Migration von F5 BIG-IP zu F5 BIG-IP VE in der Cloud AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Migration von F5 BIG-IP zu F5 BIG-IP VE in der Cloud AWS

Table of Contents

Migration von F5 BIG-IP zu F5 BIG-IP VE in der Cloud AWS

Suresh Veragoni, Amazon Web Services ()AWS

November 2020 (Verlauf der Dokumente)

Dieses Handbuch bietet einen Überblick über die Schritte, die Architektur, die Tools und die Überlegungen zur Migration der F5 BIG-IP-Sicherheits- und Verkehrsmanagementlösungen zur Amazon Web Services () Cloud.AWSF5 BIG-IP ist eine Produktsammlung, die auf Verfügbarkeits-, Zugriffskontroll- und Sicherheitslösungen ausgerichtet ist. Sie laufen auf dem F5 Traffic Management Operating System (TMOS).

Ihre F5 BIG-IP-Sicherheits- und Verkehrsmanagementlösungen werden mithilfe der Rehost- und Replattform-Migrationsstrategien aus den sieben gängigen Migrationsstrategien (7 Rs) in die AWS Cloud migriert. Der F5-Workload wird migriert, indem eine bestehende Umgebung neu gehostet und Aspekte der Plattformumstellung wie Serviceerkennung und API-Integrationen genutzt werden.

In diesem Leitfaden werden die vier wichtigsten Schritte für Ihre Migration beschrieben.

- Bewertung der Migrationskosten und Fähigkeiten— Machen Sie sich mit den Kosten der Migration vertraut und erfahren Sie, welche Kenntnisse über die Produkte und Services von AWS F5 erforderlich sind.
- Abbildung der Anwendungen und Entwurf der Architektur— beurteilen Sie, wie Ihre Anwendungen zusammenpassen, und entwerfen Sie die Architektur für ihre future Umgebung.
- Planung der Migration — Verwenden Sie einen umfassenden Plan für Ihre Migration und treffen Sie wichtige Entscheidungen darüber, was migriert werden soll.
- Daten migrieren— stellen Sie die verfügbaren Konfigurationen für die Migration von F5 BIG-IP-Workloads in die AWS Cloud bereit und migrieren Sie Ihre Daten.

Einen vollständigen Überblick über die Migrationsschritte finden Sie im Muster Migrieren eines F5 BIG-IP-Workloads zu F5 BIG-IP VE in der Cloud auf der Prescriptive Guidance-Website. AWS AWS

Dieser Leitfaden richtet sich an Teams aus den Bereichen Technik und Architektur, die Sicherheits- und Verkehrsmanagementlösungen von F5 in die Cloud migrieren. AWS

Gezielte Geschäftsergebnisse

Organizations entscheiden sich für die Migration in die AWS Cloud, um ihre Agilität und Widerstandsfähigkeit zu erhöhen. Diese Migration hat erhebliche Vorteile, birgt aber auch Risiken, die reduziert werden müssen. Insbesondere das Risiko und die Komplexität der Cloud-Einführung nehmen zu, wenn wichtige Anwendungsdienste wie Verkehrsmanagement oder Sicherheit aufgeteilt werden.

Wenn Sie F5 BIG-IP-Workloads in die AWS Cloud migrieren, können Sie sich auf Agilität konzentrieren und hochwertige Betriebsmodelle für Ihre gesamte Unternehmensarchitektur einführen. Sie werden sich auch positiv auf Ihre Cloud-Einführung auswirken, da Ihre Technologieumgebungen gebündelt werden können.

Sie können sich auch einen Geschäftsvorteil verschaffen, indem Sie die Vielzahl von Anbietern oder Tools einschränken. Dies reduziert das Risiko bei der Migration einer Anwendung, da dadurch Änderungen am Datenpfad, an den Funktionen, Tools und am Betriebsmodell in Ihrer Quellumgebung eingeschränkt oder entfernt werden.

Bewertung der Migrationskosten und Fähigkeiten

Bevor Sie sich entscheiden, Ihre F5 BIG-IP-Sicherheits- und Verkehrsmanagementlösungen in die AWS Cloud zu migrieren, müssen Sie die Kosten der Migration abschätzen und abschätzen, welche Fähigkeiten erforderlich sind.

Die folgenden Abschnitte bieten eine Zusammenfassung der potenziellen Migrationskosten sowie einen Überblick über das Wissen über die Produkte AWS und Services von F5, die Ihr Team benötigen wird.

