runbooks stellen einen kritischen Teil der Ausführung Ihres Workloads dar. Vom Onboarding eines neuen Teammitglieds bis zur Bereitstellung einer Hauptversion – Runbooks stellen kodifizierte Prozesse dar, mit denen unabhängig von der ausführenden Person konsistente Ergebnisse erzielt werden können. Runbooks sollten an einer zentralen Stelle veröffentlicht werden. Wenn sich der Prozess verändert, sollten sie aktualisiert werden; dies stellt eine zentrale Komponente des Änderungsmanagements dar. Sie sollten auch Anleitungen für Fehlerbehandlung, Tools, Berechtigungen, Ausnahmen und Eskalationen enthalten, falls ein Problem auftritt.

Wenn sich Ihre Organisation entwickelt, sollten Sie mit der Automatisierung von Runbooks beginnen. Sie sollten zunächst Runbooks automatisieren, die kurz sind und häufig verwendet werden. Verwenden Sie Skriptsprachen, um Schritte zu automatisieren oder ihre Ausführung zu vereinfachen. Nach der Automatisierung der ersten Runbooks können Sie komplexere Runbooks automatisieren. Mit der Zeit sollten die meisten Ihrer Runbooks auf die eine oder andere Art automatisiert werden.

Gewünschtes Ergebnis: Ihr Team besitzt eine Sammlung von schrittweisen Anleitungen für die Ausführung von Workload-Aufgaben. Die Runbooks enthalten Angaben zum gewünschten Ergebnis sowie zu notwendigen Tools und Berechtigungen. Darüber hinaus stellen sie Anleitungen für die Fehlerbehandlung bereit. Sie werden an einem zentralen Ort (Versionskontrollsystem) gespeichert und regelmäßig aktualisiert. Ihre Runbooks bieten Ihren Teams beispielsweise die Möglichkeit, AWS Health-Ereignisse für kritische Konten bei Anwendungsalarmen, Betriebsproblemen und geplanten Lebenszyklusereignissen zu überwachen, zu kommunizieren und darauf zu reagieren.

Typische Anti-Muster:

- Verlassen auf das Gedächtnis, um die einzelnen Schritte in einem Prozess durchzuführen.
- Manuelle Bereitstellung von Änderungen ohne Checkliste.
- Verschiedene Teammitglieder führen den gleichen Prozess aus, aber mit unterschiedlichen Schritten oder Ergebnissen.

- Runbooks sind nicht mehr mit Systemänderungen und Automatisierungen synchronisiert.

Vorteile der Nutzung dieser bewährten Methode:

- Reduzierung der Fehlerquoten für manuelle Aufgaben.
- Prozess werden konsistent ausgeführt.
- Neue Teammitglieder können schneller mit der Ausführung von Aufgaben beginnen.
- Runbooks können automatisiert werden, um den Aufwand zu reduzieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Runbooks können verschiedene Formen annehmen, abhängig vom Entwicklungsstand Ihrer Organisation. Sie sollten mindestens aus einem Schritt-für-Schritt-Textdokument bestehen. Das gewünschte Ergebnis sollte klar angegeben werden. Dokumentieren Sie klar die notwendigen Berechtigungen oder Tools. Stellen Sie für den Fall, dass etwas nicht funktioniert, detaillierte Anleitungen für Fehlerbehandlung und Eskalation bereit. Nennen Sie die Person, die für das Runbook verantwortlich ist, und veröffentlichen Sie es an einer zentralen Stelle. Validieren Sie das Runbook, nachdem Sie es dokumentiert haben, indem Sie es von einem Teammitglied ausführen lassen. Mit der weiteren Entwicklung der Verfahren sollten Sie Ihre Runbooks entsprechend Ihrem Prozess für das Änderungsmanagement aktualisieren.

Ihre textbasierten Runbooks sollten mit zunehmender Reife Ihrer Organisation automatisiert werden. Mithilfe von Services wie AWS Systems Manager-Automatisierungen können Sie einfachen Text in Automatisierungen umwandeln, die für Ihr Workload ausgeführt werden können. Diese Automatisierungen können als Reaktion auf Ereignisse ausgeführt werden, was den operativen Aufwand für die Wartung des Workloads reduziert. Die AWSSystems Manager-Automatisierung bietet auch ein visuelles Low-Code-Designerlebnis, mit dem Automatisierungs-Runbooks einfacher erstellt werden können.

Kundenbeispiel

AnyCompany Retail muss während Softwarebereitstellungen die Datenbankschemata aktualisieren. Das Cloud Operations-Team entwickelt gemeinsam mit dem Datenbankverwaltungsteam ein Runbook für die manuelle Bereitstellung dieser Änderungen. In diesem Runbook werden die einzelnen Prozessschritte in Form einer Checkliste aufgelistet. Es enthält für den Fall, dass es

ein Problem gibt, auch einen Abschnitt zur Fehlerbehandlung. Das Runbook wird wie die übrigen Runbooks im internen Wiki veröffentlicht. Das Cloud Operations-Team plant, das Runbook in der Zukunft zu automatisieren.

Implementierungsschritte

Wenn Sie noch kein Dokumenten-Repository besitzen, dann ist ein Repository für die Versionskontrolle hervorragend als Grundlage für Ihre Runbook-Bibliothek geeignet. Sie können Ihre Runbooks mithilfe von Markdown erstellen. Wir haben eine Runbook-Beispielvorlage bereitgestellt, die Sie für die Erstellung von Runbooks verwenden können.

```
# Runbook Title
## Runbook Info
| Runbook ID | Description | Tools Used | Special Permissions | Runbook Author | Last
 Updated | Escalation POC |
|-------|-------|-------|-------|-------|-------|-------|
| RUN001 | What is this runbook for? What is the desired outcome? | Tools | Permissions
 | Your Name | 2022-09-21 | Escalation Name |
## Steps
1. Step one
2. Step two
```

1. Wenn Sie noch kein Dokumentations-Repository oder -Wiki besitzen, sollten Sie in Ihrem Versionskontrollsystem ein neues Versionskontroll-Repository erstellen.
2. Identifizieren Sie einen Prozess, für den es kein Runbook gibt. Ein idealer Prozess hierfür ist ein Prozess, der halbregelmäßig ausgeführt wird, nur wenige Schritte enthält und bei Fehlern nur geringe Auswirkungen hat.
3. Erstellen Sie in Ihrem Dokument-Repository ein neues Markdown-Entwurfsdokument auf der Basis der Vorlage. Füllen Sie den Runbook-Titel und die Pflichtfelder unter Runbook-Informationen aus.
4. Füllen Sie ab dem ersten Schritt den Abschnitt Schritte im Runbook aus.
5. Geben Sie das Runbook einem Teammitglied. Lassen Sie das Teammitglied das Runbook ausführen, um die Schritte zu validieren. Aktualisieren Sie das Runbook, wenn etwas fehlt oder unklar ist.
6. Veröffentlichen Sie das Runbook in Ihrem internen Dokumentationsspeicher. Informieren Sie Ihr Team und die übrigen Stakeholder über das Runbook, nachdem es veröffentlicht wurde.
7. Mit der Zeit entsteht dadurch eine Bibliothek von Runbooks. Beginnen Sie mit der Automatisierung von Runbooks, wenn diese Bibliothek wächst.

Aufwand für den Implementierungsplan: niedrig. Eine schrittweise Anleitung in Textform ist der Mindeststandard für ein Runbook. Die Automatisierung von Runbooks kann den Implementierungsaufwand erhöhen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer
- OPS07-BP04 Verwenden von Playbooks zum Untersuchen von Problemen
- OPS10-BP01 Verwenden eines Prozesses für die Bewältigung von Ereignissen, Vorfällen und Problemen
- OPS10-BP02 Implementieren eines Prozesses für jede Warnmeldung
- OPS11-BP04 Wissensmanagement

Zugehörige Dokumente:

- AWS Well-Architected Framework: Konzepte: Runbook-Entwicklung
- Operative Kompetenz durch automatisierte Playbooks und Runbooks
- AWS Systems Manager: Arbeiten mit Runbooks
- Migrations-Playbook für große AWS-Migrationen – Aufgabe 4: Verbesserung Ihrer Migrations-Runbooks
- Verwendung von AWS Systems Manager-Automation-Runbooks zur Lösung operativer Aufgaben

Zugehörige Videos:

- AWS re:Invent 2019: DIY-Leitfaden für Runbooks, Vorfallberichte und Vorfallreaktion
- Automatisierung von IT-Abläufen in AWS | Amazon Web Services
- Integration von Skripts in AWS Systems Manager

Zugehörige Beispiele:

- Well-Architected Labs: Automatisieren von Vorgängen mit Playbooks und Runbooks
- AWS-Blogbeitrag: Aufbau einer Cloud-Automatisierungspraxis für Operational Excellence: Bewährte Methoden von AWS Managed Services

- AWS Systems Manager: Exemplarische Vorgehensweisen zur Automatisierung
- AWS Systems Manager: Runbook für die Wiederherstellung eines Root-Volumes anhand des letzten Snapshots
- Entwicklung eines Runbooks für Vorfallreaktionen in AWS mit Jupyter Notebooks und CloudTrail Lake
- Gitlab – Runbooks
- Rubix – eine Python-Bibliothek für die Erstellung von Runbooks in Jupyter Notebooks
- Verwendung von Document Builder für die Erstellung angepasster Runbooks

Zugehörige Services:

- AWS Systems Manager-Automatisierung

OPS07-BP04 Verwenden von Playbooks zum Untersuchen von Problemen

Playbooks sind schrittweise Anleitungen zur Untersuchung von Vorfällen. Wenn Vorfälle auftreten, werden Playbooks verwendet, um sie zu untersuchen, die Auswirkungen abzuschätzen und Ursachen zu identifizieren. Playbooks werden für verschiedene Szenarien eingesetzt, von fehlgeschlagenen Bereitstellungen bis hin zu Sicherheitsvorfällen. In vielen Fällen identifizieren Playbooks Ursachen, die dann mithilfe eines Runbooks beseitigt werden. Playbooks sind eine sehr wichtige Komponente der Vorfallreaktionspläne Ihrer Organisation.

Ein gutes Playbook weist einige zentrale Merkmale auf. Es leitet den Nutzer Schritt für Schritt durch den Erkennungsprozess. Welche Schritte sollten befolgt werden, um einen Vorfall zu diagnostizieren? Legen Sie im Playbook klar fest, ob bestimmte Tools oder erhöhte Berechtigungen benötigt werden. Ein wichtiger Teil ist ein Kommunikationsplan, um alle Stakeholder über den Status der Untersuchung zu informieren. Für den Fall, dass die eigentliche Ursache des Vorfalls nicht identifiziert werden kann, sollte das Playbook einen Eskalationsplan enthalten. Wenn die Ursache identifiziert wurde, sollte das Playbook auf ein Runbook verweisen, das beschreibt, wie die Ursache zu beheben ist. Playbooks sollten zentral gespeichert und regelmäßig gepflegt werden. Wenn Playbooks für bestimmte Warnungmeldungen verwendet werden, sollte Ihr Team in den Warnungmeldungen auf das Playbook verwiesen werden.

Im Zuge der Weiterentwicklung Ihrer Organisation sollten Sie Ihre Playbooks automatisieren. Beginnen Sie mit Playbooks für Vorfälle mit geringem Risikograd. Automatisieren Sie die

Erkennungsschritte mit Skripts. Stellen Sie sicher, dass Sie über begleitende Runbooks für die Behebung typischer Ursachen verfügen.

Gewünschtes Ergebnis: Ihre Organisation verfügt über Playbooks für typische Vorfälle. Die Playbooks werden an einem zentralen Ort gespeichert und sind für Ihre Teammitglieder verfügbar. Playbooks werden häufig aktualisiert. Für alle bekannten Ursachen werden begleitende Runbooks erstellt.

Typische Anti-Muster:

- Es gibt kein Standardverfahren für die Untersuchung von Vorfällen.
- Teammitglieder verlassen sich auf ihr Gedächtnis oder allgemein vorhandenes Wissen, um eine fehlgeschlagene Bereitstellung zu beheben.
- Neue Teammitglieder lernen die Untersuchung von Problemen durch Ausprobieren.
- Es werden keine bewährten Methoden für die Untersuchung von Problemen zwischen Teams ausgetauscht.

Vorteile der Nutzung dieser bewährten Methode:

- Playbooks verbessern Ihre Fähigkeit zum Umgang mit Vorfällen.
- Verschiedene Teammitglieder können dasselbe Playbook verwenden, um Ursachen in konsistenter Weise zu ermitteln.
- Für bekannte Ursachen können Runbooks entwickelt werden, um die Wiederherstellungszeit zu verkürzen.
- Mit Playbooks können Teammitglieder schneller Beiträge leisten.
- Mit wiederholbaren Playbooks können Teams ihre Prozesse skalieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Wie Sie Ihre Playbooks aufbauen und verwenden, hängt vom Reifegrad Ihrer Organisation ab. Wenn Sie noch neu in der Cloud sind, erstellen Sie Playbooks in Textform in einem zentralen Dokumenten-Repository. Wenn sich Ihre Organisation weiterentwickelt, können Playbooks mit Skriptsprachen wie Python teilweise automatisiert werden. Diese Skripts können zur Beschleunigung der Untersuchung in einem Jupyter Notebook ausgeführt werden. Fortgeschrittene Organisationen haben vollständig automatisierte Playbooks für häufig auftretende Probleme, die dann mit Runbooks automatisch behoben werden.

Beginnen Sie die Arbeit an Ihren Playbooks mit der Auflistung typischer Vorfälle bei Ihren Workloads. Wählen Sie Playbooks zunächst für Vorfälle mit geringem Risiko, bei denen die Ursache eingegrenzt werden kann. Wenn Sie über Playbooks für einfachere Szenarien verfügen, gehen Sie zu Szenarien mit höheren Risiken oder zu Szenarien über, bei denen die Ursache nicht vollständig klar ist.

Ihre textbasierten Runbooks sollten mit zunehmender Reife Ihrer Organisation automatisiert werden. Mithilfe von Services wie AWS Systems Manager-Automatisierungen kann einfacher Text in Automatisierungen umgewandelt werden. Diese Automatisierungen können dann für Ihren Workload ausgeführt werden, um die Untersuchungen zu beschleunigen. Sie können als Reaktion auf Ereignisse aktiviert werden, wodurch sich der durchschnittliche Zeitaufwand für die Untersuchung und Behebung von Vorfällen reduziert.

Kunden können AWS Systems Manager Incident Manager verwenden, um auf Vorfälle zu reagieren. Dieser Service bietet eine einzige Oberfläche für die Untersuchung von Vorfällen, die Information der Stakeholder über Untersuchung und Abhilfemaßnahmen und die Zusammenarbeit während des gesamten Vorgangs. Er verwendet AWS Systems Manager-Automatisierungen zur Beschleunigung von Untersuchung und Wiederherstellung.

Kundenbeispiel

Ein Produktionsvorfall hat Auswirkungen auf AnyCompany Retail. Der zuständige Techniker untersuchte das Problem mithilfe eines Playbooks. Im Zuge der einzelnen Schritte wurden anhand des aktuellen Playbooks die Beteiligten identifiziert. Der Techniker ermittelte einen Race-Zustand in einem Backend-Service als Ursache für den Vorfall. Mithilfe eines Runbooks startete er den Service neu und brachte AnyCompany Retail so wieder online.

Implementierungsschritte

Wenn Sie noch kein Dokumenten-Repository besitzen, dann sollten Sie ein Versionskontroll-Repository für Ihre Runbook-Bibliothek erstellen. Sie können Ihre Playbooks mit Markdown erstellen, das mit den meisten Playbook-Automatisierungssystemen kompatibel ist. Wenn Sie neu beginnen, verwenden Sie die folgende Beispielvorlage für ein Playbook.

```
# Playbook Title
## Playbook Info
| Playbook ID | Description | Tools Used | Special Permissions | Playbook Author | Last
 Updated | Escalation POC | Stakeholders | Communication Plan |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| RUN001 | What is this playbook for? What incident is it used for? | Tools |
 Permissions | Your Name | 2022-09-21 | Escalation Name | Stakeholder Name | How will
 updates be communicated during the investigation? |
```

```
## Steps
1. Step one
2. Step two
```

1. Wenn Sie noch kein Dokumenten-Repository oder -Wiki besitzen, sollten Sie in Ihrem Versionskontrollsystem ein neues Versionskontroll-Repository für Ihre Playbooks erstellen.
2. Identifizieren Sie ein typisches Problem, das eine Untersuchung erfordert. Dies sollte ein Szenario sein, bei dem die Ursache auf wenige Probleme eingegrenzt werden kann und das Risiko insgesamt niedrig ist.
3. Füllen Sie mithilfe der Markdown-Vorlage den Abschnitt Playbook-Name und die Felder unter Playbook-Informationen aus.
4. Geben Sie die Schritte zur Fehlerbehebung ein. Benennen Sie die zu treffenden Maßnahmen bzw. die zu untersuchenden Bereiche so klar wie möglich.
5. Geben Sie das Playbook einem Teammitglied zur Prüfung. Wenn darin etwas fehlt oder nicht klar ist, aktualisieren Sie das Playbook.
6. Veröffentlichen Sie Ihr Playbook in Ihrem Dokumenten-Repository und informieren Sie Ihr Team und alle Stakeholder darüber.
7. Diese Playbook-Bibliothek wächst mit der Zeit an. Sobald Sie mehrere Playbooks haben, beginnen Sie mithilfe von Tools wie AWS Systems Manager Automations mit ihrer Automatisierung.

Aufwand für den Implementierungsplan: niedrig. Ihre Playbooks sollten an einem zentralen Ort gespeicherte Textdokumente sein. Ausgereiftere Organisationen gehen zu automatisierten Playbooks über.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer
- OPS07-BP03 Verwenden von Runbooks zur Durchführung von Verfahren
- OPS10-BP01 Verwenden eines Prozesses für die Bewältigung von Ereignissen, Vorfällen und Problemen
- OPS10-BP02 Implementieren eines Prozesses für jede Warnmeldung
- OPS11-BP04 Wissensmanagement

Zugehörige Dokumente:

- AWS Well-Architected Framework: Konzepte: Playbook-Entwicklung
- Operative Kompetenz durch automatisierte Playbooks und Runbooks
- AWS Systems Manager: Arbeiten mit Runbooks
- Verwendung von AWS Systems Manager-Automation-Runbooks zur Lösung operativer Aufgaben

Zugehörige Videos:

- AWS re:Invent 2019: DIY-Leitfaden für Runbooks, Vorfallberichte und Vorfallreaktion (SEC318-R1)
- AWS Systems Manager Incident Manager – AWS Virtuelle Workshops
- Integration von Skripts in AWS Systems Manager

Zugehörige Beispiele:

- AWS Customer Playbook Framework
- AWS Systems Manager: Exemplarische Vorgehensweisen zur Automatisierung
- Entwicklung eines Runbooks für Vorfallreaktionen in AWS mit Jupyter Notebooks und CloudTrail Lake
- Rubix – Eine Python-Bibliothek für die Erstellung von Runbooks in Jupyter Notebooks
- Verwendung von Document Builder für die Erstellung angepasster Runbooks
- Well-Architected Labs: Automatisieren von Vorgängen mit Playbooks und Runbooks
- Well-Architected Labs: Playbook für Vorfallreaktion mit Jupyter

Zugehörige Services:

- AWS Systems Manager-Automatisierung
- AWS Systems Manager Incident Manager

OPS07-BP05 Treffen fundierter Entscheidungen für die Bereitstellung von Systemen und Änderungen

Nutzen Sie Prozesse für erfolgreiche und erfolglose Änderungen an Ihrem Workload. Eine Pre-mortem-Übung ist eine Übung, bei der ein Team einen Fehler simuliert, um Strategien zur Behebung

zu entwickeln. Beugen Sie wo möglich Fehlern vor und stellen Sie entsprechende Abläufe auf. Bewerten Sie den Nutzen und die Risiken der Bereitstellung von Änderungen an Ihrem Workload. Überprüfen Sie, ob alle Änderungen mit der Governance übereinstimmen.

Gewünschtes Ergebnis:

- Sie treffen bei der Bereitstellung von Änderungen an Ihrem Workload fundierte Entscheidungen.
- Änderungen entsprechen der Governance.

Typische Anti-Muster:

- Sie stellen eine Änderung an Ihrem Workload bereit, ohne einen Prozess für die Verarbeitung einer fehlgeschlagenen Bereitstellung zu haben.
- Sie nehmen Änderungen an Ihrer Produktionsumgebung vor, die nicht mit den Governance-Anforderungen vereinbar sind.
- Sie stellen eine neue Version Ihres Workloads bereit, ohne eine Baseline für die Ressourcenauslastung zu erstellen.

Vorteile der Nutzung dieser bewährten Methode:

- Sie sind auf fehlgeschlagene Änderungen an Ihrem Workload vorbereitet.
- Änderungen an Ihrem Workload sind konform mit den Governance-Richtlinien.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

Verwenden Sie Pre-Mortem-Übungen, um Prozesse für fehlgeschlagene Änderungen zu entwickeln. Dokumentieren Sie Ihre Prozesse für fehlgeschlagene Änderungen. Stellen Sie sicher, dass alle Änderungen mit der Governance übereinstimmen. Evaluieren Sie die Vorteile und Risiken der Bereitstellung von Änderungen an Ihrem Workload.

Kundenbeispiel

AnyCompany Retail führt regelmäßig Pre-Mortems durch, um die Prozesse für fehlgeschlagene Änderungen zu validieren. Die Prozesse werden in einem gemeinsamen Wiki dokumentiert und regelmäßig aktualisiert. Alle Änderungen entsprechen den Governance-Anforderungen.

Implementierungsschritte

1. Treffen Sie fundierte Entscheidungen, wenn Sie Änderungen an Ihrem Workload bereitstellen. Legen Sie Kriterien für eine erfolgreiche Bereitstellung fest und überprüfen Sie diese. Entwickeln Sie Szenarien oder Kriterien, die ein Rollback einer Änderung auslösen würden. Wägen Sie den Nutzen der Bereitstellung von Änderungen gegen die Risiken einer fehlgeschlagenen Änderung ab.
2. Überprüfen Sie, ob alle Änderungen mit den Governance-Richtlinien übereinstimmen.
3. Planen Sie anhand von Pre-Mortems fehlgeschlagene Änderungen und dokumentieren Sie Strategien zur Schadensbegrenzung. Führen Sie eine Table-Top-Übung durch, um eine fehlgeschlagene Änderung zu modellieren und Rollback-Verfahren zu validieren.

Grad des Aufwands für den Implementierungsplan: moderat. Die Einführung von Pre-Mortems erfordert die Koordination und den Einsatz aller Stakeholder in Ihrer gesamten Organisation

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP03 Bewerten der Governance-Anforderungen - Governance-Anforderungen sind ein Schlüssel bei der Entscheidung zur Bereitstellung einer Änderung.
- OPS06-BP01 Einkalkulieren nicht erfolgreicher Änderungen - Erstellen Sie Pläne zur Eindämmung einer fehlgeschlagenen Bereitstellung und verwenden Sie Pre-Mortems, um diese zu validieren.
- OPS06-BP02 Testbereitstellungen - Jede Softwareänderung sollte vor der Bereitstellung ordnungsgemäß getestet werden, um Fehler in der Produktion zu reduzieren.
- OPS07-BP01 Sicherstellen des Know-hows der Mitarbeiter - Ausreichend trainierte Mitarbeiter zur Unterstützung des Workloads sind unerlässlich, um eine fundierte Entscheidung über die Bereitstellung einer Systemänderung zu treffen.

Zugehörige Dokumente:

- Amazon Web Services: Risiko und Compliance
- AWS-Modell der geteilten Verantwortung
- Governance in the AWS Cloud: The Right Balance Between Agility and Safety (Governance in der AWS Cloud: Das richtige Gleichgewicht zwischen Agilität und Sicherheit)

OPS07-BP06 Aktivieren von Supportplänen für Produktions-Workloads

Aktivieren Sie Support für sämtliche Software und Services, auf denen Ihr Produktions-Workload basiert. Wählen Sie ein geeignetes Support-Level für Ihre Servicelevel-Anforderungen in der Produktion. Supportpläne für diese Abhängigkeiten sind wichtig für den Fall von Serviceunterbrechungen oder Softwareproblemen. Dokumentieren Sie Supportpläne sowie die Verfahren zur Anfrage nach Support bei allen Service- und Software-Anbietern. Implementieren Sie Mechanismen zur Prüfung, ob Support-Kontaktpunkte stets aktuell sind.

Gewünschtes Ergebnis:

- Implementieren Sie Supportpläne für Software und Services, auf denen Ihre Workloads basieren.
- Wählen Sie einen geeigneten Supportplan auf der Grundlage Ihrer Service-Level-Anforderungen.
- Dokumentieren Sie die Supportpläne, die Supportlevels und die Vorgehensweise bei Supportanfragen.

Typische Anti-Muster:

- Sie haben keinen Supportplan für einen kritischen Softwareanbieter. Dies beeinflusst Ihren Workload, und Sie haben keine Möglichkeit, schnell einen Fix oder rechtzeitige Updates von dem Anbieter zu erhalten.
- Ein Entwickler, der der primäre Ansprechpartner bei einem Softwareanbieter war, hat das Unternehmen verlassen. Sie können den Support des Anbieters nicht direkt erreichen. Sie müssen Zeit aufwenden, um sich durch generische Kontaktsysteme zu arbeiten, was die Reaktionszeiten verlängert.
- Bei einem Softwareanbieter ereignet sich ein Produktionsausfall. Es gibt keine Dokumentation dazu, wie ein Supportfall einzureichen ist.

Vorteile der Nutzung dieser bewährten Methode:

- Mit dem richtigen Supportlevel können Sie schnell eine Reaktion erhalten, die dem Service-Level entspricht.
- Als Kunde mit Support stehen Ihnen bei Produktionsproblemen Eskalationsmöglichkeiten zur Verfügung.
- Software- und Serviceanbieter können Ihnen bei Vorfällen Unterstützung bei der Fehlerbehebung bieten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

Aktivieren Sie Support für sämtliche Software- und Service-Anbieter, von denen Ihr Produktions-Workload abhängt. Richten Sie geeignete Supportpläne ein, um Service-Level einhalten zu können. Für AWS-Kunden bedeutet dies die Aktivierung von AWS Business Support oder einer höheren Stufe für alle Konten mit Produktions-Workloads. Treffen Sie sich regelmäßig mit Supportanbietern, um Neues zu Supportangeboten, -prozessen und -ansprechpartnern zu erfahren. Dokumentieren Sie das Supportverfahren bei Software- und Serviceanbietern, einschließlich der Eskalationsmöglichkeiten bei Ausfällen. Implementieren Sie Mechanismen, um die Supportkontakte stets auf aktuellem Stand zu halten.

Kundenbeispiel

Bei AnyCompany Retail gibt es für alle kommerziellen Software- und Service-Abhängigkeiten Supportpläne. Beispielsweise hat das Unternehmen AWS Enterprise Support für alle Konten mit Produktions-Workloads. Jeder Entwickler kann bei einem Problem einen Supportfall auslösen. Es gibt eine Wiki-Seite mit Informationen zum Verfahren bei Supportanfragen, zu den Ansprechpartnern und zu bewährten Methoden dafür.

Implementierungsschritte

1. Arbeiten Sie mit den Beteiligten in Ihrer Organisation, um Software- und Serviceanbieter zu identifizieren, von denen Ihr Workload abhängt. Dokumentieren Sie diese Abhängigkeiten.
2. Legen Sie die Service-Level-Anforderungen für Ihren Workload fest. Wählen Sie einen Supportplan, der dazu passt.
3. Richten Sie für kommerzielle Software und Services einen Supportplan bei den Anbietern ein.
    a. Ein Abonnement von AWS Business Support oder höher für alle Produktionskonten bietet schnellere Reaktionszeiten von AWS Support und wird dringend empfohlen. Wenn Sie keinen Premium-Support haben, benötigen Sie einen Aktionsplan für den Umgang mit Problemen, bei denen Hilfe von AWS Support erforderlich ist. AWS Support stellt Ihnen verschiedenste Tools und Technologien, Fachpersonal und Programme zur Verfügung, die Sie proaktiv bei der Performance-Optimierung, Kostensenkung und schnelleren Entwicklung neuer Innovationen unterstützen. AWS Business Support bietet zusätzliche Vorteile, darunter den Zugriff auf AWS Trusted Advisor und das AWS Personal Health Dashboard sowie kürzere Reaktionszeiten.
4. Dokumentieren Sie den Supportplan in Ihrem Wissensmanagement-Tool. Berücksichtigen Sie dabei, wie eine Supportanfrage durchgeführt wird, wer in einem solchen Fall zu benachrichtigen

ist und wie Vorfälle eskaliert werden können. Ein Wiki ist ein gutes Hilfsmittel, das allen Beteiligten ermöglicht, erforderliche Aktualisierungen der Dokumentation vorzunehmen, wenn ihnen Änderungen bei Supportprozessen oder Ansprechpartnern bekannt werden.

Grad des Aufwands für den Implementierungsplan: niedrig. Die meisten Software- und Serviceanbieter bieten Opt-in-Supportpläne an. Durch die Dokumentation und die Weitergabe bewährter Supportmethoden in Ihrem Wissensmanagementsystem können Sie sicherstellen, dass Ihr Team weiß, was bei einem Produktionsproblem zu tun ist.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP02 Prozesse und Verfahren haben feste Besitzer

Zugehörige Dokumente:

- AWS Support Plans (AWS Support-Pläne)

Zugehörige Services:

- AWS Business Support
- AWS Enterprise Support

Betrieb

Erfolg bedeutet, dass die gewünschten Ergebnisse erreicht werden. Gemessen wird der Erfolg über Metriken, die Sie definieren. Durch das Verständnis des Zustands Ihres Workloads und Ihrer Betriebsabläufe können Sie feststellen, wann organisatorische und betriebliche Ergebnisse gefährdet werden oder gefährdet sind und entsprechend reagieren.

Um erfolgreich zu sein, müssen Sie folgende Voraussetzungen erfüllen:

Themen

Nutzung der Workload-Beobachtbarkeit

Sorgen Sie für einen optimalen Zustand des Workloads, indem Sie Beobachtbarkeit nutzen. Nutzen Sie relevante Metriken, Protokolle und Traces, um sich einen umfassenden Überblick über die Leistung Ihres Workloads zu verschaffen und Probleme effizient zu beheben.

Beobachtbarkeit ermöglicht es Ihnen, sich auf aussagekräftige Daten zu konzentrieren und die Interaktionen und Ergebnisse Ihrer Workloads zu verstehen. Indem Sie sich auf wichtige Erkenntnisse konzentrieren und unnötige Daten eliminieren, behalten Sie einen einfachen Ansatz zum Verständnis der Workload-Leistung bei.

Es ist wichtig, Daten nicht nur zu erfassen, sondern sie auch richtig zu interpretieren. Definieren Sie klare Ausgangswerte, legen Sie geeignete Alarmschwellenwerte fest und überwachen Sie aktiv, ob Abweichungen vorliegen. Wenn eine wichtige Metrik abweicht, insbesondere wenn sie mit anderen Daten korreliert, kann dies spezifische Problembereiche aufzeigen.

Mit Beobachtbarkeit sind Sie besser in der Lage, potenzielle Herausforderungen vorherzusehen und zu bewältigen sowie sicherzustellen, dass Ihr Workload reibungslos funktioniert und den Geschäftsanforderungen entspricht.

AWS bietet spezielle Tools wie Amazon CloudWatch zur Überwachung und Protokollierung und AWS X-Ray zur verteilten Nachverfolgung. Diese Services lassen sich mühelos in verschiedene AWS-Ressourcen integrieren und ermöglichen eine effiziente Datenerfassung, die Einrichtung von

Warnmeldungen auf der Grundlage vordefinierter Schwellenwerte und die Darstellung von Daten auf Dashboards zur einfachen Interpretation. Mithilfe dieser Erkenntnisse können Sie fundierte, datengestützte Entscheidungen treffen, die Ihren betrieblichen Zielen entsprechen.

Bewährte Methoden

- OPS08-BP01 Analysieren von Workload-Metriken
- OPS08-BP02 Analysieren von Workload-Protokollen
- OPS08-BP03 Analysieren von Workload-Traces
- OPS08-BP04 Erstellen umsetzbarer Warnmeldungen
- OPS08-BP05 Erstellen von Dashboards

OPS08-BP01 Analysieren von Workload-Metriken

Analysieren Sie nach der Implementierung der Anwendungstelemetrie regelmäßig die gesammelten Metriken. Latenz, Anfragen, Fehler und Kapazität (oder Kontingente) liefern zwar Erkenntnisse zur Systemleistung, es ist jedoch wichtig, die Überprüfung der Metriken zu Geschäftsergebnissen zu priorisieren. Dadurch wird sichergestellt, dass Sie datengestützte Entscheidungen treffen, die auf Ihre Geschäftsziele abgestimmt sind.

Gewünschtes Ergebnis: Präzise Erkenntnisse zur Workload-Leistung, die als Grundlage für datengestützte Entscheidungen dienen und die Abstimmung mit den Geschäftszielen sicherstellen.

Typische Anti-Muster:

- Isolierte Analyse von Metriken, ohne deren Auswirkungen auf die Geschäftsergebnisse zu berücksichtigen.
- Übermäßiges Vertrauen in technische Metriken, während Geschäftsmetriken ignoriert werden.
- Seltene Überprüfung von Metriken, Entscheidungsmöglichkeiten in Echtzeit werden verpasst.

Vorteile der Nutzung dieser bewährten Methode:

- Verbessertes Verständnis des Zusammenhangs zwischen technischer Leistung und Geschäftsergebnissen.
- Verbesserter Entscheidungsprozess auf der Grundlage von Echtzeitdaten.
- Proaktive Identifizierung und Minderung von Problemen, bevor sie sich auf die Geschäftsergebnisse auswirken.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Nutzen Sie Tools wie Amazon CloudWatch zur Durchführung metrischer Analysen. Sie können AWS-Services wie AWS Cost Anomaly Detection und Amazon DevOps Guru zur Erkennung von Anomalien verwenden, insbesondere wenn statische Schwellenwerte unbekannt sind oder wenn Verhaltensmuster besser für die Erkennung von Anomalien geeignet sind.

Implementierungsschritte

1. Analysieren und überprüfen Sie Metriken: Überprüfen Sie regelmäßig Ihre Workload-Metriken und werten Sie sie aus.
   a. Priorisieren Sie Metriken zu Geschäftsergebnissen gegenüber rein technischen.
   b. Machen Sie sich mit der Bedeutung von Spitzen, Rückgängen oder Mustern in Ihren Daten vertraut.
2. Nutzen Sie Amazon CloudWatch: Verwenden Sie Amazon CloudWatch für eine zentrale Ansicht und detaillierte Analysen.
   a. Konfigurieren Sie CloudWatch-Dashboards, um Ihre Metriken zu visualisieren und sie im Zeitverlauf zu vergleichen.
   b. Nutzen Sie Perzentile in CloudWatch, um einen klaren Überblick über die metrische Verteilung zu erhalten, der Ihnen helfen kann, SLAs zu verstehen und einzelne Ausreißer nachzuvollziehen.
   c. Richten Sie AWS Cost Anomaly Detection ein, um ungewöhnliche Muster zu identifizieren, ohne sich auf statische Schwellenwerte zu verlassen.
   d. Implementieren Sie die kontenübergreifende Beobachtbarkeit mit CloudWatch, um Anwendungen zu überwachen und Fehler zu beheben, die mehrere Konten innerhalb einer Region betreffen.
   e. Nutzen Sie CloudWatch Metric Insights, um metrische Daten über Konten und Regionen hinweg abzufragen und zu analysieren und Trends und Anomalien zu identifizieren.
   f. Wenden Sie CloudWatch Metric Math an, um Ihre Metriken zu transformieren, zu aggregieren oder Berechnungen für den Erhalt tieferer Einblicke durchzuführen.
3. Machen Sie Gebrauch von Amazon DevOps Guru: Integrieren Sie Amazon DevOps Guru wegen seiner Machine Learning-gestützten Anomalieerkennung, mit der Sie frühzeitig Anzeichen von Betriebsproblemen Ihrer Serverless-Anwendungen erkennen und diese beheben können, bevor sie sich auf Ihre Kunden auswirken.

4. Optimieren Sie auf der Grundlage von Erkenntnissen: Treffen Sie fundierte Entscheidungen auf der Grundlage Ihrer Metrikanalyse, um Ihre Workloads anzupassen und zu verbessern.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS04-BP02 Implementieren einer Anwendungstelemetrie

Zugehörige Dokumente:

- The Wheel Blog - Emphasizing the importance of continually reviewing metrics (Die Bedeutung der kontinuierlichen Überprüfung von Metriken)
- Percentile are important (Perzentile sind wichtig)
- Using AWS Cost Anomaly Detection (Verwendung von AWS Cost Anomaly Detection)
- CloudWatch cross-account observability (kontenübergreifende Beobachtbarkeit mit CloudWatch)
- Query your metrics with CloudWatch Metrics Insights (Metrikabfrage mit CloudWatch Metrics Insights)

Zugehörige Videos:

- Enable Cross-Account Observability in Amazon CloudWatch (Kontenübergreifende Beobachtbarkeit in Amazon CloudWatch aktivieren)
- Introduction to Amazon DevOps Guru (Einführung in Amazon DevOps Guru)
- Continuously Analyze Metrics using AWS Cost Anomaly Detection (Fortlaufende Metrikanalyse mit AWS Cost Anomaly Detection)

Zugehörige Beispiele:

- Workshop zur Beobachtbarkeit
- Gaining operation insights with AIOps using Amazon DevOps Guru (Operative Erkenntnisse gewinnen mit AIOps und Amazon DevOps Guru)

OPS08-BP02 Analysieren von Workload-Protokollen

Die regelmäßige Analyse von Workload-Protokollen ist unerlässlich, um ein tieferes Verständnis der operativen Aspekte Ihrer Anwendung zu erlangen. Durch effizientes Durchsuchen, Visualisieren und Interpretieren von Protokolldaten können Sie die Leistung und Sicherheit von Anwendungen kontinuierlich optimieren.

Gewünschtes Ergebnis: Umfassende Erkenntnisse zum Anwendungsverhalten und zu Operationen, die aus einer gründlichen Protokollanalyse gewonnen wurden und für eine proaktive Problemerkennung und -behebung sorgen.

Typische Anti-Muster:

- Die Analyse von Protokollen vernachlässigen, bis ein kritisches Problem auftritt.
- Die Suite verfügbarer Tools für die Protokollanalyse nicht nutzen und wichtige Erkenntnisse verpassen.
- Alleiniges Vertrauen auf die manuelle Überprüfung von Protokollen, ohne Automatisierungs- und Abfragefunktionen zu nutzen.

Vorteile der Nutzung dieser bewährten Methode:

- Proaktive Identifizierung von operativen Engpässen, Sicherheitsbedrohungen und anderen potenziellen Problemen.
- Effiziente Nutzung von Protokolldaten für die kontinuierliche Anwendungsoptimierung.
- Verbessertes Verständnis des Anwendungsverhaltens, Unterstützung beim Debuggen und bei der Problembehandlung.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Amazon CloudWatch Logs ist ein leistungsstarkes Tool für die Protokollanalyse. Integrierte Features wie CloudWatch Logs Insights und Contributor Insights sorgen für eine intuitive und effiziente Ableitung aussagekräftiger Informationen aus Protokollen.

Implementierungsschritte

1. Einrichtung von CloudWatch Logs: Konfigurieren Sie Anwendungen und Services so, dass Protokolle an CloudWatch Logs gesendet werden.
2. Verwendung der Erkennung von Protokollanomalien: Verwenden Sie die Amazon CloudWatch Logs-Anomalieerkennung, um ungewöhnliche Protokollmuster automatisch zu identifizieren und Warnmeldungen zu erhalten. Mit diesem Tool können Sie Anomalien in Ihren Protokollen proaktiv verwalten und potenzielle Probleme frühzeitig erkennen.
3. Einrichten von CloudWatch Logs-Insights: Verwenden Sie CloudWatch Logs-Insights, um Ihre Protokolldaten interaktiv zu durchsuchen und zu analysieren.
    a. Erstellen Sie Abfragen, um Muster zu extrahieren, Protokolldaten zu visualisieren und umsetzbare Erkenntnisse abzuleiten.
    b. Verwenden Sie die Musteranalyse für CloudWatch Logs-Erkenntnisse, um häufige Protokollmuster zu analysieren und zu visualisieren. Dieses Feature hilft Ihnen, allgemeine Betriebstrends und potenzielle Ausreißer in Ihren Protokolldaten nachzuvollziehen.
    c. Verwenden Sie CloudWatch Logs compare (diff), um eine Differenzanalyse zwischen verschiedenen Zeiträumen oder Protokollgruppen vorzunehmen. Verwenden Sie diese Funktion, um Änderungen zu lokalisieren und deren Auswirkungen auf die Leistung oder das Verhalten Ihres Systems zu bewerten.
4. Überwachen Sie Protokolle in Echtzeit mit Live Tail: Verwenden Sie Amazon CloudWatch Logs Live Tail, um Protokolldaten in Echtzeit anzuzeigen. Sie können die Betriebsaktivitäten Ihrer Anwendung in Echtzeit aktiv überwachen, um sich einen unmittelbaren Einblick in die Systemleistung und potenzielle Probleme zu verschaffen.
5. Nutzung von Contributor Insights: Verwenden Sie CloudWatch Contributor Insights, um Top-Talker in Dimensionen mit hoher Kardinalität wie IP-Adressen oder Benutzeragenten zu identifizieren.
6. Implementieren von CloudWatch Logs-Metrikfiltern: Konfigurieren Sie CloudWatch Logs-Metrikfilter, um Protokolldaten in umsetzbare Metriken umzuwandeln. Auf diese Weise können Sie Alarme einstellen oder Muster näher analysieren.
7. Implementieren von kontoübergreifender CloudWatch-Beobachtbarkeit: Überwachen Sie Anwendungen, die sich über mehrere Konten innerhalb einer Region erstrecken, und beheben Sie Fehler.
8. Regelmäßige Überprüfung und Verfeinerung: Überprüfen Sie regelmäßig Ihre Protokollanalysestrategien, um alle relevanten Informationen zu erfassen und die Anwendungsleistung kontinuierlich zu optimieren.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS04-BP02 Implementieren einer Anwendungstelemetrie
- OPS08-BP01 Analysieren von Workload-Metriken

Zugehörige Dokumente:

- Analysieren von Protokolldaten mit CloudWatch Logs Insights
- Nutzung von CloudWatch Contributor Insights
- Erstellen und Verwalten von CloudWatch Logs-Metrikfiltern

Zugehörige Videos:

- Analysieren von Protokolldaten mit CloudWatch Logs Insights
- Mit CloudWatch Contributor Insights Daten mit hoher Kardinalität analysieren

Zugehörige Beispiele:

- CloudWatch Logs-Beispielabfragen
- Workshop zur Beobachtbarkeit

OPS08-BP03 Analysieren von Workload-Traces

Die Analyse von Trace-Daten ist entscheidend, wenn es darum geht, einen umfassenden Überblick über den Betriebsverlauf einer Anwendung zu erhalten. Durch die Visualisierung und das Verständnis der Interaktionen zwischen verschiedenen Komponenten können die Leistung optimiert, Engpässe identifiziert und das Benutzererlebnis verbessert werden.

Gewünschtes Ergebnis: Sie verschaffen sich einen klaren Überblick über die verteilten Abläufe Ihrer Anwendung und erzielen dadurch eine schnellere Problemlösung und ein verbessertes Benutzererlebnis.

Typische Anti-Muster:

- Trace-Daten werden übersehen und man verlässt sich ausschließlich auf Protokolle und Metriken.
- Trace-Daten werden nicht mit zugehörigen Protokollen in Zusammenhang gebracht.
- Aus Traces abgeleitete Metriken wie Latenz und Fehlerraten werden ignoriert.