Themen

Bewertung der Lizenz- und Instanzkosten

Die Kosten für die Ausführung von F5 BIG-IP-Workloads in der AWS Cloud hängen von Ihren kombinierten Lizenz- und Instanzkosten ab. Wenn Sie zur AWS Cloud migrieren, müssen Sie Ihre vorhandenen Lizenzen anpassen und Funktionen von Ihrem Quellsystem zum Zielsystem aktivieren.

Für F5-Produkte gibt es mehrere Lizenzmodelle, aber Ihre geschäftlichen und technischen Anforderungen überschneiden sich in der Regel mit den folgenden Modellen: Bring Your Own License (BYOL), Marketplace, private Angebote, Abonnement und Enterprise License Agreements (ELA).

Die Migrationskosten hängen auch davon ab pay-as-you-go, ob Sie Instances mit jährlichem Preis nutzen oder ob Sie eine individuelle Vereinbarung mit Ihnen abgeschlossen haben. AWS Wichtig ist, dass sich die Kosten für eine F5-Lizenz auch je nach Modell und Ihren individuellen Anforderungen ändern können.

Sie können den AWS Preisrechner verwenden, um Ihre potenziellen Betriebskosten abzuschätzen. Die folgenden drei Beispiele geben Aufschluss über die Kosten von AWS Instanzen und Infrastruktur.

- F5 BIG-IP klein — 100 Mbit/s
- F5 BIG-IP Medium — 200 Mbit/s
- F5 BIG-IP groß — 800 Mbit/s

Evaluierung AWS und F5-Wissensdatenbank

Bevor Sie mit der Migration Ihres F5 BIG-IP-Workloads beginnen, sollten Sie sicherstellen, dass Ihr Team über Kenntnisse der folgenden Produkte AWS und Dienstleistungen von F5 verfügt.

AWS Produkte und Dienstleistungen

- AWS CloudFormationhilft Ihnen dabei, AWS Infrastrukturbereitstellungen vorhersehbar und wiederholt zu erstellen und bereitzustellen.
- Amazon CloudWatch bietet eine zuverlässige, skalierbare und flexible Überwachungslösung, die Sie innerhalb weniger Minuten einsetzen können.
- Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der skalierbare Rechenkapazität bietet, damit Sie Ihre Softwaresysteme erstellen und hosten können.
- AWS Identity and Access Management (IAM) ist ein Webservice zur sicheren Steuerung des Zugriffs auf Dienste. AWS
- AWS Landing Zone ist eine Lösung, mit der Kunden schnell eine sichere AWS Umgebung mit mehreren Konten einrichten können, die auf AWS bewährten Verfahren basiert.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Token Service (AWS STS) hilft Ihnen dabei, temporäre Anmeldeinformationen mit eingeschränkten Rechten für Benutzer anzufordern.
- AWS Transit Gatewayist ein hochverfügbarer und skalierbarer Service zur Konsolidierung der Amazon VPC-Routing-Konfiguration für eine AWS-Region hub-and-spoke WIT-Architektur.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen.

> **Important**
>
> Ihr Team sollte die verschiedenen Möglichkeiten kennen, eine oder mehrere virtuelle private Clouds (VPCs) mit vorhandenen Rechenzentren zu verbinden, und auch wissen, wie Sie Ressourcen in Ihrer AWS Infrastruktur erstellen können. Weitere Informationen dazu finden Sie unter Network-to-Amazon VPC-Konnektivitätsoptionen in der Amazon VPC-Dokumentation.

Produkte und Dienstleistungen von F5

- Das Traffic Management Operating System (F5 TMOS) ist die Softwarebasis für alle Netzwerk- oder Verkehrsprodukte von F5.
- Local Traffic Manager (F5 LTM) hilft Ihnen bei der Steuerung des Netzwerkverkehrs und bei der Auswahl des richtigen Ziels auf der Grundlage von Serverleistung, Sicherheit und Verfügbarkeit.
- Global Traffic Manager (F5 GTM) verteilt DNS- und Benutzeranwendungsanfragen auf der Grundlage von Geschäftsrichtlinien, Rechenzentrums- und Cloud-Servicebedingungen, Benutzerstandort und Anwendungsleistung.
- Access Policy Manager (F5 APM) sichert, vereinfacht und zentralisiert den Zugriff auf Apps und Daten, unabhängig davon APIs, wo sich Benutzer und ihre Apps befinden.
- Application Security Manager (F5 ASM) ist eine flexible Webanwendungs-Firewall, die Webanwendungen in herkömmlichen, virtuellen und privaten Cloud-Umgebungen schützt.
- Advanced Firewall Manager (F5 AFM) mindert Netzwerkbedrohungen, bevor sie kritische Rechenzentrumsressourcen stören.
- F5 BIG-IQ bietet einen zentralen Kontrollpunkt für physische und virtuelle Geräte von F5 sowie für die darauf laufenden Lösungen.

Abbildung der Anwendungen und Entwurf der Architektur

In den folgenden Abschnitten erfahren Sie, wie Ihre Anwendungen in ihre bestehende Umgebung passen und wie Sie ihre neue Architektur entwerfen können.

Themen

Zuordnung der Anwendungen

Es gibt keinen Standardansatz, wenn Sie Anwendungen und die damit verbundenen Abhängigkeiten in die AWS Cloud migrieren. Die folgende Tabelle bietet einen Überblick über die wichtigsten Überlegungen zu verschiedenen Anwendungen, die häufig mit F5 BIG-IP-Workloads in die Cloud migriert werden. AWS

Anwendungstyp	Anwendungsfall	Vorgeschlagene Aktion
Maßgeschneiderte oder kommerzielle (COT) Anwendungen off-the-shelf	Sie planen entweder, ein Rechenzentrum oder eine Colocation-Instanz zu schließen, nachdem Sie Anwendungen in die AWS Cloud migriert haben, oder Sie möchten eine Mischung aus lokalen Systemen und AWS Produkten oder Diensten ausführen. Sie haben nicht vor, diese Anwendungen zu modernisieren. Möglicherweise haben Sie den F5 Application Delivery Controller (ADC) als Teil der Anwendungslogik integriert und verlangt, dass er dieselbe	Überprüfen Sie die aktuellen F5-Konfigurationen und unterteilen Sie sie in die Anwendungskomponenten, die migriert werden müssen. Stellen Sie sicher, dass Sie dem verwendeten Lizenzmod ell entsprechen, entweder über die Module oder über das F5-Programm Good, Better, Best (GBB).

Anwendungstyp	Anwendungsfall	Vorgeschlagene Aktion
	Logik in die Cloud portieren muss. AWS Die Anwendungskomponenten können gleichzeitig migriert werden oder auch nicht.	
Anwendungen mit hohen Compliance- oder Sicherheitsanforderungen	Diese Anwendungen können zwar neu gehostet, auf eine neue Plattform gebracht oder neu gestaltet werden, erfordern jedoch erweiterte Schutzmaßnahmen. Diese erweiterten Schutzmaßnahmen können Verhaltensschutz, Sicherheit mobiler Apps, erweiterte Bot-Erkennung, umfassende IP-Intelligenz und Ausgangsfilterung von Antwortdaten umfassen.	Wenn Sie F5 ASM bereits verwenden, stellen Sie sicher, dass Sie die Sicherheits- oder Compliance-Richtlinie migrieren. Wenn es sich um eine neue Anwendung handelt, sollten Sie prüfen, wie Sie F5 ASM oder F5 Web Application Firewall (F5 WAF) am besten nutzen können.
Cloud-native Anwendungen der nächsten Generation, die auf Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) oder Amazon Hosting K8S gehostet werden EC2	Diese Anwendungen erfordern eine Protokolloptimierung, z. B. mobile oder andere verlustbehaftete Netzwerktypen, HTTP-Optimierungen, programmierbare Datenebene (iRules) oder erweiterte Dienste, die die Algorithmen für den Lastenausgleich aufeinander abstimmen.	Informationen zum Container-Ingress finden Sie in der F5-Dokumentation unter F5 Container Ingress Services.

Anwendungstyp	Anwendungsfall	Vorgeschlagene Aktion
Verbundener Namespace oder Hybridanwendungen	Dabei handelt es sich um Anwendungen, bei denen die Bereitstellung der Präsentat ionsebene in einer hybriden Bereitstellung gebündelt ist oder bei denen sich die genutzten Dienste in einer hybriden Bereitstellung befinden. Sie könnten beispielsweise F5 GTM zusammen mit F5 LTM vor Ort verwenden und die erweiterten Funktionen von F5 GTM genutzt haben, um komplexe Abhängigk eiten und eine erweiterte Logik darüber abzubilden, an welchen Standort Kunden geschickt werden sollen.	Diese Bereitstellung sollte über mindestens zwei F5-DNS-Systeme oder F5 Distributed Cloud DNS verfügen. Für die Bereitstellung müssen eines oder mehrere VPCs in der AWS Cloud erstellt werden. Eine VPC muss dem System als Rechenzentrum zugeordne t werden. Dies können mehrere sein, VPCs wenn Sie ein Transit-VPC-Design verwenden.