Vorteile der Nutzung dieser bewährten Methode:

- Sie verbessern die Fehlersuche und reduzieren die durchschnittliche Zeit für die Behebung (Mean Time to Resolution, MTTR).
- Sie gewinnen Erkenntnisse über Abhängigkeiten und deren Auswirkungen.
- Sie können Leistungsprobleme rasch identifizieren und beheben.
- Sie nutzen von aus Trace abgeleitete Metriken für fundierte Entscheidungen.
- Sie erzielen ein besseres Benutzererlebnis durch optimierte Komponenteninteraktionen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

AWS X-Ray bietet eine umfassende Suite für die Analyse von Trace-Daten, die einen ganzheitlichen Überblick über Serviceinteraktionen, die Überwachung von Benutzeraktivitäten und die Erkennung von Leistungsproblemen bietet. Features wie ServiceLens, X-Ray Insights, X-Ray Analytics und Amazon DevOps Guru erhöhen die Tiefe verwertbarer Erkenntnisse, die aus Trace-Daten gewonnen werden.

Implementierungsschritte

Die folgenden Schritte bieten einen strukturierten Ansatz zur effektiven Implementierung der Trace-Datenanalyse mithilfe von AWS-Services:

1. Integrate AWS X-Ray: Stellen Sie sicher, dass in Ihre Anwendungen X-Ray integriert ist, um Trace-Daten zu erfassen.
2. Analysieren Sie X-Ray Metriken: Untersuchen Sie anhand von X-Ray Traces abgeleitete Metriken wie Latenz, Anforderungsraten, Fehlerraten und Reaktionszeitverteilungen, und verwenden Sie die Service Map, um den Zustand der Anwendung zu überwachen.

3. Verwendung von ServiceLens: Nutzen Sie die ServiceLens-Map für eine verbesserte Beobachtbarkeit Ihrer Services und Anwendungen. Dies ermöglicht eine integrierte Anzeige von Traces, Metriken, Protokollen, Alarmen und anderen Statusinformationen.
4. Aktivieren Sie X-Ray Insights:
   a. Aktivieren Sie X-Ray Insights für die automatische Erkennung von Anomalien in Traces.
   b. Untersuchen Sie Erkenntnisse, um Muster zu identifizieren und die Ursachen zu ermitteln, z. B. erhöhte Fehlerraten oder Latenzen.
   c. Eine chronologische Analyse der erkannten Probleme finden Sie in der Insights-Timeline.
5. Verwendung von X-Ray Analytics: X-Ray Analytics ermöglicht es Ihnen, Daten gründlich zu untersuchen, Muster zu lokalisieren und Erkenntnisse zu gewinnen.
6. Verwendung von Gruppen in X-Ray: Erstellen Sie Gruppen in X-Ray, um Traces nach Kriterien wie hoher Latenz zu filtern und so eine gezieltere Analyse zu ermöglichen.
7. Integration von Amazon DevOps Guru: Setzen Sie Amazon DevOps Guru ein, um von Machine-Learning-Modellen zu profitieren, die betriebliche Anomalien in Traces lokalisieren.
8. Verwendung von CloudWatch Synthetics: Verwenden Sie CloudWatch Synthetics, um Canaries für die kontinuierliche Überwachung Ihrer Endpunkte und Workflows zu erstellen. Sie können diese Canaries in X-Ray integrieren, um Trace-Daten für eine eingehende Analyse der getesteten Anwendungen bereitzustellen.
9. Verwendung von Real User Monitoring (RUM): Mit AWS X-Ray und CloudWatch RUM können Sie den Anforderungspfad analysieren und debuggen, angefangen bei den Endbenutzern Ihrer Anwendung bis hin zu nachgelagerten AWS-verwalteten Services. Auf diese Weise können Sie Latenztrends und Fehler identifizieren, die sich auf Ihre Endbenutzer auswirken.
10. Korrelieren mit Protokollen: Korrelieren Sie Trace-Daten mit zugehörigen Protokollen in der X-Ray-Trace-Ansicht, um sich einen detaillierten Überblick über das Anwendungsverhalten zu verschaffen. Auf diese Weise können Sie Protokollereignisse anzeigen, die direkt mit verfolgten Transaktionen verknüpft sind.
11. Implementieren von kontoübergreifender CloudWatch-Beobachtbarkeit: Überwachen Sie Anwendungen, die sich über mehrere Konten innerhalb einer Region erstrecken, und beheben Sie Fehler.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS08-BP01 Analysieren von Workload-Metriken
- OPS08-BP02 Analysieren von Workload-Protokollen

Zugehörige Dokumente:

- Verwenden von ServiceLens zur Überwachung des Zustands Ihrer Anwendungen
- Erkunden von Trace-Daten mit X-Ray Analytics
- Mit X-Ray Insights Anomalien in Traces erkennen
- Fortlaufende Überwachung mit CloudWatch Synthetics

Zugehörige Videos:

- Analysieren und Debuggen von Anwendungen mithilfe von Amazon CloudWatch Synthetics und AWS X-Ray
- Nutzung von AWS X-Ray Insights

Zugehörige Beispiele:

- Workshop zur Beobachtbarkeit
- Implementieren von X-Ray mit AWS Lambda
- Vorlagen für CloudWatch Synthetics Canary

OPS08-BP04 Erstellen umsetzbarer Warnmeldungen

Es ist entscheidend, Abweichungen im Verhalten Ihrer Anwendung umgehend zu erkennen und darauf zu reagieren. Besonders wichtig ist es, zu erkennen, wann die auf den wichtigsten Leistungsindikatoren (KPIs) basierenden Ergebnisse gefährdet sind oder unerwartete Anomalien auftreten. Wenn Sie Warnmeldungen auf KPIs basieren, stellen Sie dadurch sicher, dass die Signale, die Sie erhalten, direkt mit geschäftlichen oder betrieblichen Auswirkungen verknüpft sind. Der Ansatz mit umsetzbaren Warnmeldungen fördert proaktive Reaktionen und trägt zur Aufrechterhaltung der Systemleistung und Zuverlässigkeit bei.

Gewünschtes Ergebnis: Sie erhalten rechtzeitig relevante und umsetzbare Warnmeldungen, um potenzielle Probleme schnell zu erkennen und zu beheben, insbesondere wenn die KPI-Ergebnisse gefährdet sind.

Typische Anti-Muster:

- Es werden zu viele unkritische Warnmeldungen eingerichtet, was zu einer Übermüdung durch Warnmeldungen führt.
- Warnmeldungen werden nicht anhand von KPIs priorisiert, was es schwierig macht, die geschäftlichen Auswirkungen von Problemen zu verstehen.
- Die eigentlichen Ursachen werden vernachlässigt, was zu wiederholten Warnmeldungen für dasselbe Problem führt.

Vorteile der Nutzung dieser bewährten Methode:

- Geringere Ermüdung durch Warnmeldungen durch Fokussierung auf umsetzbare und relevante Warnmeldungen.
- Verbesserte Systemverfügbarkeit und -zuverlässigkeit durch proaktive Problemerkennung und -behebung.
- Verbesserte Teamzusammenarbeit und schnellere Problemlösung durch die Integration in übliche Warnmeldungs- und Kommunikationstools.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Um einen effektiven Warnmechanismus zu schaffen, ist es wichtig, Metriken, Protokolle und Trace-Daten zu verwenden, die darauf hinweisen, wenn auf KPIs basierende Ergebnisse gefährdet sind oder Anomalien erkannt werden.

Implementierungsschritte

1. Ermitteln von Key Performance Indicators (KPIs): Identifizieren Sie die KPIs Ihrer Anwendung. Warnmeldungen sollten mit diesen KPIs verknüpft werden, damit sie die Auswirkungen auf das Unternehmen genau widerspiegeln.
2. Implementierung der Erkennung von Anomalien:
    - Verwendung der Amazon CloudWatch-Anomalieerkennung: Richten Sie die Amazon CloudWatch-Anomalieerkennung ein, um ungewöhnliche Muster automatisch zu erkennen, damit Warnmeldungen nur für echte Anomalien generieren werden.
    - Nutzung von AWS X-Ray Insights:

   a. Richten Sie X-Ray Insights ein, um Anomalien in Trace-Daten zu erkennen.
   b. Konfigurieren Sie Benachrichtigungen für X-Ray Insights, um bei erkannten Problemen Warnmeldungen zu erhalten.

- Integration mit Amazon DevOps Guru:
   a. Nutzung von Amazon DevOps Guru für die Machine-Learning-Fähigkeiten bei der Erkennung betrieblicher Anomalien anhand vorhandener Daten.
   b. Navigieren Sie zu den Benachrichtigungseinstellungen unter DevOps Guru, um Anomaliewarnmeldungen einzurichten.

3. Implementieren umsetzbarer Warnmeldungen: Entwerfen Sie Warnmeldungen, die angemessene Informationen für sofortige Maßnahmen enthalten.
   1. Überwachen Sie AWS Health-Ereignisse mithilfe von Amazon EventBridge-Regeln oder integrieren Sie sie programmgesteuert in die AWS Health API, um Aktionen zu automatisieren, wenn Sie AWS Health-Ereignisse erhalten. Dies können allgemeine Aktionen sein, z. B. das Senden aller geplanten Lebenszyklus-Ereignisnachrichten an eine Chat-Oberfläche, oder spezifische Aktionen, wie das Initiieren eines Workflows in einem IT-Servicemanagement-Tool.
4. Reduzieren der Warnmeldungsmüdigkeit: Minimieren Sie unkritische Warnmeldungen. Wenn Teams mit zahllosen unbedeutenden Warnmeldungen überfordert werden, können sie den Überblick über kritische Probleme verlieren, was die Gesamteffektivität des Warnmechanismus beeinträchtigt.
5. Einrichten von zusammengesetzten Alarmen: Verwenden Sie zusammengesetzte Amazon CloudWatch-Alarme, um mehrere Alarme zu kombinieren.
6. Integrieren von Warnmeldungs-Tools: Integrieren Sie Tools wie Ops Genie und PagerDuty.
7. Nutzung von AWS Chatbot: Integrieren Sie AWS Chatbot, um Warnmeldungen an Amazon Chime, Microsoft Teams und Slack weiterzuleiten.
8. Warnmeldung basierend auf Protokollen: Verwenden Sie Protokoll-Metrikfilter in CloudWatch, um Alarme basierend auf bestimmten Protokollereignissen zu erstellen.
9. Überprüfen und iterieren: Überprüfen und Sie die Warnkonfigurationen regelmäßig und passen Sie sie an.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS04-BP02 Implementieren einer Anwendungstelemetrie
- OPS04-BP03 Implementieren von Telemetrie für Benutzererfahrung
- OPS04-BP04 Implementieren einer Abhängigkeitstelemetrie
- OPS04-BP05 Implementieren der verteilten Nachverfolgung
- OPS08-BP01 Analysieren von Workload-Metriken
- OPS08-BP02 Analysieren von Workload-Protokollen
- OPS08-BP03 Analysieren von Workload-Traces

Zugehörige Dokumente:

- Verwendung von Amazon CloudWatch-Alarmen
- Erstellung eines zusammengesetzten Alarms
- Erstellung eines CloudWatch-Alarms auf der Grundlage der Anomalieerkennung
- DevOps Guru-Benachrichtigungen
- X-Ray Insights – Benachrichtigungen
- Überwachung, Betrieb und Fehlerbehebung Ihrer AWS-Ressourcen mit interaktiven ChatOps
- Amazon CloudWatch-Integrationsleitfaden | PagerDuty
- Integration von OpsGenie mit Amazon CloudWatch

Zugehörige Videos:

- Erstellung zusammengesetzter Alarme in Amazon CloudWatch
- AWS Chatbot Übersicht
- AWS On Air ft. Veränderliche Befehle in AWS Chatbot

Zugehörige Beispiele:

- Alarme, Vorfallmanagement und Problembehebung in der Cloud mit Amazon CloudWatch
- Tutorial: Erstellen einer Amazon EventBridge-Regel, die Benachrichtigungen an AWS Chatbot sendet
- Workshop zur Beobachtbarkeit

OPS08-BP05 Erstellen von Dashboards

Dashboards sind die anwenderorientierte Sicht auf die Telemetriedaten Ihrer Workloads. Sie stellen zwar eine wichtige visuelle Schnittstelle dar, sollten aber nicht als Ersatz, sondern als Ergänzung für Warnmechanismen dienen. Wenn sie sorgfältig zusammengestellt werden, liefern sie nicht nur schnelle Erkenntnisse zum Status und zur Leistung des Systems, sondern bieten Stakeholdern auch Echtzeitinformationen über Geschäftsergebnisse und die Auswirkungen von Problemen.

Gewünschtes Ergebnis:

Klare, umsetzbare Erkenntnisse zur System- und Geschäftsstabilität mithilfe visueller Darstellungen.

Typische Anti-Muster:

- Überkomplizierte Dashboards mit zu vielen Metriken.
- Sich auf Dashboards verlassen, ohne Warnmeldungen zur Erkennung von Anomalien zu nutzen.
- Fehlende Aktualisierung der Dashboards im Laufe des Workload-Fortschritts.

Vorteile dieser bewährten Methode:

- Sofortiger Einblick in wichtige Systemmetriken und KPIs.
- Verbesserte Kommunikation und mehr Verständnis unter den Interessengruppen.
- Rasche Erkenntnisse zu den Auswirkungen operativer Probleme.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Geschäftsorientierte Dashboards

Dashboards, die auf Geschäfts-KPIs zugeschnitten sind, sprechen ein breiteres Spektrum von Stakeholdern an. Auch wenn diese Personen vielleicht nicht an Systemmetriken interessiert sind, haben sie dennoch großes Interesse daran, die geschäftlichen Auswirkungen dieser Zahlen zu verstehen. Ein geschäftsorientiertes Dashboard stellt sicher, dass alle technischen und betrieblichen Metriken, die überwacht und analysiert werden, auf die übergeordneten Geschäftsziele ausgerichtet sind. Diese Ausrichtung sorgt für Klarheit und stellt sicher, dass alle gleich darüber informiert sind, was wichtig ist und was nicht. Darüber hinaus sind Dashboards, die Geschäfts-KPIs hervorheben, in der Regel leichter umzusetzen. Sie bieten Stakeholdern die Möglichkeit, in kürzester Zeit den Status

der Abläufe, die Bereiche, die Aufmerksamkeit erfordern, und die potenziellen Auswirkungen auf die Geschäftsergebnisse zu verstehen.

Vor diesem Hintergrund sollten Sie bei der Erstellung Ihrer Dashboards sicherstellen, dass ein Gleichgewicht zwischen technischen Metriken und Geschäfts-KPIs besteht. Beide sind wichtig, richten sich aber an unterschiedliche Zielgruppen. Idealerweise sollten Sie über Dashboards verfügen, die einen ganzheitlichen Überblick über den Status und die Leistung des Systems bieten und gleichzeitig wichtige Geschäftsergebnisse und deren Auswirkungen hervorheben.

Amazon CloudWatch-Dashboards sind anpassbare Startseiten in der CloudWatch-Konsole zur Überwachung Ihrer Ressourcen in einer einzigen Ansicht, auch wenn sie über verschiedene AWS-Regionen und Konten verteilt sind.

Implementierungsschritte

1. Erstellen eines einfachen Dashboards: Erstellen Sie ein neues Dashboard in CloudWatch und geben Sie ihm einen aussagekräftigen Namen.
2. Verwenden von Markdown-Widgets: Bevor Sie sich mit den Metriken befassen, verwenden Sie Markdown-Widgets, um oben in Ihrem Dashboard inhaltlichen Kontext hinzuzufügen. Dieser sollte den Inhalt des Dashboards beschreiben und angeben, welche Bedeutung den dargestellten Metriken zukommt. Er kann auch Links zu anderen Dashboards und Tools zur Fehlerbehebung enthalten.
3. Erstellen von Dashboard-Variablen: Integrieren Sie gegebenenfalls Dashboard-Variablen, um dynamische und flexible Dashboard-Ansichten zu ermöglichen.
4. Erstellung von Metrik-Widgets: Fügen Sie Metrik-Widgets hinzu, um verschiedene Metriken zu visualisieren, die Ihre Anwendung ausgibt, und passen Sie diese Widgets so an, dass sie den Systemstatus und die Geschäftsergebnisse effektiv darstellen.
5. Protokollieren von Insights-Abfragen: Nutzen Sie CloudWatch Log Insights, um aus Ihren Protokollen umsetzbare Metriken abzuleiten und diese Erkenntnisse in Ihrem Dashboard anzuzeigen.
6. Einrichten von Alarmen: Integrieren Sie CloudWatch-Alarme in Ihr Dashboard, um sich einen schnellen Überblick über alle Metriken zu verschaffen, die ihre Schwellenwerte überschreiten.
7. Verwenden von Contributor Insights: Integrieren Sie CloudWatch Contributor Insights, um Felder mit hoher Kardinalität zu analysieren und die besten Mitarbeiter Ihrer Ressource zu identifizieren.
8. Entwerfen benutzerdefinierter Widgets: Erwägen Sie die Erstellung von benutzerdefinierten Widgets für spezielle Anforderungen, die von Standard-Widgets nicht erfüllt werden. Diese können Daten aus verschiedenen Quellen abrufen oder sie auf einzigartige Weise darstellen.

9. Verwendung von AWS Health Dashboard: Verwenden Sie AWS Health Dashboard, um detailliertere Einblicke in den Zustand Ihres Kontos, in Ereignisse und bevorstehende Änderungen zu erhalten, die sich auf Ihre Services und Ressourcen auswirken könnten. Sie können auch eine zentrale Übersicht über Statusereignisse in AWS Organizations abrufen oder Ihre eigenen benutzerdefinierten Dashboards erstellen (weitere Informationen finden Sie unter „Verwandte Beispiele“).
10. Iteration und Anpassung: Im Laufe der Entwicklung Ihrer Anwendung sollten Sie Ihr Dashboard regelmäßig überprüfen, um sicherzustellen, dass es weiterhin relevant ist.

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS08-BP01 Analysieren von Workload-Metriken
- OPS08-BP02 Analysieren von Workload-Protokollen
- OPS08-BP03 Analysieren von Workload-Traces
- OPS08-BP04 Erstellen umsetzbarer Warnmeldungen

Zugehörige Dokumente:

- Erstellung von Dashboards für operative Sichtbarkeit
- Verwendung von Amazon CloudWatch-Dashboards

Zugehörige Videos:

- Erstellung von konto- und regionenübergreifenden CloudWatch-Dashboards
- AWS re:Invent 2021 – Mehr Unternehmenstransparenz mit geschäftsorientierten AWS Cloud-Dashboards

Zugehörige Beispiele:

- Workshop zur Beobachtbarkeit
- Anwendungsüberwachung mit Amazon CloudWatch
- Intelligence Dashboards und Erkenntnisse zu AWS Health-Ereignissen

- Visualisieren Sie AWS Health-Ereignisse mit Amazon Managed Grafana

Grundlegendes zum betrieblichen Status

Definieren, erfassen und analysieren Sie Metriken für Operationen, um einen Einblick in die Aktivitäten Ihrer Operations-Teams zu erhalten. Dies ist wichtig, damit Sie bei Bedarf entsprechende Maßnahmen ergreifen können.

Ihre Organisation sollte in der Lage sein, den operativen Zustand problemlos in Erfahrung zu bringen. Sie sollten die Geschäftsziele Ihrer Operations-Teams definieren, wichtige Leistungsindikatoren identifizieren, die diese widerspiegeln, und dann Metriken auf der Grundlage der Betriebsergebnisse entwickeln, um nützliche Erkenntnisse zu gewinnen. Aus diesen Metriken sollten Sie Dashboards und Berichte erstellen, die Aufschluss über geschäftliche und technische Aspekte geben, damit Führungskräfte und Stakeholder gut fundierte Entscheidungen treffen können.

AWS macht es einfacher, Ihre Betriebsprotokolle zusammenzuführen und zu analysieren, sodass Sie Metriken generieren, den Status Ihrer betrieblichen Abläufe kennen und Einblicke in die Abläufe im Laufe der Zeit gewinnen können.

Bewährte Methoden

- OPS09-BP01 Messen operativer Ziele und KPIs mit Metriken
- OPS09-BP02 Kommunizieren von Status und Trends zur Sicherung der operativen Transparenz
- OPS09-BP03 Überprüfen der Betriebsmetriken und Priorisieren von Verbesserungen

OPS09-BP01 Messen operativer Ziele und KPIs mit Metriken

Ermitteln Sie Ziele und KPIs in Ihrem Unternehmen, die operativen Erfolg definieren, und legen Sie Metriken fest, die diese Werte widerspiegeln. Legen Sie Baselines als Bezugspunkt fest und bewerten Sie diese regelmäßig neu. Entwickeln Sie Mechanismen, um diese Metriken von Teams zur Bewertung zu erfassen.

Gewünschtes Ergebnis:

- Die Ziele und KPIs für die Operations-Teams der Organisation wurden veröffentlicht und geteilt.
- Metriken, die diese KPIs widerspiegeln, wurden festgelegt. Mögliche Beispiele:
  - Tiefe der Ticket-Queue oder Durchschnittsalter der Tickets
  - Anzahl der Tickets, gruppiert nach Art des Problems

- Aufgewendete Zeit für die Bearbeitung von Problemen mit oder ohne standardisierte Betriebsverfahren (SOP)
- Zeit, die zur Wiederherstellung nach einem fehlgeschlagenen Code-Push aufgewendet wurde
- Anrufaufkommen

Typische Anti-Muster:

- Bereitstellungsfristen werden nicht eingehalten, weil Entwickler mit der Lösung von Problemen beauftragt werden. Entwicklerteams fordern mehr Personal, können aber nicht einschätzen, wie viele Personen benötigt werden, da der Zeitaufwand nicht gemessen werden kann.
- Für die Abwicklung von Kundenanrufen wurde ein Problem-Desk Stufe 1 eingerichtet. Im Laufe der Zeit kamen weitere Workloads hinzu, aber dem Problem-Desk Stufe 1 wurde kein zusätzliches Personal zugewiesen. Die Kundenzufriedenheit leidet, da immer mehr Anrufe nötig sind und Probleme länger ungelöst bleiben. Das Management sieht diese Anzeichen jedoch nicht und ermöglicht keine Gegenmaßnahmen.
- Ein problematischer Workload wurde zur Bearbeitung an ein separates Operations-Team übergeben. Im Gegensatz zu anderen Workloads wurde dieser neue Workload nicht mit ordnungsgemäßer Dokumentation und Runbooks geliefert. Daher verbringen Teams mehr Zeit damit, Fehler zu suchen und zu beheben. Es gibt jedoch keine Metriken, die dies dokumentieren, was die Rechenschaftspflicht erschwert.