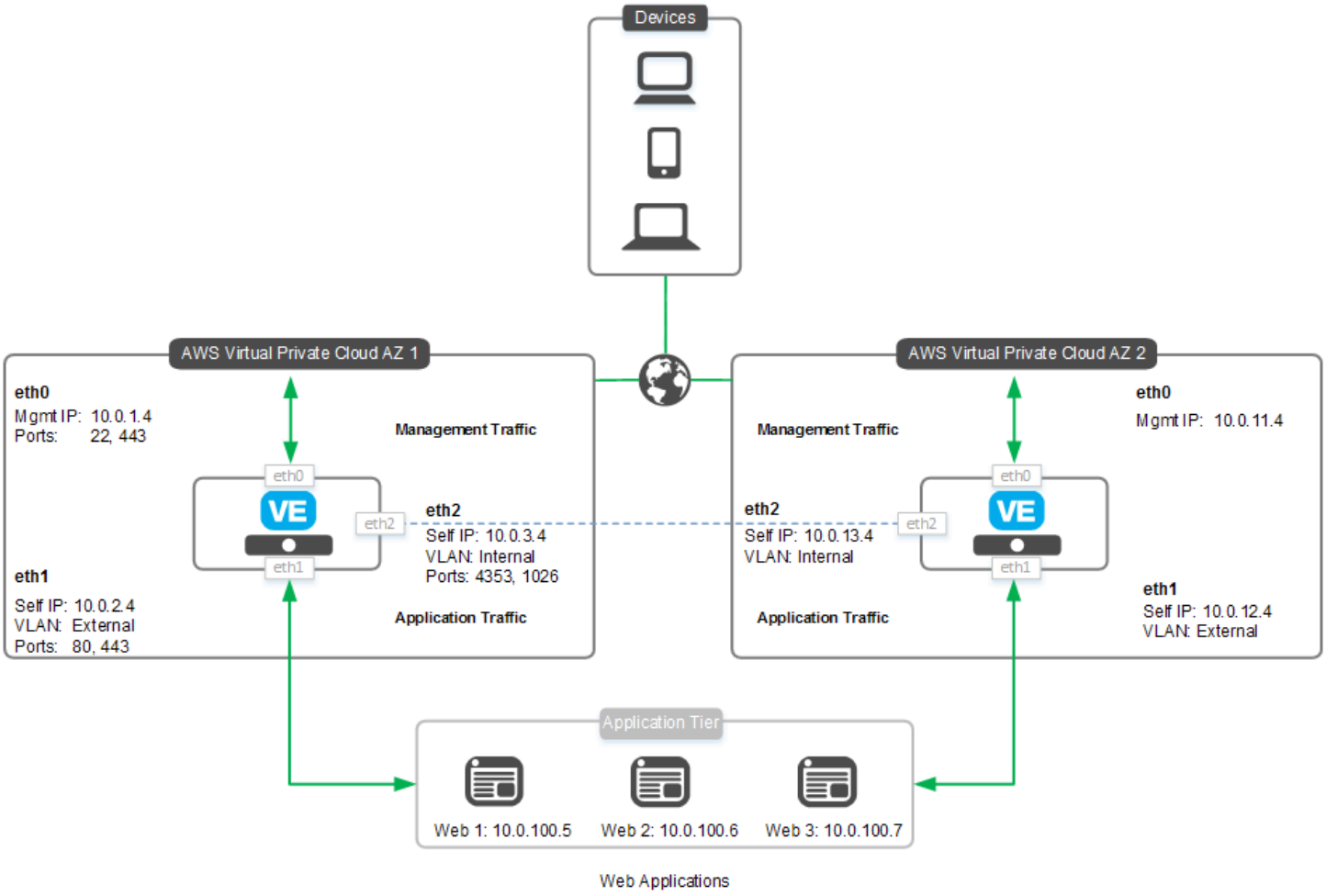
Anwendungstyp	Anwendungsfall	Vorgeschlagene Aktion
Leistungsoptimierte Anwendungen	Anwendungen, für die möglicherweise hochgradig optimierte Profile auf Sitzungs- (L4) und Anwendung sebene (L7) gelten, mobile Anwendungen oder Anwendungen, bei denen es aufgrund der Migration zur und aus der Cloud um erhöhte Latenz, HTTP-Optimierungen (SPDY) und Komprimierung geht. AWS	Dies erfordert die Bereitste llung des F5-LTM-Systems, auf dem virtuelle Standards erver (vollständiger TTCP-Proxy) oder höher (Anwendun gsproxy wie HTTP) ausgeführ t werden, wobei der Datenverk ehr zwischen den Anwendung sservern und den Kunden symmetrisch ist. Der Datenverkehr kann durch eine Source Network Address Translation (SNAT) verarbeitet werden, oder die F5 BIG-IP-In stances können das Standard-Gateway für die Instanz und die Routentabelle sein.
Interne Anwendung in mehreren Availability Zones, Hochverfügbarkeit (HA), aber kein DNS	Sie müssen eine Anwendung bereitstellen und möchten zonenübergreifende Unterstüt zung für eine höhere Verfügbarkeit anbieten, möchten aber kein DNS verwenden und können die IP-Adresse nicht ändern.	Sie müssen Kunden-Ga teways in der VPC verwenden , die mit einem Virtual Private Gateway verbunden sind, um den Alien-Adressraum anzukündigen. Außerdem müssen Sie die F5 Advanced HA iApp-Vorlage verwenden , um die Routentabelle zu bearbeiten. F5-Systeme können die Kunden-Gateways in der VPC sein, oder eine Drittanbieter-Lösung kann das Kunden-Gateway sein.