Vorteile der Nutzung dieser bewährten Methode: Während die Workload-Überwachung den Status unserer Anwendungen und Services anzeigt, liefert die Überwachung von Operations-Teams den Verantwortlichen Erkenntnisse hinsichtlich Veränderungen bei den Nutzern dieser Workloads, wie z. B. sich ändernde Geschäftsanforderungen. Messen Sie die Effektivität dieser Teams und bewerten Sie sie im Hinblick auf Ihre operativen Ziele, indem Sie Metriken erstellen, die den operativen Status widerspiegeln können. Anhand von Metriken können Supportprobleme aufgezeigt oder Abweichungen von einem angestrebten Servicelevel erkannt werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Planen Sie Meetings mit der Geschäftsleitung und den Stakeholdern, um die allgemeinen Ziele des Services festzulegen. Ermitteln Sie, worin die Aufgaben der verschiedenen Operations-Teams bestehen sollten und mit welchen Herausforderungen sie beauftragt werden könnten. Führen Sie

anhand dieser Daten ein Brainstorming der wichtigsten Leistungsindikatoren (KPIs) durch, die diese operativen Ziele widerspiegeln könnten. Dies können Faktoren wie Kundenzufriedenheit, Zeitspanne zwischen Entwurf und Bereitstellung von Funktionen, durchschnittlicher Zeitaufwand für die Problemlösung und andere sein.

Identifizieren Sie anhand der KPIs die Metriken und Datenquellen, die diese Ziele am besten widerspiegeln könnten. Kundenzufriedenheit kann eine Kombination aus verschiedenen Metriken wie Warte- oder Reaktionszeiten bei Anrufen, Zufriedenheitswerte und Art der dargelegten Probleme sein. Die Bereitstellungszeiten können die Summe des Zeitaufwands sein, der für Tests und Bereitstellungen benötigt wird, zuzüglich aller Korrekturen nach der Bereitstellung, die hinzugefügt werden mussten. Statistiken, aus denen hervorgeht, wie viel Zeit für verschiedene Arten von Problemen aufgewendet wurde (oder wie viele dieser Probleme auftraten), können Aufschluss darüber geben, wo gezielte Anstrengungen erforderlich sind.

Ressourcen

Zugehörige Dokumente:

- Amazon QuickSight - Using KPIs (Amazon QuickSight – Verwendung von KPIs)
- Amazon CloudWatch - Using Metrics (Amazon CloudWach – Verwendung von Metriken)
- Erstellung von Dashboards
- Wie Sie mit dem KPI-Dashboard Ihre KPIs zur Kostenoptimierung nachverfolgen

OPS09-BP02 Kommunizieren von Status und Trends zur Sicherung der operativen Transparenz

Wenn Sie in Erfahrung bringen wollen, wann Ergebnisse gefährdet sein könnten, ob zusätzliche Workloads unterstützt werden können oder nicht oder welche Auswirkungen Änderungen auf Ihre Teams hatten, müssen Sie unbedingt den Status Ihrer Betriebsabläufe und deren Trendrichtung kennen. Bei Betriebsereignissen können Statusseiten, auf denen Benutzer und Operations-Teams Informationen abrufen können, den Druck auf die Kommunikationskanäle verringern und Informationen proaktiv verbreiten.

Gewünschtes Ergebnis:

- Betriebsleiter erhalten auf einen Blick Erkenntnisse darüber, welches Anrufvolumen ihre Teams bewältigen müssen und welche Maßnahmen möglicherweise im Gange sind, z. B. Bereitstellungen.

- Wenn Auswirkungen auf den normalen Betrieb auftreten, werden Warnmeldungen an Stakeholder und Nutzergemeinschaften versendet.
- Unternehmensleitung und Stakeholder können als Reaktion auf eine Warnung oder Auswirkung eine Statusseite aufrufen und Informationen zu einem betrieblichen Ereignis abrufen, z. B. Kontaktstellen, Ticketinformationen und erwartete Wiederherstellungszeiten.
- Führungskräften und anderen Stakeholdern werden Berichte zur Verfügung gestellt, damit sie über Betriebsstatistiken wie das Anrufvolumen über einen bestimmten Zeitraum, Nutzerzufriedenheitswerte, Anzahl ausstehender Tickets und deren Alter informiert sind.

Typische Anti-Muster:

- Ein Workload fällt aus und ein Dienst wird nicht verfügbar. Das Anrufvolumen steigt, da Benutzer wissen möchten, was vor sich geht. Manager erhöhen dieses Volumen, da sie nachfragen, wer an dem Problem arbeitet. Verschiedene Operations-Teams bemühen sich doppelt, Untersuchungen durchzuführen.
- Der Wunsch nach neuen Funktionen führt dazu, dass mehrere Mitarbeiter umpositioniert werden, um an einem speziellen technischen Vorhaben zu arbeiten. Dadurch entstehende Lücken werden nicht aufgefüllt und die Problemlösungszeiten steigen. Diese Informationen werden nicht erfasst, und erst nach mehreren Wochen und viel negativem Feedback unzufriedener Nutzer wird die Unternehmensleitung auf das Problem aufmerksam.

Vorteile der Nutzung dieser bewährten Methode: Bei betrieblichen Ereignissen, die das Geschäft beeinträchtigen, wird manchmal viel Zeit und Energie damit verschwendet, Informationen von verschiedenen Teams abzufragen, die versuchen, die Situation zu verstehen. Durch die Einrichtung und Verbreitung von Statusseiten und Dashboards können Stakeholder rasch Informationen darüber abrufen, ob ein Problem festgestellt wurde oder nicht, wer mit der Lösung des Problems beschäftigt ist oder wann mit einer Rückkehr zum normalen Betrieb zu rechnen ist. Dadurch müssen die Teammitglieder nicht zu viel Zeit damit verbringen, anderen den Status mitzuteilen und haben mehr Zeit, Probleme zu lösen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Erstellen Sie Dashboards, die die aktuellen Schlüsselmetriken für Ihre Operations-Teams anzeigen, und machen Sie sie sowohl für die Betriebsleitung als auch für das Management leicht zugänglich.

Erstellen Sie Statusseiten, die schnell aktualisiert werden können, um zu zeigen, wann sich ein Vorfall oder ein Ereignis abspielt, wer dafür verantwortlich ist und wer die Reaktion darauf koordiniert. Kommunizieren Sie auf dieser Seite alle Schritte oder Problemumgehungen, die Benutzer in Betracht ziehen sollten, und machen Sie sie für alle Beteiligten verfügbar. Bitten Sie Benutzer, zuerst diese Seite zu überprüfen, wenn sie mit einem unbekannten Problem konfrontiert werden.

Erfassen Sie Daten und stellen Sie Berichte bereit, die den Zustand der Betriebsabläufe im Zeitverlauf aufzeigen, und verteilen Sie diese an Führungskräfte und Entscheidungsträger, um die Arbeit des Betriebs sowie die Herausforderungen und Bedürfnisse zu veranschaulichen.

Teilen Sie die Metriken und Berichte, die die Ziele und KPIs am besten widerspiegeln, mit den Teams, und zeigen Sie ihnen, wo sie besonders deutlich einen Wandel vorangetrieben haben. Nehmen Sie sich Zeit für diese Aktivitäten, um den Abläufen innerhalb und zwischen Teams mehr Bedeutung beizumessen.

Ressourcen

Zugehörige Dokumente:

- Measure Progress (Fortschritt messen)
- Building Dashboards for Operational Visibility (Erstellung von Dashboards für operative Sichtbarkeit)

Zugehörige Lösungen:

- Datenoperationen

OPS09-BP03 Überprüfen der Betriebsmetriken und Priorisieren von Verbesserungen

Durch die Bereitstellung von Zeit und Ressourcen für die Überprüfung des Betriebsstatus wird sichergestellt, dass die Betreuung der täglichen Geschäftstätigkeit weiterhin Priorität hat. Bringen Sie Betriebsleiter und Stakeholder an einen Tisch, um regelmäßig Metriken zu überprüfen, Ziele und Vorgaben zu bestätigen oder zu ändern und Verbesserungen zu priorisieren.

Gewünschtes Ergebnis:

- Betriebsleiter und Mitarbeiter treffen sich regelmäßig, um die Metriken für einen bestimmten Berichtszeitraum zu überprüfen. Herausforderungen werden kommuniziert, Erfolge gefeiert und gewonnene Erkenntnisse geteilt.
- Stakeholder und Unternehmensleiter werden regelmäßig über den Stand der laufenden Operationen informiert und um ihre Meinung gebeten, was Ziele, KPIs und zukünftige Initiativen angeht. Kompromisse zwischen Servicebereitstellung, Betrieb und Wartung werden erörtert und in Zusammenhang gebracht.

Typische Anti-Muster:

- Ein neues Produkt wird auf den Markt gebracht, aber die Operations-Teams der Stufe 1 und 2 sind nicht ausreichend geschult, um Support zu leisten, oder bräuchten zusätzliches Personal. Metriken, die den Anstieg der Bearbeitungsdauer von Tickets und der Anzahl der Vorfälle belegen, werden von Führungskräften nicht berücksichtigt. Erst Wochen später werden Maßnahmen ergriffen, weil die Zahl der Abonnements zu sinken beginnt, da unzufriedene Benutzer die Plattform verlassen.
- Ein manuelles Verfahren zur Durchführung von Wartungsarbeiten an einem Workload gibt es schon lange. Der Wunsch nach Automatisierung war zwar vorhanden, hatte aber angesichts der geringen Bedeutung des Systems nur geringe Priorität. Im Laufe der Zeit hat das System jedoch an Bedeutung gewonnen, und heute nehmen diese manuellen Prozesse einen Großteil der Betriebszeit in Anspruch. Es sind keine Ressourcen für die Bereitstellung von mehr Tools für den Betrieb vorgesehen, was zu einer Überlastung der Mitarbeiter führt, wenn der Workload zunimmt. Die Unternehmensleitung wird sich der Probleme bewusst, als sie erfährt, dass Mitarbeiter zu anderen Wettbewerbern wechseln.

Vorteile der Nutzung dieser bewährten Methode: In einigen Unternehmen kann es zu einer Herausforderung werden, für die Servicebereitstellung die gleiche Zeit und Aufmerksamkeit aufzuwenden, die neuen Produkten oder Angeboten entgegengebracht wird. Wenn dies zutrifft, kann der Geschäftsbereich darunter leiden und das erwartete Serviceniveau verschlechtert sich nach und nach. Dies liegt daran, dass sich der Betrieb nicht mit dem wachsenden Geschäft ändert und weiterentwickelt, wodurch er bald ins Hintertreffen gerät. Ohne eine regelmäßige Überprüfung der Erkenntnisse, die Operations erfasst, wird das Risiko für das Unternehmen möglicherweise erst sichtbar, wenn es zu spät ist. Wenn jedoch sowohl dem Betriebspersonal als auch den Führungskräften Zeit für die Überprüfung von Metriken und Verfahren eingeräumt wird, bleibt die entscheidende Rolle, die der Betrieb spielt, sichtbar und Risiken können erkannt werden, lange bevor sie ein kritisches Niveau erreichen. Operations-Teams erhalten einen besseren Überblick über bevorstehende Geschäftsänderungen und Initiativen, sodass proaktive Maßnahmen ergriffen werden

können. Wenn Führungskräfte die Gelegenheit haben, die Betriebsmetriken zu prüfen, erkennen sie, welche Rolle diese Teams für die Kundenzufriedenheit spielen –sowohl intern als auch extern. So können sie Operations die Möglichkeit geben, Entscheidungen im Hinblick auf Prioritäten besser abzuwägen oder sicherzustellen, dass die Teams über die Zeit und die Ressourcen verfügen, um mit neuen Geschäfts- und Workload-Initiativen zu wachsen und sich weiterzuentwickeln.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Nehmen Sie sich Zeit, um die Betriebsmetriken gemeinsam mit Stakeholdern und Operations-Teams zu überprüfen und die Berichtsdaten zu lesen. Stellen Sie diese Berichte in den Kontext der Ziele und Vorgaben der Organisation, um festzustellen, ob sie erreicht werden. Identifizieren Sie Unklarheiten, bei denen die Ziele nicht eindeutig sind oder wo Konflikte bestehen zwischen dem, was verlangt wird, und dem, was gegeben wird.

Identifizieren Sie, wo Zeit, Mitarbeiter und Tools zu Betriebsergebnissen beitragen können. Ermitteln Sie, auf welche KPIs sich dies auswirken würde und welche Erfolgsziele verfolgt werden sollten. Greifen Sie Ihre Überlegungen regelmäßig wieder auf, um sicherzustellen, dass der Betrieb über ausreichende Ressourcen verfügt, um den Geschäftsbereich zu unterstützen.

Ressourcen

Zugehörige Dokumente:

- Amazon Athena
- Amazon CloudWatch metrics and dimensions reference (Referenzinformationen zu Metriken und Dimensionen von Amazon CloudWatch)
- Amazon QuickSight
- AWS Glue
- AWS Glue Data Catalog
- Collect metrics and logs from Amazon EC2 instances and on-premises servers with the Amazon CloudWatch Agent (Erfassen von Metriken und Protokollen aus Amazon EC2-Instances und On-Premises-Servern mit dem Amazon CloudWatch Agent)
- Using Amazon CloudWatch metrics (Verwenden von Amazon CloudWatch-Metriken)

Reagieren auf Ereignisse

Sie sollten für betriebliche Ereignisse Vorsorge tragen. Das gilt sowohl für geplante Ereignisse (z. B. Verkaufsaktionen, Bereitstellungen oder Fehlertests) als auch für ungeplante Ereignisse (z. B. Auslastungsspitzen oder Ausfälle von Komponenten). Beim Reagieren auf Alarme sollten Sie Ihre Runbooks und Playbooks zu Rate ziehen, um konsistente Resultate zu erbringen. Für definierte Alarme sollte eine Rolle oder ein Team als Besitzer festgelegt sein, das für die Reaktion und Eskalation verantwortlich ist. Sie werden auch wissen möchten, welche geschäftlichen Auswirkungen Systemkomponenten haben, um bei Bedarf zielgerichtete Maßnahmen einleiten zu können. Nach Ereignissen sollten Sie eine Ursachenanalyse durchführen und anschließend dafür sorgen, dass sich der Fehler nicht wiederholt, oder notieren, wie sich das Problem zukünftig umgehen lässt.

AWS stellt geeignete Tools für alle Aspekte Ihrer Workloads und Betriebsabläufe als Code bereit und macht es Ihnen damit leichter, auf Ereignisse zu reagieren. Mithilfe dieser Tools können Sie Reaktionen auf betriebliche Ereignisse in Skripts definieren und diese Skripts dann als Reaktion auf Überwachungsdaten starten.

In AWS können Sie die Zeitdauer von Wiederherstellungsvorgängen verkürzen, indem Sie ausgefallene Komponenten einfach durch funktionierende Versionen ersetzen lassen, anstatt sie zu reparieren. Die ausgefallene Ressource können Sie dann genauer untersuchen, nachdem sie außer Betrieb genommen wurde.

Bewährte Methoden

- OPS10-BP01 Verwenden eines Prozesses für die Bewältigung von Ereignissen, Vorfällen und Problemen
- OPS10-BP02 Implementieren eines Prozesses für jede Warnmeldung
- OPS10-BP03 Priorisieren von betrieblichen Ereignissen auf Basis der Auswirkung auf das Unternehmen
- OPS10-BP04 Definieren von Eskalationspfaden
- OPS10-BP05 Definieren eines Kundenkommunikationsplan für Ereignisse, die sich auf den Service auswirken
- OPS10-BP06 Bekanntgeben des Status über Dashboards
- OPS10-BP07 Automatisieren von Reaktionen auf Ereignisse

OPS10-BP01 Verwenden eines Prozesses für die Bewältigung von Ereignissen, Vorfällen und Problemen

Die Fähigkeit, Ereignisse, Vorfälle und Probleme effizient zu verwalten, ist der Schlüssel zur Aufrechterhaltung des Workloads und der Leistung. Es ist wichtig, die Unterschiede zwischen diesen Elementen zu erkennen und zu verstehen, um eine effektive Reaktions- und Lösungsstrategie zu entwickeln. Die Einrichtung und Einhaltung eines klar definierten Prozesses für jeden Aspekt hilft Ihrem Team, alle auftretenden betrieblichen Herausforderungen schnell und effektiv zu bewältigen.

Gewünschtes Ergebnis: Ihr Unternehmen verwaltet betriebliche Ereignisse, Vorfälle und Probleme effektiv durch gut dokumentierte und zentral gespeicherte Prozesse. Diese Prozesse werden ständig aktualisiert, um Änderungen zu berücksichtigen, die Handhabung zu optimieren und eine hohe Servicezuverlässlichkeit und Workload-Leistung aufrechtzuerhalten.

Typische Anti-Muster:

- Sie reagieren eher reaktiv als proaktiv auf Ereignisse.
- Bei verschiedenen Arten von Ereignissen oder Vorfällen werden inkonsistente Ansätze verfolgt.
- Ihr Unternehmen analysiert keine Vorfälle und lernt nicht aus ihnen, um zukünftige Vorfälle zu verhindern.

Vorteile der Nutzung dieser bewährten Methode:

- optimierte und standardisierte Reaktionsprozesse
- geringere Auswirkungen von Vorfällen auf Services und Kunden
- beschleunigte Problemlösung
- kontinuierliche Verbesserung der betrieblichen Abläufe

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Wenn Sie diese bewährte Methode implementieren, bedeutet dies, dass Sie Workload-Ereignisse nachverfolgen. Sie haben Prozesse für den Umgang mit Vorfällen und Problemen. Die Prozesse werden dokumentiert, geteilt und oft aktualisiert. Die Probleme werden identifiziert, priorisiert und behoben.

Verstehen von Ereignissen, Vorfällen und Problemen

- Ereignisse: Bei einem Ereignis kann es sich um eine Beobachtung einer Aktion, eines Vorkommens oder einer Statusänderung handeln. Ereignisse können geplant oder ungeplant sein und sie können intern oder extern zum Workload entstehen.
- Vorfälle: Vorfälle sind Ereignisse, die eine Reaktion erfordern, wie ungeplante Unterbrechungen oder Beeinträchtigungen der Servicequalität. Sie stellen Störungen dar, die sofortige Aufmerksamkeit erfordern, um den normalen Workload-Betrieb wiederherzustellen.
- Probleme: Probleme sind die zugrundeliegenden Ursachen für einen oder mehrere Vorfälle. Bei der Identifizierung und Lösung von Problemen geht es darum, den Vorfällen auf den Grund zu gehen, um zukünftige Vorfälle zu verhindern.

Implementierungsschritte

Ereignisse

1. Überwachen von Ereignissen:
   - Implementieren Sie die Beobachtbarkeit und nutzen Sie die Beobachtbarkeit des Workloads.
   - Monitor-Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in AWS CloudTrailaufgezeichnet.
   - Reagieren Sie auf betriebliche Änderungen in Ihren Anwendungen in Echtzeit mit Amazon EventBridge,.
   - Kontinuierliche Bewertung, Überwachung und Aufzeichnung von Änderungen der Ressourcenkonfiguration mit AWS Config.
2. Erstellen von Prozessen:
   - Entwickeln Sie ein Verfahren zur Beurteilung, welche Ereignisse signifikant sind und überwacht werden müssen. Dies beinhaltet die Festlegung von Schwellenwerten und Parametern für normale und abnormale Aktivitäten.
   - Legen Sie Kriterien für die Eskalation eines Ereignisses in Bezug auf einen Vorfall fest. Dies kann auf Grundlage des Schweregrads, der Auswirkungen auf die Benutzer oder der Abweichung vom erwarteten Verhalten erfolgen.
   - Überprüfen Sie regelmäßig die Prozesse zur Überwachung und Reaktion auf Ereignisse. Dazu gehören die Analyse früherer Vorfälle, die Anpassung von Schwellenwerten und die Verfeinerung von Warnmechanismen.

Vorfälle

1. Reaktion auf Vorfälle:
   - Nutzen Sie die Erkenntnisse aus den Tools zur Beobachtbarkeit, um Vorfälle schnell zu erkennen und darauf zu reagieren.
   - Implementieren Sie AWS Systems Manager Ops Center , um betriebliche Aufgaben und Vorfälle zu sammeln, zu organisieren und zu priorisieren.
   - Verwenden Sie Services wie Amazon CloudWatch und AWS X-Ray für eingehendere Analysen und Problembehebungen.
   - Ziehen Sie AWS Managed Services (AMS) für ein verbessertes Vorfallmanagement in Betracht, indem Sie die proaktiven, präventiven und detektivischen Fähigkeiten nutzen. AMS erweitert den betrieblichen Support um Services wie Überwachung, Vorfallserkennung und -reaktion sowie Sicherheitsmanagement.
   - Kunden von Enterprise Support können AWS-Vorfallerkennung und -reaktionverwenden, wodurch eine kontinuierliche proaktive Überwachung und ein Vorfallmanagement für Produktions-Workloads ermöglicht wird.
2. Erstellen eines Vorfallmanagementprozesses:
   - Richten Sie einen strukturierten Vorfallmanagementprozess ein, der klare Rollen, Kommunikationsprotokolle und Lösungsschritte umfasst.
   - Integrieren Sie das Vorfallmanagement mit Tools wie AWS Chatbot für eine effiziente Reaktion und Koordination.
   - Kategorisieren Sie Vorfälle nach Schweregrad mit vordefinierten Plänen zur Vorfallreaktion für die einzelnen Kategorien.
3. Lernen und Verbessern:
   - Führen Sie Analysen nach Vorfällen durch, um die Grundursachen und die Effektivität der Lösung zu verstehen.
   - Aktualisieren und verbessern Sie die Reaktionspläne kontinuierlich auf Grundlage von Überprüfungen und sich entwickelnden Praktiken.
   - Dokumentieren Sie die gewonnenen Erkenntnisse und geben Sie sie an andere Teams weiter, um die betriebliche Widerstandsfähigkeit zu verbessern.
   - Kunden mit Enterprise Support können den Workshop zum Vorfallmanagement bei ihrem Technical Account Manager anfordern. Dieser angeleitete Workshop testet Ihren vorhandenen Reaktionsplan für Vorfälle und hilft Ihnen, Verbesserungsmöglichkeiten zu identifizieren.