Anwendungstyp	Anwendungsfall	Vorgeschlagene Aktion
WAF- oder IDS/IPS-Anwendungen	Diese Anwendungen erfordern erweiterte Sicherheitsfunktionen wie SNORT-Signaturen, Bot-Schutz, umfangreiche und komplexe WAF-Regelsätze (über 2900 Signaturen) und die Integration von Sicherheitsscannern.	Wählen Sie eine AWS CloudFormation Vorlagentopologie, die den Anforderungen der Anwendung entspricht (Hochverfügbarkeit AWS Auto Scaling, Standalone), und erstellen und validieren Sie dann die entsprechende Sicherheitsrichtlinie.
Sicherheit und Dienste übertragen VPC-Anwendungen	Dies ist eine Variante einer Transit-VPC, in der Sie die Sicherheit und die Dienste für das Internet oder Intranet zentralisieren und sie mit anderen verbinden. VPCs Diese Topologie kann zusammen mit den anderen Anwendungstypen und Anwendungsfalllisten verwendet werden. Es wird verwendet, um die Angriffsfläche der VPC-Struktur eines Unternehmens über das Internet zu reduzieren, Kontrollen zu zentralisieren und Aufgaben zu trennen. Es wird auch verwendet, um erweiterte Anwendungs- und Sicherheitsdienste zwischen einer bestimmten VPC, einer anderen VPCs und dem Internet einzufügen.	Stellen Sie eine Transit-VPC zusammen mit den Sichtbarkeitsanforderungen für die Peer-VPC-VPC-IP-Adresse bereit.

Anwendungstyp	Anwendungsfall	Vorgeschlagene Aktion
DNS-Sicherheit, Express- und Hybridanwendungen	Replizieren Sie sichere und konsistente DNS-Lookup-Tabellen in der AWS Cloud und im Rechenzentrum mit der Fähigkeit, große Mengen an DNS-Abfragen zu verarbeiten. Überstehen Sie einen direkten Verbindungsausfall über AWS Direct Connect zentral verwaltetes, richtlinienbasiert es DNS in der gesamten Umgebung, DNS-Caching und DNS-Protokollvalidierung und -Sicherheit (DNSSEC).	Verwenden Sie bewährte Methoden, um DNS bereitzus tellen und jede VPC als virtuelles Rechenzentrum zu behandeln.