Probleme

1. Identifizieren von Problemen:
   - Verwenden Sie Daten aus früheren Vorfällen, um wiederkehrende Muster zu erkennen, die auf tiefere systemische Probleme hinweisen könnten.
   - Nutzen Sie Tools wie AWS CloudTrail und Amazon CloudWatch, um Trends zu analysieren und zugrunde liegende Probleme aufzudecken.
   - Binden Sie funktionsübergreifende Teams ein, einschließlich Betriebs-, Entwicklungs- und Geschäftsbereiche, um unterschiedliche Sichtweisen auf die Grundursachen zu gewinnen.
2. Erstellen eines Problemmanagementprozesses:
   - Entwickeln Sie einen strukturierten Prozess für das Problemmanagement, der sich auf langfristige Lösungen statt auf schnelle Lösungen konzentriert.
   - Integrieren Sie Techniken zur Ursachenanalyse, um die zugrunde liegenden Ursachen von Vorfällen zu untersuchen und zu verstehen.
   - Aktualisieren Sie Betriebsrichtlinien, Verfahren und Infrastruktur auf Grundlage der Ergebnisse, um Wiederholungen zu verhindern.
3. Kontinuierliche Verbesserungen:
   - Fördern Sie eine Kultur des ständigen Lernens und der Verbesserung und ermutigen Sie Ihre Teams, potenzielle Probleme proaktiv zu erkennen und anzugehen.
   - Überprüfen und überarbeiten Sie regelmäßig die Problemmanagementprozesse und -tools, um sie an die sich entwickelnde Geschäfts- und Technologielandschaft anzupassen.
   - Tauschen Sie Erkenntnisse und bewährte Methoden innerhalb des Unternehmens aus, um eine widerstandsfähigere und effizientere Betriebsumgebung zu schaffen.
4. Einsatz von AWS Support:
   - Verwenden Sie AWS-Support-Ressourcen, wie z. B. AWS Trusted Advisor,für proaktive Anleitungen und Optimierungsempfehlungen.
   - Kunden von Enterprise Support können auf spezielle Programme wie AWS-Countdown zugreifen, um bei kritischen Ereignissen Unterstützung zu erhalten.
   -

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS04-BP02 Implementieren einer Anwendungstelemetrie
- OPS07-BP03 Verwenden von Runbooks zur Durchführung von Verfahren
- OPS07-BP04 Verwenden von Playbooks zum Untersuchen von Problemen
- OPS08-BP01 Analysieren von Workload-Metriken
- OPS11-BP02 Durchführen von Analysen nach Vorfällen

Zugehörige Dokumente:

- Leitfaden für AWS Security Incident Response
- AWS-Vorfallerkennung und -reaktion
- AWS Cloud Adoption Framework: Betriebsperspektive – Vorfall- und Problemmanagement
- Vorfallmanagement im Zeitalter von DevOps und SRE
- PagerDuty - What is Incident Management?

Zugehörige Videos:

- Die besten Tipps zur Reaktion auf Vorfälle in AWS
- AWS re:Invent 2022 – Die Amazon Builders' Library: 25 Jahre operative Exzellenz von Amazon
- AWS re:Invent 2022 – AWS-Vorfallerkennung und -reaktion (SUP201)
- Einführung von Incident Manager von AWS Systems Manager

Zugehörige Beispiele:

- AWS Proactive Services – Workshop zum Vorfallmanagement
- Automatisierung der Vorfallbehandlung mit PagerDuty und AWS Systems Manager Incident Manager
- Einbeziehung des Notfallteams in die Bereitschaftsdienstpläne in AWS Systems Manager Incident Manager

- Verbesserung der Sichtbarkeit und Zusammenarbeit bei der Bearbeitung von Vorfällen in AWS Systems Manager Incident Manager
- Vorfallberichte und Serviceanfragen in AMS

Zugehörige Services:

- Amazon EventBridge,

OPS10-BP02 Implementieren eines Prozesses für jede Warnmeldung

Die Einrichtung eines klaren und definierten Prozesses für jede Warnmeldung in Ihrem System ist für ein effektives und effizientes Vorfallmanagement unerlässlich. Diese Vorgehensweise stellt sicher, dass jede Warnmeldung zu einer spezifischen, umsetzbaren Reaktion führt, wodurch die Zuverlässigkeit und Reaktionsfähigkeit Ihrer Abläufe verbessert wird.

Gewünschtes Ergebnis: Jede Warnmeldung leitet einen bestimmten, genau definierten Reaktionsplan ein. Wenn möglich, werden die Antworten automatisiert, mit klaren Zuständigkeiten und einem definierten Eskalationspfad. Warnmeldungen sind mit einer aktuellen Wissensdatenbank verknüpft, sodass jeder Bediener konsistent und effektiv reagieren kann. Die Antworten sind schnell und einheitlich, was die betriebliche Effizienz und Zuverlässigkeit erhöht.

Typische Anti-Muster:

- Für Warnmeldungen gibt es keinen vordefinierten Reaktionsprozess, was zu provisorischen und verzögerten Lösungen führt.
- Eine Überlastung mit Warnmeldungen führt dazu, dass wichtige Warnmeldungen übersehen werden.
- Warnmeldungen werden uneinheitlich gehandhabt, da es an klaren Zuständigkeiten und Verantwortlichkeiten mangelt.

Vorteile der Nutzung dieser bewährten Methode:

- Weniger Ermüdungserscheinungen, da nur umsetzbare Warnmeldungen ausgelöst werden.
- Geringere durchschnittliche Zeit bis zur Behebung (MTTR) von Betriebsproblemen.
- Geringere durchschnittliche Zeit bis zur Untersuchung, was zur Verringerung der MTTR beiträgt.
- Verbesserte Fähigkeit, operative Reaktionen zu skalieren.

- Verbesserte Konsistenz und Zuverlässigkeit bei der Behandlung von Betriebsereignissen.

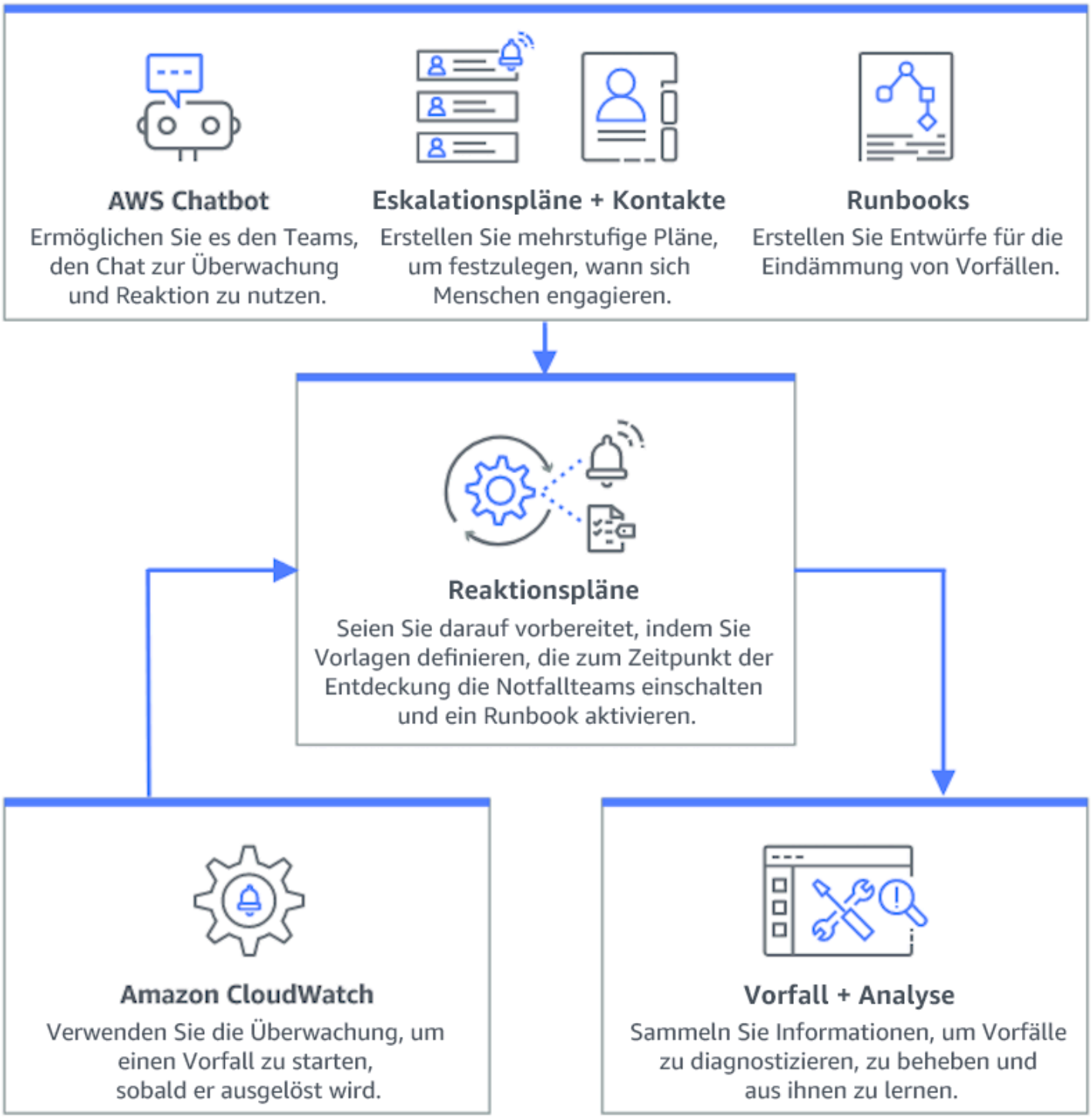
Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Ein Prozess pro Warnmeldung beinhaltet die Erstellung eines klaren Reaktionsplans für jede Warnmeldung, die Automatisierung von Reaktionen (soweit dies möglich ist) und die kontinuierliche Optimierung dieser Prozesse auf Grundlage des betrieblichen Feedbacks und der sich entwickelnden Anforderungen.

Implementierungsschritte

Das folgende Diagramm veranschaulicht den Arbeitsablauf für das Vorfallmanagement in AWS Systems Manager Incident Manager. Es ist so konzipiert, dass es schnell auf betriebliche Probleme reagiert, indem es automatisch Vorfälle als Reaktion auf bestimmte Ereignisse von Amazon CloudWatch oder Amazon EventBridgegeneriert. Wenn ein Vorfall entweder automatisch oder manuell erstellt wird, zentralisiert Incident Manager die Verwaltung des Vorfalls, organisiert relevante Informationen über AWS-Ressourcen und initiiert vordefinierte Reaktionspläne. Dazu gehört das Ausführen von Systems Manager-Automation-Runbooks für sofortige Maßnahmen sowie das Erstellen eines übergeordneten betrieblichen Arbeitselements in OpsCenter, um verwandte Aufgaben und Analysen zu verfolgen. Dieser optimierte Prozess beschleunigt und koordiniert die Reaktion auf Vorfälle in Ihrer gesamten AWS-Umgebung.



1. Zusammengesetzte Alarme, Erstellen Sie zusammengesetzte Alarme in CloudWatch, um zusammenhängende Alarme zu gruppieren, das Rauschen zu reduzieren und sinnvollere Reaktionen zu ermöglichen.

2. Integrieren Sie Amazon CloudWatch-Alarme mit Incident Manager Konfigurieren Sie CloudWatch-Alarme zur automatischen Erstellung von Vorfällen in AWS Systems Manager Incident Manager.
3. Verwenden von Amazon EventBridge mit Incident Manager: Erstellen Sie EventBridge-Regeln, um auf Ereignisse zu reagieren und Vorfälle mithilfe definierter Reaktionspläne zu erstellen.
4. Vorbereitung auf Vorfälle in Incident Manager:
   - Stellen Sie detaillierte Reaktionspläne in Incident Manager für jede Art von Warnmeldung auf.
   - Richten Sie über AWS Chatbot Chat-Kanäle ein, die mit Reaktionsplänen in Incident Manager verknüpft sind und die Echtzeitkommunikation bei Vorfällen über Plattformen wie Slack, Microsoft Teams und Amazon Chime ermöglichen.
   - Integrieren Sie Systems Manager-Automation-Runbooks in Incident Manager, um automatisierte Reaktionen auf Vorfälle zu ermöglichen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS04-BP01 Ermitteln wichtiger Leistungskennzahlen
- OPS08-BP04 Erstellen umsetzbarer Warnmeldungen

Zugehörige Dokumente:

- AWS Cloud Adoption Framework: Betriebsperspektive – Vorfall- und Problemmanagement
- Verwenden von Amazon CloudWatch-Alarmen
- Erste Schritte mit AWS Systems Manager Incident Manager
- Vorbereitung auf Vorfälle in Incident Manager

Zugehörige Videos:

- Die besten Tipps zur Reaktion auf Vorfälle in AWS

Zugehörige Beispiele:

- AWS-Workshops – AWS Systems Manager Incident Manager – Automatisierung der Reaktion auf Sicherheitsvorfälle

OPS10-BP03 Priorisieren von betrieblichen Ereignissen auf Basis der Auswirkung auf das Unternehmen

Eine schnelle Reaktion auf Betriebsereignisse ist von entscheidender Bedeutung, aber nicht alle Ereignisse sind gleich. Wenn Sie Ihre Prioritäten auf Grundlage der geschäftlichen Auswirkungen festlegen, müssen Sie sich auch vorrangig mit Ereignissen befassen, die erhebliche Folgen haben könnten, wie z. B. Sicherheit, finanzielle Verluste, Verstöße gegen Vorschriften oder Rufschädigung.

Gewünschtes Ergebnis: Die Reaktionen auf betriebliche Ereignisse werden auf Grundlage der potenziellen Auswirkungen auf die Geschäftsabläufe und -ziele priorisiert. Dadurch werden die Reaktionen effizient und effektiv.

Typische Anti-Muster:

- Jedes Ereignis wird mit der gleichen Dringlichkeit behandelt, was zu Verwirrung und Verzögerungen bei der Behandlung kritischer Probleme führt.
- Sie unterscheiden nicht zwischen Ereignissen mit hoher und geringer Auswirkung, was zu einer Fehlallokation von Ressourcen führt.
- Ihrem Unternehmen fehlt ein klarer Rahmen für die Priorisierung, was zu inkonsistenten Reaktionen auf Betriebsereignisse führt.
- Ereignisse werden in der Reihenfolge ihrer Meldung priorisiert und nicht nach ihrer Auswirkung auf die Geschäftsergebnisse.

Vorteile der Nutzung dieser bewährten Methode:

- Stellt sicher, dass wichtige Geschäftsfunktionen zuerst berücksichtigt werden, um mögliche Schäden zu minimieren.
- Verbessert die Ressourcenzuweisung bei mehreren gleichzeitigen Ereignissen.
- Verbessert die Fähigkeit der Organisation, das Vertrauen zu erhalten und die gesetzlichen Anforderungen zu erfüllen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Wenn Sie mit mehreren betrieblichen Ereignissen konfrontiert sind, ist ein strukturierter Ansatz zur Priorisierung auf Grundlage von Auswirkungen und Dringlichkeit unerlässlich. Dieser Ansatz hilft

Ihnen, fundierte Entscheidungen zu treffen, Ihre Maßnahmen auf die Bereiche zu lenken, wo sie am dringendsten benötigt werden, und das Risiko für die Geschäftskontinuität zu mindern.

Implementierungsschritte

1. Bewertung der Auswirkungen: Entwickeln Sie ein Klassifizierungssystem, um den Schweregrad von Ereignissen im Hinblick auf ihre potenziellen Auswirkungen auf den Geschäftsbetrieb und die Ziele zu bewerten. Das folgende Beispiel zeigt die Wirkungskategorien:

Auswirkungsgrad	Beschreibung
Hoch	Betrifft viele Mitarbeiter oder Kunden, hohe finanzielle Auswirkungen, hoher Reputatio nsschaden oder Verletzungen
Mittel	Betrifft eine Gruppe von Mitarbeitern oder Kunden, mäßige finanzielle Auswirkungen oder mäßiger Reputationsschaden
Niedrig	Betrifft einzelne Mitarbeiter oder Kunden, geringe finanzielle Auswirkungen oder geringer Reputationsschaden

2. Bewertung der Dringlichkeit: Definieren Sie Dringlichkeitsstufen danach, wie schnell auf ein Ereignis reagiert werden muss, und berücksichtigen Sie dabei Faktoren wie Sicherheit, finanzielle Auswirkungen und Service Level Agreements (SLAs). Das folgende Beispiel zeigt die Dringlichkeitskategorien:

Dringlichkeitsstufe	Beschreibung
Hoch	Exponentiell steigender Schaden, Beeinträc htigung zeitkritischer Aufgaben, drohende Eskalation oder betroffene VIP-Benutzer oder Gruppen
Mittel	Der Schaden nimmt im Laufe der Zeit zu oder es ist ein einzelner VIP-Benutzer oder eine Gruppe betroffen

Dringlichkeitsstufe	Beschreibung
Niedrig	Geringfügige Schadenszunahme im Laufe der Zeit oder nicht zeitkritische Arbeit beeinträc htigt

3. Erstellen einer Priorisierungsmatrix:
    - Verwenden Sie eine Matrix, um Auswirkungen und Dringlichkeit miteinander zu vergleichen, und weisen Sie verschiedenen Kombinationen Prioritätsstufen zu.
    - Machen Sie die Matrix allen Teammitgliedern, die für die Reaktion auf betriebliche Ereignisse verantwortlich sind, zugänglich und verständlich.
    - Die folgende Beispielmatrix zeigt den Schweregrad eines Vorfalls nach Dringlichkeit und Auswirkung an:

Dringlichkeit und Auswirkungen	Hoch	Mittel	Niedrig
Hoch	Kritisch	Dringend	Hoch
Mittel	Dringend	Hoch	Normal
Niedrig	Hoch	Normal	Niedrig

4. Trainieren und Kommunizieren: Schulen Sie die Response-Teams im Umgang mit der Prioritätenmatrix und der Wichtigkeit, diese während eines Ereignisses zu befolgen. Kommunizieren Sie den Priorisierungsprozess an alle Beteiligten, um klare Erwartungen zu schaffen.
5. Integration der Vorfallreaktion:
    - Integrieren Sie die Priorisierungsmatrix in Ihre Pläne und Tools zur Reaktion auf Vorfälle.
    - Automatisieren Sie nach Möglichkeit die Klassifizierung und Priorisierung von Ereignissen, um die Reaktionszeiten zu verkürzen.
    - Kunden von Enterprise Support können AWS-Vorfallerkennung und -reaktionverwenden, um die proaktive Überwachung und das Vorfallmanagement für Produktions-Workloads rund um die Uhr zu gewährleisten.

6. Überprüfen und Anpassen: Überprüfen Sie regelmäßig die Effektivität des Priorisierungsprozesses und nehmen Sie Anpassungen auf der Grundlage von Rückmeldungen und Änderungen im Geschäftsumfeld vor.

Ressourcen

Zugehörige bewährte Methoden:

- OPS03-BP03 Eskalation wird empfohlen
- OPS08-BP04 Erstellen umsetzbarer Warnmeldungen
- OPS09-BP01 Messen operativer Ziele und KPIs mit Metriken

Zugehörige Dokumente:

- Atlassian – Verständnis der Schweregrade von Vorfällen
- IT-Prozessplan – Checkliste der Vorfallpriorität

OPS10-BP04 Definieren von Eskalationspfaden

Legen Sie in Ihren Protokollen zur Vorfallreaktion klare Eskalationspfade fest, um rechtzeitige und effektive Maßnahmen zu ermöglichen. Dazu gehören die Festlegung von Aufforderungen zur Eskalation, die detaillierte Beschreibung des Eskalationsprozesses und die vorherige Genehmigung von Maßnahmen, um die Entscheidungsfindung zu beschleunigen und die durchschnittliche Zeit für die Behebung zu verkürzen.

Gewünschtes Ergebnis: Ein strukturierter und effizienter Prozess, der Vorfälle an das entsprechende Personal weiterleitet und so die Reaktionszeiten und Auswirkungen minimiert.

Typische Anti-Muster:

- Mangelnde Klarheit über die Wiederherstellungsverfahren führt zu provisorischen Maßnahmen bei kritischen Vorfällen.
- Das Fehlen von definierten Berechtigungen und Zuständigkeiten führt zu Verzögerungen, wenn dringende Maßnahmen erforderlich sind.
- Stakeholder und Kunden werden nicht erwartungsgemäß informiert.
- Wichtige Entscheidungen verzögern sich.

Vorteile der Nutzung dieser bewährten Methode:

- Optimierte Reaktion auf Vorfälle durch vordefinierte Eskalationsverfahren.
- Reduzierte Ausfallzeiten durch vorab genehmigte Maßnahmen und klare Zuständigkeiten.
- Verbesserte Ressourcenzuweisung und Anpassung der Support-Ebene an den Schweregrad des Vorfalls.
- Verbesserte Kommunikation mit Stakeholdern und Kunden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Richtig definierte Eskalationspfade sind entscheidend für eine schnelle Reaktion auf Vorfälle. AWS Systems Manager Incident Manager unterstützt die Einrichtung strukturierter Eskalations- und Bereitschaftspläne, die die richtigen Mitarbeiter alarmieren, damit sie bei Vorfällen handlungsbereit sind.

Implementierungsschritte

1. Einrichtung von Eskalationsaufforderungen: Richten Sie CloudWatch-Alarme ein, um einen Vorfall in AWS Systems Manager Incident Managerverwenden.
2. Erstellen von Bereitschaftsplänen: Erstellen Sie Bereitschaftspläne in Incident Manager, die mit Ihren Eskalationspfaden übereinstimmen. Statten Sie das Bereitschaftspersonal mit den erforderlichen Berechtigungen und Tools aus, um schnell handeln zu können.
3. Detaillierte Eskalationsverfahren:
   - Legen Sie bestimmte Bedingungen fest, unter denen ein Vorfall eskaliert werden sollte.
   - Erstellen Sie Eskalationspläne in Incident Manager.
   - Eskalationskanäle sollten aus einem Ansprechpartner oder einem Bereitschaftsplan bestehen.
   - Definieren Sie die Rollen und Verantwortlichkeiten des Teams auf jeder Eskalationsstufe.
4. Genehmigung von Schadensbegrenzungsmaßnahmen im Voraus: Arbeiten Sie mit Entscheidungsträgern zusammen, um Maßnahmen für erwartete Szenarien vorab zu genehmigen. Verwenden Sie Systems Manager-Automation-Runbooks, die mit Incident Manager integriert sind, um die Behebung von Vorfällen zu beschleunigen.
5. Angabe der Zuständigkeit: Identifizieren Sie eindeutig die internen Besitzer für jeden Schritt des Eskalationspfads.

6. Details zu Eskalationen mit Drittanbietern:
    - Dokumentieren Sie Service Level Agreements (SLAs) von Drittanbietern und richten Sie sie an internen Zielen aus.
    - Legen Sie klare Protokolle für die Lieferantenkommunikation bei Vorfällen fest.
    - Integrieren Sie Lieferantenkontakte in die Tools zum Vorfallmanagement, um direkten Zugriff zu erhalten.
    - Führen Sie regelmäßige Übungen durch, die Reaktionsszenarien von Drittanbietern beinhalten.
    - Sorgen Sie dafür, dass die Informationen zur Lieferanteneskalation gut dokumentiert und leicht zugänglich sind.
7. Trainieren und Testen von Eskalationsplänen: Schulen Sie Ihr Team im Eskalationsprozess und führen Sie regelmäßig Übungen zur Reaktion auf Vorfälle oder den Ernstfall durch. Kunden mit Enterprise Support können einen Workshop zum Vorfallmanagement anfordernverwenden.
8. Kontinuierliche Verbesserungen: Überprüfen Sie regelmäßig die Wirksamkeit Ihrer Eskalationspfade. Aktualisieren Sie Ihre Prozesse auf Grundlage der Erkenntnisse aus den Nachuntersuchungen von Vorfällen und dem kontinuierlichen Feedback.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS08-BP04 Erstellen umsetzbarer Warnmeldungen
- OPS10-BP02 Implementieren eines Prozesses für jede Warnmeldung
- OPS11-BP02 Durchführen von Analysen nach Vorfällen

Zugehörige Dokumente:

- AWS Systems Manager Incident Manager-Eskalationspläne
- Arbeiten mit Bereitschaftsplänen in Incident Manager
- Erstellen und Verwalten von Runbooks
- Temporäre erweiterte Zugriffsverwaltung mit AWS IAM Identity Center
- Atlassian – Eskalationsrichtlinien für effektives Vorfallmanagement

OPS10-BP05 Definieren eines Kundenkommunikationsplan für Ereignisse, die sich auf den Service auswirken

Eine effektive Kommunikation bei Ereignissen, die sich auf den Service auswirken, ist entscheidend, um das Vertrauen und die Transparenz gegenüber den Kunden aufrechtzuerhalten. Ein klar definierter Kommunikationsplan hilft Ihrem Unternehmen, bei Vorfällen schnell und klar Informationen sowohl intern als auch extern auszutauschen.

Gewünschtes Ergebnis:

- Ein robuster Kommunikationsplan, der Kunden und Interessengruppen bei Ereignissen, die sich auf den Service auswirken, effektiv informiert.
- Transparenz in der Kommunikation, um Vertrauen aufzubauen und Ängste der Kunden abzubauen.
- Minimierung der Auswirkungen von Ereignissen, die sich auf den Service in Bezug auf das Kundenerlebnis und den Geschäftsbetrieb auswirken.

Typische Anti-Muster:

- Eine unzureichende oder verzögerte Kommunikation führt zu Verwirrung und Unzufriedenheit der Kunden.
- Allzu technische oder vage Nachrichten vermitteln nicht die tatsächlichen Auswirkungen auf die Benutzer.
- Es gibt keine vordefinierte Kommunikationsstrategie, was zu inkonsistenten und reaktiven Nachrichten führt.

Vorteile der Nutzung dieser bewährten Methode:

- Mehr Vertrauen und Zufriedenheit bei den Kunden durch proaktive und klare Kommunikation.
- Entlastung der Support-Teams durch präventive Behandlung von Kundenanliegen.
- Verbesserte Fähigkeit, Vorfälle effektiv zu verwalten und zu bewältigen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Die Erstellung eines umfassenden Kommunikationsplans für Veranstaltungen, die sich auf den Service auswirken, umfasst mehrere Facetten, von der Auswahl der richtigen Kanäle bis hin zur Formulierung der Botschaft und des Tonfalls. Der Plan sollte anpassungsfähig und skalierbar sein und verschiedene Ausfallszenarien berücksichtigen.

Implementierungsschritte

1. Definieren von Rollen und Zuständigkeiten:
    - Beauftragen Sie einen Hauptzuständigen für die Vorfallreaktion mit der Überwachung der Maßnahmen.
    - Benennen Sie einen Kommunikationsmanager, der für die Koordination der gesamten externen und internen Kommunikation verantwortlich ist.
    - Beziehen Sie den Support-Manager ein, um eine konsistente Kommunikation über Support-Tickets zu gewährleisten.
2. Identifizieren von Kommunikationskanälen: Wählen Sie Kanäle wie Arbeitsplatz-Chat, E-Mail, SMS, soziale Medien, In-App-Benachrichtigungen und Statusseiten aus. Diese Kanäle sollten robust und in der Lage sein, bei Ereignissen, die den Service beeinträchtigen, unabhängig zu arbeiten.
3. Schnelle, klare und regelmäßige Kommunikation mit Kunden:
    - Entwickeln Sie Vorlagen für verschiedene Szenarien, bei denen Beeinträchtigungen des Serviceangebots vorliegen, und achten Sie dabei auf Einfachheit und wichtige Details. Fügen Sie Informationen über die Beeinträchtigung des Services, die erwartete Lösungszeit und die Auswirkungen hinzu.
    - Verwenden Sie Amazon Pinpoint, um Kunden mithilfe von Push-Benachrichtigungen, In-App-Benachrichtigungen, E-Mails, Textnachrichten, Sprachnachrichten und Nachrichten über benutzerdefinierte Kanäle zu informieren.
    - Verwenden Sie Amazon Simple Notification Service (Amazon SNS), um Subscriber programmgesteuert oder per E-Mail, mobilen Push-Benachrichtigungen und Textnachrichten zu benachrichtigen.
    - Kommunizieren Sie den Status über Dashboards, indem Sie ein Amazon CloudWatch-Dashboard öffentlich teilen.
    - Förderung des Engagements in den sozialen Medien:
        - Verfolgen Sie aktiv die sozialen Medien, um die Stimmung der Kunden zu verstehen.

    - Posten Sie auf Social-Media-Plattformen, um die Öffentlichkeit auf dem Laufenden zu halten und die Community einzubeziehen.
    - Bereiten Sie Vorlagen für eine konsistente und klare Kommunikation in den sozialen Medien vor.
4. Koordinieren Sie die interne Kommunikation: Implementieren Sie interne Protokolle mithilfe von Tools wie AWS Chatbot für die Teamkoordination und Kommunikation. Verwenden Sie CloudWatch-Dashboards, um den Status zu kommunizieren.
5. Organisation der Kommunikation mit speziellen Tools und Services:
    - Verwenden Sie AWS Systems Manager Incident Manager mit AWS Chatbot, um spezielle Chat-Kanäle für die interne Kommunikation und Koordination in Echtzeit bei Vorfällen einzurichten.
    - Verwenden Sie AWS Systems Manager Incident Manager-Runbooks, um Kundenbenachrichtigungen über Amazon Pinpoint, Amazon SNS oder Tools von Drittanbietern wie Social-Media-Plattformen bei Vorfällen zu automatisieren.
    - Integrieren Sie Genehmigungs-Workflows in Runbooks, um optional die gesamte externe Kommunikation vor dem Versand zu überprüfen und zu autorisieren.
6. Praktizieren und verbessern:
    - Führen Sie Trainingkurse zum Einsatz von Kommunikationsmitteln und -strategien durch. Ermöglichen Sie es Teams, bei Vorfällen rechtzeitig Entscheidungen zu treffen.
    - Testen Sie den Kommunikationsplan durch regelmäßige Übungen oder Ernstfallübungen. Mithilfe dieser Tests können Sie Ihre Botschaften präzisieren und die Effektivität der Kanäle bewerten.
    - Implementieren Sie Feedback-Mechanismen, um die Effektivität der Kommunikation bei Vorfällen zu bewerten. Entwickeln Sie den Kommunikationsplan auf Grundlage des Feedbacks und der sich ändernden Bedürfnisse kontinuierlich weiter.

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- OPS07-BP03 Verwenden von Runbooks zur Durchführung von Verfahren
- OPS10-BP06 Bekanntgeben des Status über Dashboards
- OPS11-BP02 Durchführen von Analysen nach Vorfällen

Zugehörige Dokumente:

- Atlassian – Bewährte Methoden der Kommunikation bei Vorfällen
- Atlassian – Verfassen eines guten Status-Updates
- PagerDuty – Leitfaden für die Kommunikation bei Vorfällen

Zugehörige Videos:

- Atlassian – Erstellung eines eigenen Kommunikationsplans für Vorfälle: Vorlagen für Zwischenfälle

Zugehörige Beispiele:

- AWS Health-Dashboard
- Beispiel für AWS-Status-Updates

OPS10-BP06 Bekanntgeben des Status über Dashboards

Verwenden Sie Dashboards als strategisches Werkzeug, um den Betriebsstatus und wichtige Metriken in Echtzeit an verschiedene Zielgruppen zu vermitteln, darunter interne technische Teams, Führungskräfte und Kunden. Diese Dashboards bieten eine zentrale, visuelle Darstellung des Systemzustands und der Geschäftsleistung und erhöhen so die Transparenz und die Effizienz der Entscheidungsfindung.

Gewünschtes Ergebnis:

- Ihre Dashboards bieten einen umfassenden Überblick über das System und die Geschäftskennzahlen, die für verschiedene Interessengruppen relevant sind.
- Stakeholder können proaktiv auf Betriebsinformationen zugreifen, sodass keine häufigen Statusanfragen mehr erforderlich sind.
- Die Entscheidungsfindung in Echtzeit wird während des normalen Betriebs und bei Vorfällen verbessert.

Typische Anti-Muster:

- Techniker, die an einem Vorfallmanagementgespräch teilnehmen, benötigen Statusaktualisierungen, um sich auf dem Laufenden zu halten.

- Sie verlassen sich auf die manuelle Berichterstattung für das Management, was zu Verzögerungen und möglichen Ungenauigkeiten führt.
- Die Arbeit der Operations-Teams wird bei Vorfällen häufig für Statusaktualisierungen unterbrochen.

Vorteile der Nutzung dieser bewährten Methode:

- Ermöglicht Stakeholdern den sofortigen Zugriff auf wichtige Informationen und fördert so fundierte Entscheidungen.
- Reduziert betriebliche Ineffizienzen, indem manuelle Berichte und häufige Statusabfragen minimiert werden.
- Erhöht die Transparenz und das Vertrauen durch Echtzeiteinblicke in die Systemleistung und Geschäftskennzahlen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Dashboards vermitteln effektiv den Status Ihrer Systeme und Geschäftskennzahlen und können auf die Bedürfnisse verschiedener Zielgruppen zugeschnitten werden. Mit Tools wie Amazon CloudWatch-Dashboards und Amazon QuickSight können Sie interaktive Echtzeit-Dashboards für die Systemüberwachung und Business Intelligence erstellen.

Implementierungsschritte

1. Ermittlung der Bedürfnisse der Stakeholder: Ermitteln Sie den spezifischen Informationsbedarf verschiedener Zielgruppen, z. B. technische Teams, Führungskräfte und Kunden.
2. Wählen der richtigen Tools: Wählen Sie geeignete Tools wie Amazon CloudWatch-Dashboards für die Systemüberwachung und Amazon QuickSight für interaktive Business Intelligence aus.
3. Entwicklung effektiver Dashboards:
    - Entwickeln Sie Dashboards, um relevante Metriken und KPIs übersichtlich darzustellen und sicherzustellen, dass sie verständlich und umsetzbar sind.
    - Integrieren Sie bei Bedarf Ansichten auf System- und Unternehmensebene.
    - Inkludieren Sie sowohl Dashboards auf hoher Ebene (für umfassende Übersichten) als auch auf niedriger Ebene (für detaillierte Analysen).
    - Integrieren Sie automatische Alarme in Dashboards, um kritische Probleme hervorzuheben.

- Kommentieren Sie Dashboards mit wichtigen Schwellenwerten und Zielen für sofortige Sichtbarkeit.

4. Integration von Datenquellen:
   - Verwenden Sie Amazon CloudWatch, um Metriken von verschiedenen AWS-Services zu aggregieren und anzuzeigen und Metriken aus anderen Datenquellen abzufragen.So erhalten Sie einen einheitlichen Überblick über den Zustand Ihres Systems und Ihre Geschäftsmetriken.
   - Nutzen Sie Features wie CloudWatch Logs Insights, um Protokolldaten aus verschiedenen Anwendungen und Services abzufragen und zu visualisieren.
5. Bereitstellung von Selfservice-Zugriff:
   - Teilen Sie CloudWatch-Dashboards mit relevanten Stakeholdern für den Selfservice-Zugriff auf Informationen mithilfe von Dashboard-Freigabe-Features.
   - Stellen Sie sicher, dass Dashboards leicht zugänglich sind und aktuelle Informationen in Echtzeit bereitstellen.
6. Regelmäßige Aktualisierungen und Verbesserungen:
   - Aktualisieren und verbessern Sie die Dashboards kontinuierlich, um sie an die sich entwickelnden Geschäftsanforderungen und das Feedback der Stakeholder anzupassen.
   - Überprüfen Sie die Dashboards regelmäßig, um sicherzustellen, dass sie relevant und effektiv sind, um die erforderlichen Informationen zu vermitteln.

Ressourcen

Zugehörige bewährte Methoden:

- OPS08-BP05 Erstellen von Dashboards

Zugehörige Dokumente:

- Erstellung von Dashboards für operative Sichtbarkeit
- Verwenden von Amazon CloudWatch-Dashboards
- Erstellen flexibler Dashboards mit Dashboard-Variablen
- Freigabe von CloudWatch-Dashboards
- Abfrage von Metriken aus anderen Datenquellen
- Hinzufügen eines benutzerdefinierten Widgets zu einem CloudWatch-Dashboard

Zugehörige Beispiele:

- Workshop zur Beobachtbarkeit – Dashboards

OPS10-BP07 Automatisieren von Reaktionen auf Ereignisse

Die Automatisierung von Reaktionen auf Ereignisse ist der Schlüssel für eine schnelle, konsistente und fehlerfreie operative Abwicklung. Erstellen Sie optimierte Prozesse und verwenden Sie Tools, um Ereignisse automatisch zu verwalten und darauf zu reagieren, um manuelle Eingriffe zu minimieren und die betriebliche Effizienz zu steigern.

Gewünschtes Ergebnis:

- weniger menschliche Fehler und schnellere Lösungszeiten durch Automatisierung
- konsistente und zuverlässige Handhabung betrieblicher Ereignisse
- verbesserte betriebliche Effizienz und Systemzuverlässigkeit

Typische Anti-Muster:

- manuelle Behandlung von Ereignissen führt zu Verzögerungen und Fehlern
- bei sich wiederholenden, kritischen Aufgaben wird die Automatisierung übersehen
- sich wiederholende, manuelle Aufgaben führen zu Ermüdungserscheinungen und zum Übersehen kritischer Probleme

Vorteile der Nutzung dieser bewährten Methode:

- beschleunigte Reaktionen auf Ereignisse, wodurch sich die Ausfallzeiten des Systems reduzieren
- zuverlässiger Betrieb mit automatisierter und konsistenter Ereignisbehandlung

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Integrieren Sie Automatisierung, um effiziente Arbeitsabläufe zu schaffen und manuelle Eingriffe zu minimieren.

Implementierungsschritte

1. Identifizieren von Möglichkeiten zur Automatisierung: Bestimmen Sie sich wiederholende Aufgaben für die Automatisierung, wie beispielsweise Problembehebung, Ticketverbesserung, Kapazitätsmanagement, Skalierung, Bereitstellung und Tests.
2. Identifizieren von Automatisierungsaufforderungen:
   - Bewerten und definieren Sie bestimmte Bedingungen oder Metriken, die automatische Reaktionen mithilfe von Amazon CloudWatch-Alarmaktionenauslösen.
   - Verwendung von Amazon EventBridge, um auf Ereignisse in AWS-Services, benutzerdefinierten Workloads und SaaS-Anwendungen zu reagieren.
   - Denken Sie an Initiationsereignisse wie bestimmte Protokolleinträge, Schwellenwerte für Leistungsmetrikenoder Zustandsänderungen in AWS-Ressourcen.
3. Implementieren der ereignisgesteuerten Automatisierung:
   - Verwenden Sie AWS Systems Manager-Automation-Runbooks, um die Wartung, Bereitstellung und Problembehebung zu vereinfachen.
   - Beim Erstellen von Vorfällen in Incident Manager werden automatisch Details zu den betroffenen AWS-Ressourcen erfasst und dem Vorfall hinzugefügt.
   - Überwachen Sie Quoten proaktiv mit Quota Monitor für AWS.
   - Passen Sie die Kapazität mit AWS Auto Scaling automatisch an, um Verfügbarkeit und Leistung aufrechtzuerhalten.
   - Automatisieren Sie Entwicklungspipelines mit Amazon CodeCatalyst.
   - Führen Sie Smoke Tests durch oder überwachen Sie Endpunkte und APIs kontinuierlich mit synthetischer Überwachung.
4. Schadensbegrenzung durch Automatisierung:
   - Implementieren Sie automatisierte Sicherheitsmaßnahmen, um schnell auf Risiken zu reagieren.
   - Verwenden Sie AWS Systems Manager State Manager, um Konfigurationsabweichungen zu reduzieren.
   - Korrigieren Sie nicht konforme Ressourcen mit AWS-Config-Regeln.

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- OPS08-BP04 Erstellen umsetzbarer Warnmeldungen
- OPS10-BP02 Implementieren eines Prozesses für jede Warnmeldung

Zugehörige Dokumente:

- Verwendung von Systems-Manager-Automation-Runbooks mit Incident Manager
- Erstellen von Vorfällen in Incident Manager
- AWS Service Quotas
- Überwachen der Ressourcennutzung und Senden von Benachrichtigungen, wenn das Kontingent fast erreicht ist
- AWS Auto Scaling
- Was ist Amazon CodeCatalyst?
- Verwenden von Amazon CloudWatch-Alarmen
- Verwenden von Amazon CloudWatch-Alarmaktionen
- Korrigieren von nicht konformen AWS-Config-Regeln-Ressourcen
- Erstellen von Metriken aus Protokollereignissen mit Filtern
- AWS Systems Manager State Manager

Zugehörige Videos:

- Erstellen von Automation-Runbooks mit AWS Systems Manager
- Automatisierung von IT-Abläufen in AWS
- Automatisierungsregeln für AWS Security Hub
- Amazon CodeCatalyst-Vorlagen sorgen für einen schnellen Start Ihres Softwareprojekts

Zugehörige Beispiele:

- Amazon CodeCatalyst-Tutorial: Erstellen eines Projekts mit der dreistufigen Vorlage für moderne Webanwendungen
- Workshop zur Beobachtbarkeit
- Reaktion auf Vorfälle mit Incident Manager

Weiterentwicklung

Weiterentwicklung bedeutet eine ständige Verbesserung im Laufe der Zeit. Implementieren Sie häufige kleine inkrementelle Änderungen basierend auf den aus Ihren Betriebsaktivitäten gewonnenen Erfahrungen.

Um Ihre Vorgänge im Laufe der Zeit weiterentwickeln zu können, müssen Sie Folgendes tun:

Themen

Lernen, Teilen und Verbessern

Es ist wichtig, dass Sie regelmäßig Zeiten einplanen, um betriebliche Aktivitäten und Fehler zu analysieren, zu experimentieren und Verbesserungen vorzunehmen. Wenn etwas schief läuft, soll Ihr Team und Ihr ganzes technisches Umfeld daraus lernen. Analysieren Sie Fehler, um daraus etwas zu lernen und entsprechende Verbesserungen zu planen. Gehen Sie Ihre Erkenntnisse mit anderen Teams durch, um sie zu überprüfen.

Bewährte Methoden

OPS11-BP01 Implementieren eines Prozesses für die kontinuierliche Verbesserung

Bewerten Sie Ihren Workload mithilfe bewährter Methoden für interne und externe Architekturen. Führen Sie häufige, bewusste Workload-Überprüfungen durch. Räumen Sie Verbesserungsmöglichkeiten in Ihrem Softwareentwicklungsplan Priorität ein.

Gewünschtes Ergebnis:

- Sie analysieren Ihren Workload mindestens einmal im Jahr anhand bewährter Methoden für die Architektur.
- Sie räumen den Features in Ihrem Softwareentwicklungsprozess die gleiche Priorität wie Verbesserungsmöglichkeiten ein.

Typische Anti-Muster:

- Sie haben seit der Bereitstellung Ihres Workloads vor einigen Jahren keine Architekturüberprüfung durchgeführt.
- Verbesserungsmöglichkeiten haben geringere Priorität. Im Vergleich zu neuen Features bleiben diese Möglichkeiten im Backlog.
- In der Organisation gibt keinen Standard für die Umsetzung von Änderungen an bewährten Methoden.