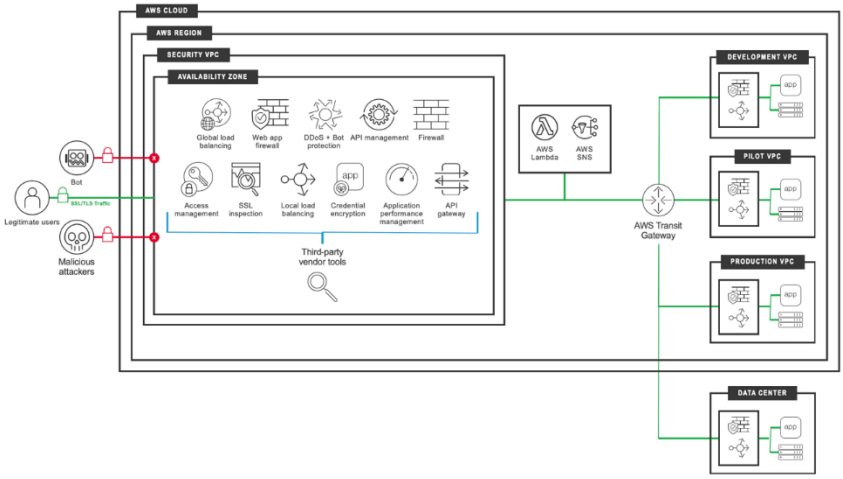
Planung der Architektur

Das folgende Diagramm zeigt die Basisarchitektur von Edge-VPC und Anwendung VPCs, die über AWS Transit Gateway verbunden sind. Sie VPCs können Teil derselben oder verschiedener Konten sein.



Beispielsweise stellt eine landing zone in der Regel ein Netzwerkkonto bereit, das den Edge VPCs steuert. Diese Architektur hilft Benutzern, gemeinsame Richtlinien, Prozesse und Plattformen in der gesamten Anwendungssuite zu nutzen.

Das folgende Diagramm zeigt zwei Netzwerkschnittstellen-Instanzen (NIC) aus einem F5 BIG-IP-Workload, der in einem aktiven Standby-Cluster bereitgestellt wird. Sie können diesen Systemen bis zur Instanzbeschränkung weitere elastische Netzwerkschnittstellen hinzufügen. F5 empfiehlt, dass Sie für Ihre Bereitstellung ein Multi-AZ-Muster verwenden, um einen Ausfall der Availability Zone zu vermeiden.


AWS CLOUD
AWS REGION
SECURITY VPC
AVAILABILITY ZONE
Global load balancing
Web app firewall
DDoS + Bot protection
API management
Firewall
Bot
SSL/TLS traffic
Legitimate users
Malicious attackers
Access management
SSL inspection
Local load balancing
Credential encryption
Application performance management
API gateway
Third-party vendor tools
AWS Lambda
AWS SNS
AWS Transit Gateway
DEVELOPMENT VPC
PILOT VPC
PRODUCTION VPC
DATA CENTER
app

Planung der Migration

Die Planung Ihres Migrationsprozesses ist entscheidend für eine reibungslose und erfolgreiche Migration. In den folgenden Abschnitten wird beschrieben, wie Sie Ihre Migration planen, und die wichtigsten Überlegungen dazu erläutern.

Themen

Entscheiden Sie, was migriert werden soll

Bei der Migration müssen Sie entscheiden, welche Workloads unverzichtbar sind, welche „nett zu haben“, aber nicht unbedingt erforderlich sind und welche Workloads nicht erforderlich sind und nach Abschluss der Migration zurückgezogen werden können.

Ein wesentlicher Teil Ihres Entscheidungsprozesses wird Ihre individuellen Anforderungen an Automatisierung, API, Tools und andere Prozesse beinhalten. Sie müssen auch die Funktions- und Leistungsanforderungen Ihres Unternehmens berücksichtigen.

Möglicherweise haben Sie in einem vorhandenen Rechenzentrum mit Benutzerpartitionen gemeinsam genutzte Hardwareplattformen verwendet. Ihre Migration erfordert jedoch möglicherweise, dass Dienste auf Systemen ausgeführt werden, die aufgrund der Leistungseinschränkungen bei der Umstellung von hardwarebeschleunigten Lösungen nicht so häufig gemeinsam genutzt werden. Beispielsweise könnten Secure Sockets Layer (SSL) -Transaktionen pro Sekunde (TPS) erfordern, dass ein bestimmter Dienst nicht auf einem gemeinsam genutzten System ausgeführt wird.

Nachdem Sie die zu migrierenden Anwendungen und deren Anforderungen identifiziert und dokumentiert haben, müssen Sie Ihre Quellsysteme anhand der folgenden bewährten Methoden vorbereiten.

- Führen Sie dieselbe Version von F5 TMOS aus, die Sie in der AWS Cloud ausführen werden. Version 14.1 oder höher wird empfohlen, es kann jedoch auch Version 13.1 oder höher verwendet

werden. Sie können Version 12.1.x zwar migrieren, es können jedoch Probleme mit Sicherheit, Automatisierung und Wartbarkeit auftreten.