Vorteile der Nutzung dieser bewährten Methode:

- Ihr Workload wird durch bewährte Methoden für die Architektur auf dem aktuellen Stand gehalten.
- Sie entwickeln Ihren Workload gezielt weiter.
- Sie können die bewährten Methoden der Organisation nutzen, um alle Workloads zu verbessern.
- Sie erzielen marginale Gewinne, deren kumulative Wirkung jedoch zu einer höheren Effizienz führen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Führen Sie regelmäßig eine Überprüfung der Architektur Ihres Workloads durch. Bewerten Sie anhand interner und externer bewährter Methoden Ihren Workload und ermitteln Sie Verbesserungsmöglichkeiten. Räumen Sie Verbesserungsmöglichkeiten in Ihrem Softwareentwicklungsplan Priorität ein.

Implementierungsschritte

1. Führen Sie in vereinbarten Intervallen Überprüfungen der Architektur Ihrer Produktionsworkloads durch. Verwenden Sie einen dokumentierten Architekturstandard mit AWS-spezifischen bewährten Methoden.
   a. Verwenden Sie Ihre intern definierten Standards für diese Bewertungen. Wenn Sie nicht über einen internen Standard verfügen, verwenden Sie das AWS Well-Architected Framework.
   b. Verwenden Sie AWS Well-Architected Tool, um einen Fokusbereich Ihrer internen bewährten Methoden zu erstellen und Ihre Architekturprüfung durchzuführen.
   c. Wenden Sie sich an Ihren AWS Solution Architect oder Technical Account Manager, um einen geführten Well-Architected Framework Review Ihres Workload durchzuführen.
2. Räumen Sie den während der Überprüfung ermittelten Verbesserungsmöglichkeiten in Ihrem Softwareentwicklungsprozess Priorität ein.

Aufwand des Implementierungsplans: niedrig Sie können das AWS Well-Architected Framework zur Durchführung Ihrer jährlichen Architekturprüfung verwenden.

Ressourcen

Zugehörige bewährte Methoden:

- OPS11-BP02 Durchführen von Analysen nach Vorfällen
- OPS11-BP08 Dokumentieren und Weitergeben von Erkenntnissen
- OPS04 Implementieren von Beobachtbarkeit

Zugehörige Dokumente:

- AWS Well-Architected Tool – Fokusbereiche
- AWS Well-Architected Whitepaper – Die Überprüfung

- Anpassen von Well-Architected-Prüfungen mit Fokusbereichen und dem AWS Well-Architected Tool
- Implementieren des AWS Well-Architected-Fokusbereich-Lebenszyklus in Ihre Organisation

Zugehörige Videos:

- Well-Architected Labs – Stufe 100: Fokusbereiche auf AWS Well-Architected Tool
- AWS re:Invent 2023 – Skalierung bewährter Methoden von AWS Well-Architected in Ihrer Organisation

Zugehörige Beispiele:

- AWS Well-Architected Tool

OPS11-BP02 Durchführen von Analysen nach Vorfällen

Überprüfen Sie die Ereignisse mit Auswirkungen auf Kunden und bestimmen Sie die beitragenden Faktoren und Präventivmaßnahmen. Entwickeln Sie anhand dieser Informationen Abhilfemaßnahmen, um Wiederholungen einzuschränken oder zu verhindern. Entwickeln Sie Verfahren für schnelle und effektive Reaktionen. Informieren Sie nach Bedarf auf zielgruppengerechte Weise über beitragende Faktoren und Korrekturmaßnahmen.

Gewünschtes Ergebnis:

- Sie haben Prozesse für das Vorfallmanagement eingerichtet, die auch Analysen nach dem Vorfall beinhalten.
- Sie verfügen über Pläne zur Beobachtbarkeit, um Daten über Ereignisse zu sammeln.
- Anhand dieser Daten können Sie Metriken verstehen und erfassen, die Sie bei der Analyse nach einem Vorfall unterstützen.
- Sie lernen aus Vorfällen, um zukünftige Ergebnisse zu verbessern.

Typische Anti-Muster:

- Sie verwalten einen Anwendungsserver. Ungefähr alle 23 Stunden und 55 Minuten werden alle Ihre aktiven Sitzungen beendet. Sie haben versucht, festzustellen, wo der Fehler auf Ihrem Anwendungsserver liegt. Sie vermuten, dass es sich um ein Netzwerkproblem handeln könnte, das

Netzwerkteam zeigt sich jedoch unkooperativ, da es für Ihr Anliegen zu beschäftigt ist. Sie haben keinen vordefinierten Prozess, den Sie befolgen könnten, um Support zu erhalten und die nötigen Informationen zu sammeln, um dem Problem auf den Grund zu gehen.

- Bei Ihrem Workload kam es zu Datenverlust. Dies ist das erste Mal, dass dieses Problem aufgetreten ist, und die Ursache ist nicht klar. Sie entscheiden, dass es nicht wichtig ist, da Sie die Daten wiederherstellen können. Datenverluste beginnen mit größerer Häufigkeit aufzutreten und wirken sich auf Ihre Kunden aus. Dadurch steigt auch der betriebliche Aufwand, wenn Sie die fehlenden Daten wiederherstellen.

Vorteile der Nutzung dieser bewährten Methode:

- Durch vordefinierte Prozesse zur Bestimmung der Komponenten, Bedingungen, Maßnahmen und Ereignisse, die zu einem Vorfall beigetragen haben, können Sie Verbesserungsmöglichkeiten ermitteln.
- Sie können Daten aus der Analyse nach einem Vorfall nutzen, um Verbesserungen vorzunehmen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Verwenden Sie einen Prozess zur Ermittlung der Faktoren, die dazu beitragen. Überprüfen Sie alle Vorfälle, die sich auf Kunden auswirken. Erarbeiten Sie ein Verfahren, um die beitragenden Faktoren eines Vorfalls zu ermitteln und zu dokumentieren. Damit können Sie Abhilfemaßnahmen entwickeln, um ein erneutes Auftreten einzudämmen oder gänzlich zu verhindern, und Verfahren für eine rasche und wirksame Reaktion erstellen. Informieren Sie gegebenenfalls über die Ursachen von Vorfällen und passen Sie die Kommunikation an Ihre Zielgruppe an. Teilen Sie Ihre Erkenntnisse offen innerhalb Ihrer Organisation mit.

Implementierungsschritte

1. Erfassen Sie Metriken wie Bereitstellungsänderungen, Konfigurationsänderungen, Startzeit des Vorfalls, Zeitpunkt des Alarms, Zeitpunkt des Einsatzes, Startzeit der Schadensbegrenzung und Zeitpunkt der Behebung des Vorfalls.
2. Beschreiben Sie wichtige Zeitpunkte auf der Zeitleiste, um die Ereignisse des Vorfalls zu verstehen.
3. Stellen Sie die folgenden Fragen:
   a. Könnten Sie die Zeit bis zur Erkennung verkürzen?

   b. Gibt es Aktualisierungen von Metriken und Alarmen, durch die der Vorfall früher erkannt würde?
   c. Können Sie die Zeit bis zur Diagnose verkürzen?
   d. Gibt es Aktualisierungen Ihrer Reaktions- oder Eskalationspläne, mit denen die richtigen Notfallteams früher eingeschaltet werden könnten?
   e. Können Sie die Zeit bis zur Schadensbegrenzung verkürzen?
   f. Gibt es Runbook- oder Playbook-Schritte, die Sie hinzufügen oder verbessern könnten?
   g. Können Sie zukünftige Vorfälle verhindern?
4. Erstellen Sie Checklisten und Aktionen. Verfolgen und führen Sie alle Aktionen durch.

Aufwand für den Implementierungsplan: mittel

Ressourcen

Zugehörige bewährte Methoden:

- OPS11-BP01 Implementieren eines Prozesses für die kontinuierliche Verbesserung
- OPS 4 – Implementieren von Beobachtbarkeit

Zugehörige Dokumente:

- Durchführen einer Analyse nach einem Vorfall im Incident Manager
- Überprüfung der Einsatzbereitschaft

OPS11-BP03 Implementieren von Feedbackschleifen

Feedbackschleifen bieten umsetzbare Einblicke zur Unterstützung der Entscheidungsfindung. Integrieren Sie Feedbackschleifen in Ihre Verfahren und Workloads. Damit können Sie Probleme und Bereiche identifizieren, für die Verbesserungen erforderlich sind. Diese validieren auch Investitionen für Verbesserungen. Diese Feedbackschleifen sind die Grundlage für die kontinuierliche Verbesserung Ihres Workloads.

Feedbackschleifen können in zwei Kategorien unterteilt werden: Sofortiges Feedback und nachträgliche Analyse. Sofortiges Feedback wird durch Prüfung der Leistung und der Ergebnisse betrieblicher Aktivitäten eingeholt. Dieses Feedback kommt von Teammitgliedern, Kunden oder der automatisierten Ausgabe der Aktivität. Sofortiges Feedback kommt von Dingen wie A/B-Tests und

der Auslieferung neuer Funktionen und ist für das „Schnell scheitern“-Konzept von entscheidender Bedeutung.

Nachträgliche Analysen werden regelmäßig durchgeführt, um Feedback aus der Überprüfung betrieblicher Ergebnisse und Metriken in der Vergangenheit zu erhalten. Dies geschieht am Ende einer Phase, in regelmäßigem Rhythmus oder nach größeren Releases oder Veranstaltungen. Diese Art von Feedbackschleife validiert Investitionen in Betriebsabläufe oder Ihren Workload. Dies hilft Ihnen beim Messen des Erfolgs und bei der Validierung Ihrer Strategie.

Gewünschtes Ergebnis: Sie nutzen sofortiges Feedback und nachträgliche Analysen für weitere Verbesserungen. Es gibt einen Mechanismus zur Erfassung des Feedbacks von Benutzern und Teammitgliedern. Nachträgliche Analysen identifizieren Trends, die Verbesserungen unterstützen können.

Typische Anti-Muster:

- Sie starten einige Funktionen, haben aber keine Möglichkeit, Feedback von den Kunden dazu zu erhalten.
- Nach einer Investition in verbesserte Betriebsabläufe führen Sie keine nachträgliche Analyse für deren Validierung durch.
- Sie holen das Feedback von Kunden ein, überprüfen dies jedoch nicht regelmäßig.
- Feedbackschleifen führen zu vorgeschlagenen Maßnahmen, werden jedoch nicht in den Softwareentwicklungsprozess einbezogen.
- Kunden erhalten kein Feedback zu Verbesserungen, die sie vorgeschlagen haben.

Vorteile der Nutzung dieser bewährten Methode:

- Sie können vom Kunden aus rückwärts arbeiten, um neue Funktionen zu unterstützen.
- Ihre Organisationskultur kann schneller auf Änderungen reagieren.
- Trends dienen zur Identifizierung von Verbesserungsmöglichkeiten.
- Nachträgliche Analysen validieren in Ihre Workloads und Betriebsabläufe getätigte Investitionen.

Risikostufe, wenn diese bewährte Methode nicht genutzt wird: Hoch

Implementierungsleitfaden

Die Implementierung dieser bewährten Methode bedeutet, dass Sie sofortiges Feedback und nachträgliche Analysen verwenden. Diese Feedbackschleifen erleichtern Verbesserungen. Es gibt zahlreiche Mechanismen für sofortiges Feedback, z. B. Umfragen, Kundenbefragungen oder Feedbackformulare. Ihre Organisation nutzt nachträgliche Analysen auch, um Möglichkeiten für Verbesserungen zu identifizieren und Initiativen zu validieren.

Kundenbeispiel

AnyCompany Retail hat ein Webformular erstellt, über das Kunden Feedback abgeben oder Probleme melden können. Bei der wöchentlichen Scrum-Sitzung evaluiert das Softwareentwicklungsteam das Benutzerfeedback. Das Feedback wird regelmäßig genutzt, um die Weiterentwicklung der Plattform zu steuern. Am Ende jeder Etappe wird eine nachträgliche Analyse durchgeführt, um Punkte zu identifizieren, bei denen Verbesserungsbedarf besteht.

Implementierungsschritte

1. Sofortiges Feedback
   - Sie benötigen einen Mechanismus für den Erhalt von Feedback von Kunden und Teammitgliedern. Ihre betrieblichen Aktivitäten können auch so konfiguriert werden, dass Sie automatisiertes Feedback erhalten.
   - Ihre Organisation benötigt einen Prozess zur Prüfung dieses Feedbacks, zum Feststellen der Verbesserungsbereiche und zur Planung der Verbesserungen.
   - Das Feedback muss in Ihren Softwareentwicklungsprozess integriert werden.
   - Wenn Sie Verbesserungen durchführen, informieren Sie die Personen, die dazu Feedback gegeben haben.
     - Sie können AWS Systems Manager OpsCenter verwenden, um diese Verbesserungen als OpsItems nachzuverfolgen.
2. Nachträgliche Analyse
   - Führen Sie nachträgliche Analysen am Ende eines Entwicklungszyklus, in regelmäßigen Abständen oder nach einem größeren Release durch.
   - Laden Sie an dem Workload beteiligte Personen zu einer Nachbesprechung ein.
   - Erstellen Sie auf einem Whiteboard oder in einem Spreadsheet drei Spalten: Beenden, Starten und Beibehalten.
     - Beenden gilt für alles, mit dem Ihr Team aufhören soll.

    - Starten gilt für Ideen, die ab sofort umgesetzt werden sollen.
    - Beibehalten gilt für Elemente, die weiterhin durchgeführt werden sollen.
- Holen Sie das Feedback aller anwesenden beteiligten Personen ein.
- Priorisieren Sie das Feedback. Weisen Sie allen „Starten“- oder „Beibehalten“-Elementen Aktionen und Beteiligte zu.
- Fügen Sie die Aktionen Ihrem Softwareentwicklungsprozess hinzu und halten Sie die Beteiligten bei Ihren Verbesserungen über den Status auf dem Laufenden.

Aufwand für den Implementierungsplan: Mittel. Zur Implementierung dieser bewährten Methode benötigen Sie ein Verfahren zum Einholen und zur Analyse sofortigen Feedbacks. Dazu müssen Sie auch einen Prozess für die nachträgliche Analyse einrichten.

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP01 Kundenbedürfnisse bewerten: Feedbackschleifen sind ein Mechanismus zum Ermitteln der Anforderungen externer Kunden.
- OPS01-BP02 Bedürfnisse interner Kunden bewerten: Interne Beteiligte können Feedbackschleifen nutzen, um Bedürfnisse und Anforderungen zu kommunizieren.
- OPS11-BP02 Durchführen von Analysen nach Vorfällen: Analysen nach einem Vorfall sind eine wichtige Form nachträglicher Analyse nach Vorfällen.
- OPS11-BP07 Prüfung von Betriebsmetriken: Durch die Prüfung betrieblicher Metriken können Sie Trends und Bereiche für Verbesserungen identifizieren.

Zugehörige Dokumente:

- 7 Fehler, die Sie bei der Einrichtung eines CCOE vermeiden sollten
- Atlassian Team Playbook - Retrospectives
- E-Mail-Definitionen: Feedbackschleifen
- Einrichten von Feedbackschleifen mit der AWS Well-Architected Framework Review
- IBM Garage Methodology – Nachträgliche Analysen
- Investopedia – The PDCS Cycle
- Maximizing Developer Effectiveness von Tim Cochran

- Operations Readiness Reviews (ORR) Whitepaper - Iteration
- TIL CSI - Continual Service Improvement
- Toyota und E-Commerce: Lean bei Amazon

Zugehörige Videos:

- Building Effective Customer Feedback Loops (Aufbau effektiver Kundenfeedbackschleifen)

Zugehörige Beispiele:

- Astuto - Open-Source-Tool für Kundenfeedback
- AWS-Lösungen – QnABot auf AWS
- Fider – Eine Plattform zur Organisation von Kundenfeedback

Zugehörige Services:

- AWS Systems Manager OpsCenter

OPS11-BP04 Wissensmanagement

Das Wissensmanagement hilft den Teammitgliedern, die Informationen zu finden, die sie für ihre Arbeit benötigen. In lernenden Organisationen werden Informationen frei geteilt, was jedem Einzelnen die nötigen Kompetenzen eröffnet. Die Informationen können entdeckt oder durchsucht werden. Die Informationen sind korrekt und auf dem neuesten Stand. Es gibt Mechanismen, um neue Informationen zu erstellen, bestehende Informationen zu aktualisieren und veraltete Informationen zu archivieren. Das gängigste Beispiel für eine Wissensmanagement-Plattform ist ein Content-Management-System wie ein Wiki.

Gewünschtes Ergebnis:

- Teammitglieder haben Zugriff auf zeitnahe, präzise Informationen.
- Die Informationen sind durchsuchbar.
- Es gibt Mechanismen zum Hinzufügen, Aktualisieren und Archivieren von Informationen.

Typische Anti-Muster:

- Es gibt keinen zentralen Wissensspeicher. Die Teammitglieder verwalten ihre eigenen Notizen auf ihren lokalen Rechnern.
- Sie haben ein selbst gehostetes Wiki, aber keine Mechanismen zum Verwalten von Informationen, was dazu führt, dass die Informationen veraltet sind.
- Jemand stellt fest, dass Informationen fehlen, aber es gibt keinen Prozess, um das Hinzufügen dieser Informationen zum Team-Wiki anzustoßen. Er fügt sie selbst hinzu, aber versäumt einen wichtigen Schritt, was zu einem Ausfall führt.

Vorteile der Nutzung dieser bewährten Methode:

- Die Teammitglieder werden gestärkt, weil Informationen frei geteilt werden.
- Neue Teammitglieder werden schneller eingearbeitet, weil die Dokumentation aktuell und durchsuchbar ist.
- Die Informationen sind zeitnah, präzise und umsetzbar.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Das Wissensmanagement ist eine wichtige Facette von lernenden Organisationen. Zunächst benötigen Sie ein zentrales Repository, in dem Sie Ihr Wissen speichern (z. B. ein selbst gehostetes Wiki). Sie müssen Prozesse entwickeln, um Wissen hinzuzufügen, zu aktualisieren und zu archivieren. Entwickeln Sie Standards für das, was dokumentiert werden soll, und lassen Sie alle Beteiligten dazu beitragen.

Kundenbeispiel

AnyCompany Retail hostet ein internes Wiki, in dem das gesamte Wissen gespeichert wird. Die Teammitglieder werden ermutigt, die Wissensdatenbank im Rahmen ihrer täglichen Arbeit zu ergänzen. Ein funktionsübergreifendes Team bewertet vierteljährlich, welche Seiten am wenigsten aktualisiert werden, und entscheidet, ob sie archiviert oder aktualisiert werden sollen.

Implementierungsschritte

1. Beginnen Sie damit, das Content-Management-System zu bestimmen, in dem das Wissen gespeichert werden soll. Holen Sie die Zustimmung der Stakeholder in Ihrer Organisation ein.
   a. Wenn Sie kein vorhandenes Content-Management-System haben, können Sie ein selbst gehostetes Wiki oder ein Versionsverwaltungssystem als Ausgangspunkt verwenden.

2. Entwickeln Sie Runbooks für das Hinzufügen, Aktualisieren und Archivieren von Informationen. Informieren Sie Ihr Team über diese Prozesse.
3. Bestimmen Sie, welches Wissen im Content-Management-System gespeichert werden soll. Beginnen Sie mit den täglichen Aktivitäten (Runbooks und Playbooks), die die Teammitglieder ausführen. Arbeiten Sie mit Stakeholdern zusammen, um Prioritäten für das hinzuzufügende Wissen festzulegen.
4. Arbeiten Sie in regelmäßigen Abständen mit Stakeholdern zusammen, um veraltete Informationen zu identifizieren und sie zu archivieren oder auf den neuesten Stand zu bringen.

Grad des Aufwands für den Implementierungsplan: mittel. Wenn Sie kein vorhandenes Content-Management-System haben, können Sie ein selbst gehostetes Wiki oder ein Dokumenten-Repository mit Versionsverwaltung einrichten.

Ressourcen

Zugehörige bewährte Methoden:

- OPS11-BP08 Dokumentieren und Weitergeben von Erkenntnissen - Das Wissensmanagement erleichtert den Austausch von Informationen über gewonnene Erkenntnisse.

Zugehörige Dokumente:

- Atlassian – Wissensmanagement

Zugehörige Beispiele:

- DokuWiki
- Gollum
- MediaWiki
- Wiki.js

OPS11-BP05 Definieren von Verbesserungsfaktoren

Identifizieren Sie Verbesserungsmöglichkeiten, damit Sie Chancen basierend auf Daten und Feedback-Schleifen bewerten und priorisieren können. Erkunden Sie Verbesserungsmöglichkeiten in Ihren Systemen und Prozessen und automatisieren Sie bei Bedarf.

Gewünschtes Ergebnis:

- Sie verfolgen Daten aus Ihrer gesamten Umgebung.
- Sie korrelieren Ereignisse und Aktivitäten mit Geschäftsergebnissen.
- Sie können Umgebungen und Systeme vergleichen und gegenüberstellen.
- Sie führen einen detaillierten Aktivitätsverlauf Ihrer Bereitstellungen und Ergebnisse.
- Sie sammeln Daten, um Ihren Sicherheitsstatus zu stärken.

Typische Anti-Muster:

- Sie sammeln Daten aus Ihrer gesamten Umgebung, korrelieren jedoch keine Ereignisse und Aktivitäten.
- Sie sammeln detaillierte Daten aus Ihrem gesamten Bestand, was die Aktivität und Kosten von AWS CloudTrail und Amazon CloudWatch in die Höhe treibt. Sie ziehen jedoch keinen sinnvollen Nutzen aus diesen Daten.
- Bei der Definition von Verbesserungsfaktoren berücksichtigen Sie nicht die Geschäftsergebnisse.
- Sie messen nicht die Auswirkungen neuer Features.