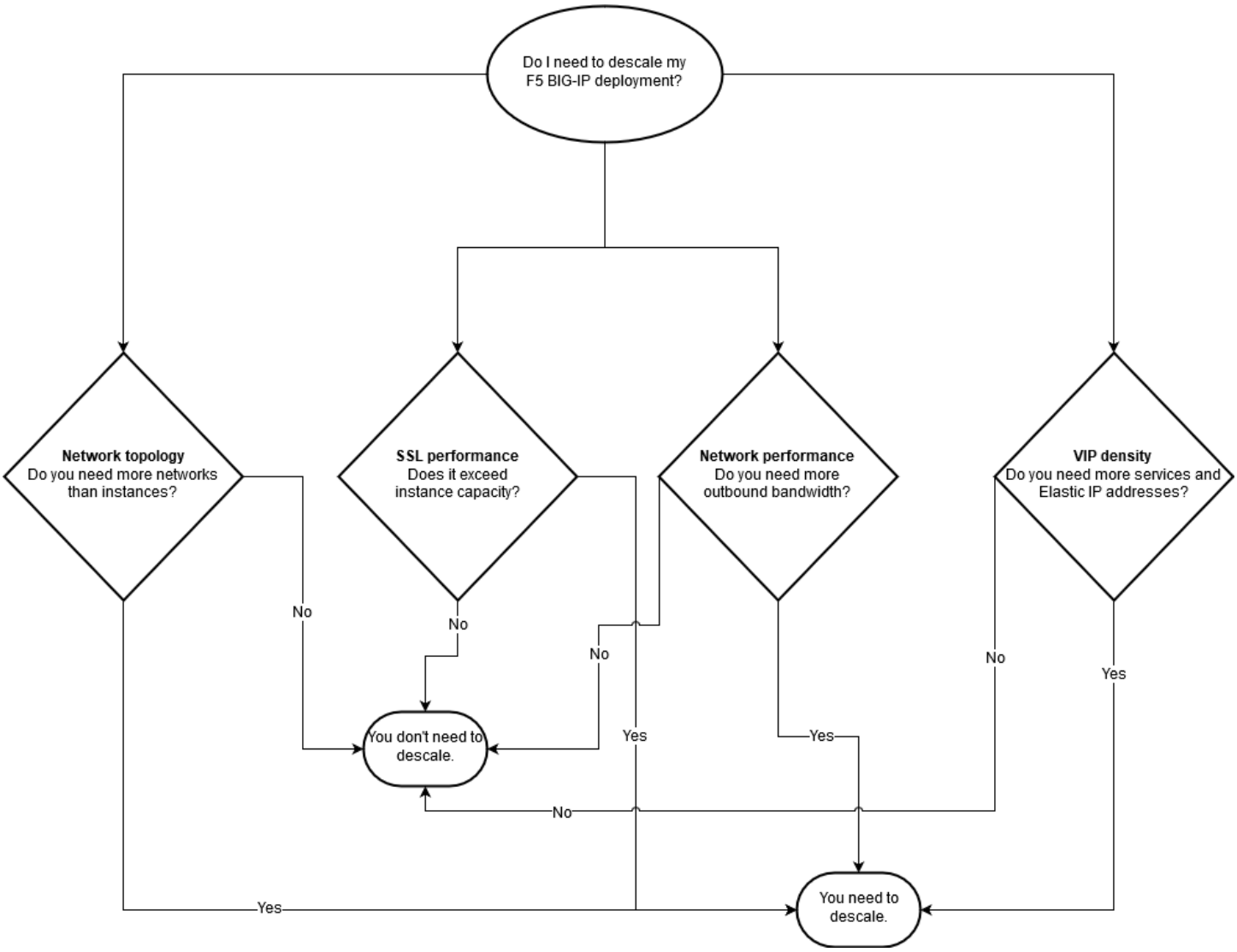
- Halten Sie gültige Backups aller Konfigurationen von jedem Gerät bereit. Da das Univention Corporate Server (UCS) -Backup Attribute und Objekte enthält, die für das Rechenzentrum spezifisch sind (wie IP-Adressen, Knoten oder Poolmitglieder), empfiehlt F5, eine Shell-Befehlsdatei (SCF) zu erstellen, um die Konfigurationen zu bearbeiten und zusammenzuführen.
- Erstellen Sie Backups aller relevanten Sicherheitszertifikate und erwägen Sie, für eine bessere Leistung von der RSA- zur ECC-Verschlüsselung zu wechseln.
- Verfügen Sie über detaillierte Leistungskennzahlen auf virtueller Serverebene für Skalierung und Kapazitätsplanung.
- Verwenden Sie eine GSLB-Lösung (Global Server Load Balancing) von F5 für die Umstellung vom Rechenzentrum auf die Cloud. AWS
- Machen Sie sich mit den Auswirkungen der Migration von einem Hardware-Appliance-Modell auf ein Software- und virtualisiertes Modell in Bezug auf Leistung, Skalierbarkeit und Hochverfügbarkeit vertraut.
- Haben Sie die Anforderungen dafür definiert, was in die AWS Cloud migriert werden soll, und beachten Sie die folgenden Überlegungen.
  - Beachten Sie, dass jede Migration zur AWS Cloud Entscheidungen darüber erfordert, ob ganze oder teilweise Konfigurationen migriert werden. In der Regel ist eine Teilbewegung nach der anderen effizienter.
  - Verstehen Sie, welche Routen und IP-Adressen sich ändern werden.
  - Identifizieren Sie, welche SNAT-Pools durch F5 SNAT Automap ersetzt werden sollten.