Vorteile der Nutzung dieser bewährten Methode:

- Sie minimieren die Auswirkungen ereignisbasierter Motivationen oder emotionaler Investitionen, indem Sie Verbesserungskriterien festlegen.
- Sie reagieren auf alle, nicht nur technische Geschäftsereignisse.
- Sie messen Ihre Umgebung, um Verbesserungsbereiche zu identifizieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

- Kenntnis der Verbesserungsfaktoren: Sie sollten ein System nur dann ändern, wenn das gewünschte Ergebnis auch unterstützt wird.
  - Gewünschte Fähigkeiten: Prüfen Sie bei der Bewertung von Verbesserungsmöglichkeiten die gewünschten Features und Fähigkeiten.
    - Neuerungen bei AWS

- Nicht akzeptable Probleme: Prüfen Sie bei der Bewertung von Verbesserungsmöglichkeiten nicht akzeptable Probleme, Fehler und Schwachstellen. Informieren Sie sich über Dimensionierungsoptionen und suchen Sie nach Optimierungsmöglichkeiten.
  - Aktuelle AWS-Sicherheitsmitteilungen
  - AWS Trusted Advisor
  - Cloud Intelligence Dashboards
- Compliance-Anforderungen: Prüfen Sie bei der Bewertung von Verbesserungsmöglichkeiten, welche Updates und Änderungen erforderlich sind, um Vorschriften bzw. Richtlinien einzuhalten oder weiterhin den Support eines Drittanbieters nutzen zu können.
  - AWS-Compliance
  - AWS-Compliance-Programme
  - Aktuelle Neuigkeiten zur AWS-Compliance

Ressourcen

Zugehörige bewährte Methoden:

- OPS01 Organisationsprioritäten
- OPS02 Beziehungen und Eigentümerschaft
- OPS04-BP01 Ermitteln wichtiger Key Performance Indicators
- OPS08 Nutzung der Workload-Beobachtbarkeit
- OPS09 Grundlegendes zum betrieblichen Status
- OPS11-BP03 Implementieren von Feedback-Schleifen

Zugehörige Dokumente:

- Amazon Athena
- Amazon QuickSight
- AWS-Compliance
- Aktuelle Neuigkeiten zur AWS-Compliance
- AWS-Compliance-Programme
- AWS Glue
- Aktuelle AWS-Sicherheitsmitteilungen

- AWS Trusted Advisor
- Exportieren Ihrer Protokolldaten zu Amazon S3
- Neuerungen bei AWS
- Die Anforderungen bei kundenorientierter Innovation
- Digitale Transformation: Hype oder strategische Notwendigkeit?

Zugehörige Videos:

- AWS re:Invent 2023 – Verbessern der betrieblichen Effizienz und Belastbarkeit mit AWS Support (SUP310)

OPS11-BP06 Prüfen von Erkenntnissen

Überprüfen Sie Ihre Analyseergebnisse und Reaktionen mit fachbereichsübergreifenden Teams und Geschäftsverantwortlichen. Schaffen Sie mithilfe dieser Prüfungen ein allgemeines Verständnis, ermitteln Sie weitere Auswirkungen und legen Sie einen Maßnahmenkatalog fest. Passen Sie die Reaktionen bei Bedarf an.

Gewünschte Ergebnisse:

- Sie überprüfen regelmäßig Erkenntnisse mit Geschäftsbereichsleitern. Geschäftsbereichsleiter liefern zusätzlichen Kontext zu neu gewonnenen Erkenntnissen.
- Sie überprüfen Erkenntnisse und bitten um Feedback von Fachkollegen, und Sie teilen Ihre Erkenntnisse mit allen Teams.
- Sie veröffentlichen Daten und Erkenntnisse, die andere technische und Geschäftsteams überprüfen können. Sie entwickeln aus Ihren Erkenntnisse neue Methoden für andere Abteilungen.
- Sie fassen neue Erkenntnisse zusammen und besprechen sie mit Führungskräften. Führungskräfte nutzen neue Erkenntnisse, um die Strategie zu definieren.

Typische Anti-Muster:

- Sie veröffentlichen ein neues Feature. Dieses Feature verändert das Verhalten einiger Ihrer Kunden. Ihre Beobachtbarkeit berücksichtigt diese Änderungen nicht. Sie quantifizieren die Vorteile dieser Änderungen nicht.

- Sie veröffentlichen ein neues Update und vernachlässigen die Aktualisierung Ihres CDN. Der CDN-Cache ist nicht mehr mit der aktuellen Version kompatibel. Sie messen den Prozentsatz der Anforderungen mit Fehlern. Alle Ihre Benutzer melden HTTP 400-Fehler bei der Kommunikation mit Backend-Servern. Sie untersuchen die Kundenfehler und stellen fest, dass Sie die Zeit verschwendet haben, weil Sie die falsche Dimension gemessen haben.
- Ihr Service Level Agreement sieht eine Verfügbarkeit von 99,9 % vor, und Ihr Wiederherstellungszeitpunkt liegt bei vier Stunden. Der Servicebesitzer behauptet, dass das System keine Ausfallzeiten hat. Sie implementieren eine teure und komplexe Replikationslösung, die Zeit und Geld verschwendet.

Vorteile der Nutzung dieser bewährten Methode:

- Durch die Prüfung von Erkenntnissen zusammen mit Geschäftsinhabern und Fachexperten bauen Sie ein gemeinsames Verständnis auf und sorgen effektiver für Verbesserungen.
- Sie entdecken verborgene Probleme und berücksichtigen sie bei zukünftigen Entscheidungen.
- Ihr Fokus verlagert sich von technischen Ergebnissen hin zu Geschäftsergebnissen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

- Prüfen von Erkenntnissen: Wenden Sie sich an die Geschäftsinhaber und Fachexperten, um sicherzustellen, dass die Bedeutung der von Ihnen gesammelten Daten allgemein verstanden und vereinbart ist. Ermitteln Sie zusätzliche Bedenken, potenzielle Auswirkungen und bestimmen Sie eine Vorgehensweise.

Ressourcen

Zugehörige bewährte Methoden:

- OPS01-BP06 Bewerten von Kompromissen und Abwägen der Vorteile und Risiken
- OPS02-BP06 Zuständigkeiten zwischen Teams werden vordefiniert oder ausgehandelt
- OPS11-BP03 Implementieren von Feedback-Schleifen

Zugehörige Dokumente:

- Planung eines Cloud-Kompetenzzentrums (CCOE)

Zugehörige Videos:

- Aufbau von Beobachtbarkeit zur Erhöhung der Resilienz

OPS11-BP07 Prüfung von Betriebsmetriken

Führen Sie regelmäßig teamübergreifend mit Teilnehmern aus verschiedenen Unternehmensbereichen nachträgliche Analysen der operationsspezifischen Metriken durch. Ermitteln Sie mithilfe dieser Prüfungen Verbesserungspotenziale sowie mögliche Maßnahmen und teilen Sie diese Erkenntnisse auch anderen mit. Berücksichtigen Sie bei Ihrer Suche nach Verbesserungsmöglichkeiten all Ihre Umgebungen (z. B. Entwicklungs-, Test- und Produktionsumgebung).

Gewünschtes Ergebnis:

- Sie überprüfen häufig Metriken, die sich auf das Geschäft auswirken.
- Sie erkennen und überprüfen Anomalien mithilfe Ihrer Beobachtbarkeitsfunktionen.
- Sie verwenden Daten, um die Erreichung von Geschäftsergebnissen und Zielen zu unterstützen.

Typische Anti-Muster:

- Ihr Wartungsfenster unterbricht eine wichtige Verkaufsaktion. Das Unternehmen weiß weiterhin nicht, dass es ein Standard-Wartungsfenster gibt, das verzögert werden könnte, wenn sich andere wichtige Ereignisse auf das Geschäft auswirken.
- Sie hatten einen längeren Ausfall, weil in Ihrer Organisation häufig eine veraltete Bibliothek verwendet wird. Inzwischen sind Sie zu einer unterstützten Bibliothek migriert. Die anderen Teams in Ihrer Organisation wissen nicht, dass diese Gefahr besteht.
- Sie überprüfen nicht regelmäßig die Einhaltung der Kunden-SLAs. Sie laufen Gefahr, die mit Kunden vereinbarten SLAs nicht zu erfüllen. Es drohen Geldstrafen bei der Nichteinhaltung von mit Kunden vereinbarten SLAs.

Vorteile der Nutzung dieser bewährten Methode:

- Indem Sie sich regelmäßig treffen, um Betriebsmetriken, Ereignisse und Vorfälle zu überprüfen, sorgen Sie für ein gemeinsames Verständnis aller Teams.
- Ihr Team trifft sich regelmäßig, um Metriken und Vorfälle zu überprüfen und auf diese Weise Maßnahmen gegen Risiken zu ergreifen und Kunden-SLAs zu erkennen.
- Sie teilen Ihre gewonnenen Erkenntnisse, die Daten zur Priorisierung und zur gezielten Verbesserung der Geschäftsergebnisse liefern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

- Führen Sie regelmäßig teamübergreifend mit Teilnehmern aus verschiedenen Unternehmensbereichen nachträgliche Analysen der operationsspezifischen Metriken durch.
- Binden Sie alle Stakeholder, einschließlich der Teams aus den Bereichen Betriebswirtschaft, Entwicklung und Operationen, ein, indem Sie Ihre Erkenntnisse aus dem sofortigen Feedback und der nachträglichen Analyse und gewonnene Erkenntnisse austauschen.
- Machen Sie sich deren Erkenntnisse zunutze, um Verbesserungspotenziale und mögliche Maßnahmen ausfindig zu machen.

Ressourcen

Zugehörige bewährte Methoden:

- OPS08-BP05 Erstellen von Dashboards
- OPS09-BP03 Überprüfen der Betriebsmetriken und Priorisieren von Verbesserungen
- OPS10-BP01 Verwenden eines Prozesses für die Bewältigung von Ereignissen, Vorfällen und Problemen

Zugehörige Dokumente:

- Amazon CloudWatch
- Referenzinformationen zu Metriken und Dimensionen von Amazon CloudWatch
- Veröffentlichen von benutzerdefinierten Metriken
- Verwendung von Amazon CloudWatch-Metriken
- Dashboards und Visualisierungen mit CloudWatch

OPS11-BP08 Dokumentieren und Weitergeben von Erkenntnissen

Dokumentieren Sie die Erkenntnisse aus den betrieblichen Aktivitäten und geben Sie diese weiter, damit Sie sie sowohl intern als auch teamübergreifend nutzen können. Die Erkenntnisse Ihres Teams sollten Sie an andere in Ihrer Organisation weitergeben, damit alle davon profitieren. Teilen Sie Informationen und Ressourcen, um vermeidbare Fehler zu verhindern und Entwicklungsbemühungen zu unterstützen, und konzentrieren Sie sich auf die Bereitstellung der angestrebten Features.

Definieren Sie mithilfe von AWS Identity and Access Management (IAM) Berechtigungen, die den gesteuerten Zugriff auf die Ressourcen ermöglichen, die Sie innerhalb von Konten und kontenübergreifend freigeben möchten.

Gewünschtes Ergebnis:

- Anschließend sollten Sie versionsgesteuerte Repositories verwenden, um Anwendungsbibliotheken, skriptbasierte Verfahren, Verfahrens- und andere Systemdokumentationen freizugeben.
- Sie teilen Ihre Infrastrukturstandards als versionskontrollierte AWS CloudFormation-Vorlagen.
- Sie überprüfen die Erkenntnisse, die Sie teamübergreifend gelernt haben.

Typische Anti-Muster:

- Sie erlitten einen längeren Ausfall, weil Ihre Organisation häufig eine fehlerhafte Bibliothek verwendet. Seitdem sind Sie zu einer zuverlässigen Bibliothek migriert. Die anderen Teams in Ihrer Organisation wissen nicht, dass diese Gefahr besteht. Niemand dokumentiert und teilt die Erfahrung mit dieser Bibliothek, und sie sind sich des Risikos nicht bewusst.
- Sie haben einen Grenzfall in einem intern gemeinsam genutzten Microservice ermittelt, der dazu führt, dass Sitzungen unterbrochen werden. Sie rufen den Service jetzt anders auf, um diesen Grenzfall zu vermeiden. Die anderen Teams in Ihrer Organisation wissen nicht, dass diese Gefahr besteht.
- Sie haben eine Möglichkeit gefunden, die Anforderungen an die CPU-Auslastung eines Ihrer Microservices deutlich zu reduzieren. Sie wissen nicht, ob andere Teams auch von diesem Verfahren profitieren könnten.

Vorteile der Etablierung dieser bewährten Methode: Teilen Sie Ihre Erfahrungen mit, um Verbesserungen zu unterstützen und den Nutzen aus Erfahrungen zu maximieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

- Dokumentieren und Weitergeben von Erkenntnissen: Implementieren Sie Verfahren zur Dokumentation der aus der Durchführung von betrieblichen Aktivitäten und nachträglichen Analysen gewonnenen Erkenntnisse, damit auch andere Teams davon profitieren.
- Weitergeben von Erkenntnissen: Nutzen Sie Verfahren für den teamübergreifenden Austausch gewonnener Erkenntnisse und zugehöriger Artefakte. Veröffentlichen Sie beispielsweise aktualisierte Verfahren, Richtlinien, Governance und bewährte Methoden in einem allgemein zugänglichen Wiki. Teilen Sie Skripte, Code und Bibliotheken über ein gemeinsames Repository.
  - Delegieren des Zugriffs auf Ihre AWS-Umgebung
  - Freigeben eines AWS CodeCommit-Repositorys

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP06 Zuständigkeiten zwischen Teams werden vordefiniert oder ausgehandelt
- OPS05-BP01 Verwendung einer Versionskontrolle
- OPS05-BP06 Gemeinsame Design-Standards
- OPS11-BP03 Implementieren von Feedback-Schleifen
- OPS11-BP07 Prüfung von Betriebsmetriken

Zugehörige Dokumente:

- Reduzieren Sie Projektverzögerungen mit einer Docs-as-Code-Lösung

Zugehörige Videos:

- Delegieren des Zugriffs auf Ihre AWS-Umgebung
- Wie AWS Support Sie unterstützt | Vorstellung der Tabletop-Übungen zum Vorfallmanagement

OPS11-BP09 Einplanen von Zeit für Verbesserungen

Reservieren Sie Zeit und Ressourcen innerhalb Ihrer Prozesse, um kontinuierliche, schrittweise Verbesserungen zu ermöglichen.

Gewünschtes Ergebnis:

- Sie können temporäre Duplikate von Umgebungen erstellen. Das senkt die Risiken, den Aufwand und Kosten, die mit dem Experimentieren und Testen verbunden sind.
- Diese duplizierten Umgebungen können Sie nutzen, um die aus Ihren Analysen gezogenen Rückschlüsse zu testen, Verbesserungen zu entwickeln und geplante Verbesserungen zu testen.
- Sie führen GameDays durch und verwenden Fault Injection Service (FIS), um die Kontrollen und den Integritätsschutz bereitzustellen, die Teams benötigen, um Experimente in einer produktionsähnlichen Umgebung durchzuführen.

Typische Anti-Muster:

- Es besteht ein bekanntes Leistungsproblem auf Ihrem Anwendungsserver. Es wird im Backlog hinter jeder geplanten Feature-Implementierung priorisiert. Bleibt die Rate der hinzugefügten geplanten Features konstant, wird das Leistungsproblem niemals behoben.
- Genehmigen Sie den Administratoren und Entwicklern, dass sie ihre Überstunden zur Auswahl und Implementierung von Verbesserungen nutzen können, um kontinuierliche Verbesserungen zu unterstützen. Es werden niemals Verbesserungen vorgenommen.
- Die Betriebsabnahme ist abgeschlossen, und Sie testen die betrieblichen Praktiken nicht erneut.

Vorteile der Nutzung dieser bewährten Methoden: Indem Sie Zeit und Ressourcen in Ihre Prozesse investieren, ermöglichen Sie kontinuierliche, schrittweise Verbesserungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

- Einplanen von Zeit für Verbesserungen: Reservieren Sie Zeit und Ressourcen innerhalb Ihrer Prozesse, um kontinuierliche, schrittweise Verbesserungen zu ermöglichen.
- Implementieren Sie Änderungen, die zu Verbesserungen führen sollen, und beurteilen Sie deren Ergebnisse.

- Versuchen Sie alternative Vorgehensweisen, wenn die Ergebnisse die Ziele nicht erfüllen und die Verbesserung immer noch Priorität hat.
- Simulieren Sie Produktionsworkloads durch GameDays, und nutzen Sie die Erkenntnisse aus diesen Simulationen, um sich zu verbessern.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP08 Verwenden mehrerer Umgebungen

Zugehörige Videos:

- AWSre:Invent 2023 – Verbessern Sie die Resilienz Ihrer Anwendungen mit AWS Fault Injection Service

Fazit

Operative Exzellenz ist ein fortlaufender und iterativer Prozess.

Richten Sie Ihr Unternehmen für Erfolg ein, indem Sie gemeinsame Ziele haben. Stellen Sie sicher, dass alle ihre Rolle beim Erreichen von Geschäftsergebnissen verstehen und wie sie sich auf die Fähigkeit anderer zum Erfolg auswirken. Stellen Sie Ihren Teammitgliedern Support bereit, damit sie Ihre Geschäftsergebnisse unterstützen können.

Betrachten Sie jeden betrieblichen Vorfall oder Ausfall als eine Gelegenheit, den Betrieb Ihrer Architektur zu verbessern. Durch das Verständnis der Anforderungen Ihrer Workloads, das Vordefinieren von Runbooks für Routineaktivitäten und Playbooks zur Behebung von Problemen, die Verwendung der betrieblichen Vorgänge als Codefunktionen in AWS und das Aufrechterhalten des Situationsbewusstseins sind Ihre Vorgänge besser vorbereitet und Sie können bei Vorfällen effektiver reagieren.

Achten Sie darauf, schrittweise Verbesserungen auf der Grundlage von sich ändernden Prioritäten vorzunehmen, ziehen Sie aus jedem Ereignis entsprechende Erkenntnisse und führen Sie nachträgliche Analysen durch. So steigern Sie die Effizienz und Effektivität Ihrer Aktivitäten und stellen dadurch den Erfolg Ihres Unternehmens sicher.

AWS soll Ihnen helfen, Architekturen zu errichten und zu betreiben, die die Effizienz maximieren, während Sie Bereitstellungen erstellen, die schnell und anpassungsfähig sind. Damit Ihre Workloads operative Exzellenz erreichen, sollten Sie die bewährten Methoden anwenden, die in diesem Dokument aufgeführt sind.

Mitwirkende

- Rich Boyd, Operational Excellence Pillar Lead, Well-Architected, Amazon Web Services
- Jon Steele, Solutions Architect Well-Architected, Amazon Web Services
- Ryan King, Sr. Technical Program Manager, Amazon Web Services
- Chris Kunselman, Advisory Consultant, Amazon Web Services
- Peter Mullen, Advisory Consultant, Amazon Web Services
- Brian Quinn, Sr. Advisory Consultant, Amazon Web Services
- David Stanley, Cloud Operating Model Lead, Amazon Web Services
- Chris Kozlowski, Senior Specialist Technical Account Manager, Enterprise Support, Amazon Web Services
- Alex Livingstone, Principal Specialist Solutions Architect, Cloud Operations, Amazon Web Services
- Paul Moran, Principal Technologist, Enterprise Support, Amazon Web Services
- Peter Mullen, Advisory Consultant, Professional Services, Amazon Web Services
- Chris Pates, Senior Specialist Technical Account Manager, Enterprise Support, Amazon Web Services
- Arvind Raghunathan, Principal Specialist Technical Account Manager, Enterprise Support, Amazon Web Services
- Ben Mergen, Senior Cost Lead Solutions Architect, Amazon Web Services

Weitere Informationen

Weitere Orientierungshilfe finden Sie in den folgenden Quellen:

- AWS Well-Architected Framework
- AWS-Architekturzentrum

Dokumentversionen

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Änderung	Beschreibung	Datum
Leitfäden zu bewährten Methoden aktualisiert	Bewährte Methoden wurden mit neuen Leitfäden für die Säule aktualisiert.	June 27, 2024
Umfangreiche Aktualisierung und Konsolidierung der Inhalte	Die Inhalte wurden aktualisiert und in mehrere Best-Practice-Bereiche zusammengefasst. Zwei Best-Practice-Bereiche (OPS 04 und OPS 08) wurden neu verfasst und mit neuen Inhalten und Schwerpunkten versehen. Die Best-Practices wurden aktualisiert und in folgende Bereiche zusammeng efasst: Design für den Betrieb, Bereitstellungsris iken abschwächenund Grundlegendes zum betriebli chen Status. Der Best-Prac tice-Bereich OPS 04 wurde geändert in Implementieren von Beobachtbarkeit. Der Best-Practice-Bereich OPS 08 wurde geändert in Nutzung der Workload-Beobachtbarkeit.	October 3, 2023
Updates für das neue Framework	Bewährte Methoden mit verbindlichen Anleitungen	April 10, 2023

	aktualisiert und neue bewährte Methoden hinzugefügt.	
Whitepaper aktualisiert	Bewährte Methoden mit neuen Implementierungsanleitungen aktualisiert.	December 15, 2022
Whitepaper aktualisiert	Weitere bewährte Methoden und Verbesserungspläne hinzugefügt.	October 20, 2022
Kleineres Update	Es wurde eine kleine redaktion elle Aktualisierung vorgenomm en.	August 8, 2022
Whitepaper aktualisiert	Aktualisierungen bezüglich neuer AWS-Services und -Funktionen sowie die neuesten bewährten Methoden.	February 2, 2022
Kleineres Update	Säule „Nachhaltigkeit“ wurde zur Einführung hinzugefügt.	December 2, 2021
Updates für das neue Framework	Aktualisierungen bezüglich neuer AWS-Services und -Funktionen sowie die neuesten bewährten Methoden.	July 8, 2020
Whitepaper aktualisiert	Aktualisierungen bezüglich neuer AWS-Services und -Funktionen sowie aktualisierte Verweise.	July 1, 2018
Erstveröffentlichung	Säule „Operative Exzellenz “ – AWS-Well-Architected-Framework veröffentlicht.	November 1, 2017