Sie sollten auch in Betracht ziehen, AWS Partner oder das F5 Professional Services-Team zu konsultieren. Dies trägt dazu bei, eine hohe Wahrscheinlichkeit einer erfolgreichen Migration sicherzustellen.

Entkalken Sie Ihre Konfigurationen

„Entkalken“ bedeutet, eine F5 BIG-IP-Konfiguration auf eine kostengünstigere oder kostengünstigere Konfiguration umzustellen, die auf den Funktionen oder Metriken basiert, die nach Ihren ersten Erkenntnissen erforderlich sind. Sie müssen all diese Optionen sorgfältig abwägen, da sie sich auf die Architektur und die Anzahl der erforderlichen Instanzen auswirken.

Anhand des folgenden Diagramms können Sie beurteilen, ob die Entkalkung für Ihre Bedürfnisse und Anforderungen geeignet ist.



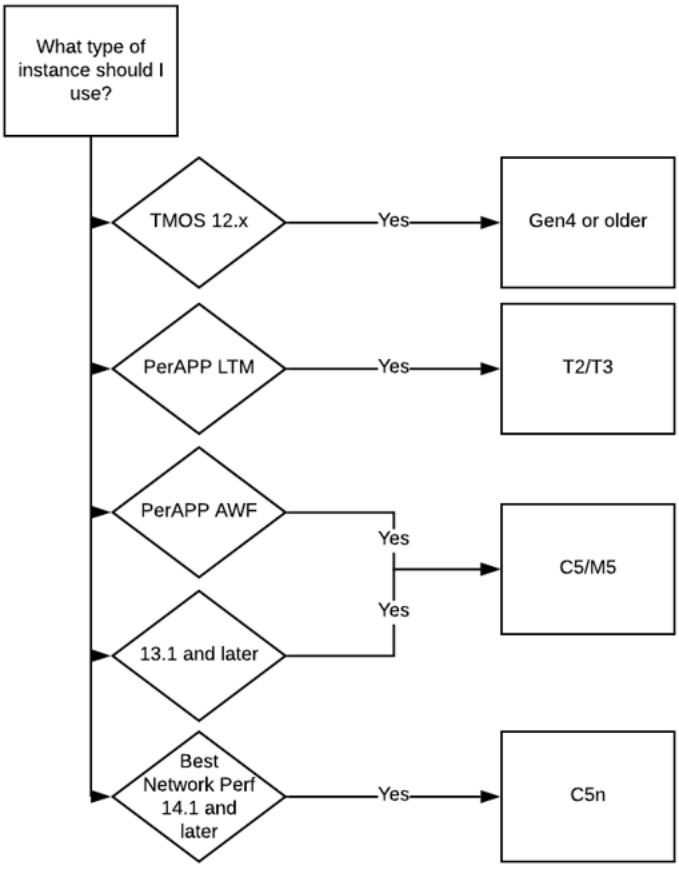
Die Migration wird auch zu neuen Überlegungen in den folgenden Bereichen führen.

- Netzwerktopologie — unterstützt derzeit AWS keine `802.1q` Tagged VLANs, sodass die Anzahl der Instanzschnittstellen (minus eine für die Verwaltung) die Anzahl der Netzwerke, die eine Instanz unterstützen kann, begrenzt. Wenn Sie eine bestimmte Topologie benötigen, müssen Sie sie mit den verschiedenen Instanzen vergleichen, die F5 in der Cloud unterstützt. AWS
- SSL-Leistung — F5-Appliances und Chassis verfügen über eine SSL-Leistung, die das, was erreicht werden kann, übertrifft. `x86` Sie müssen die aggregierten SSL-Anforderungen und die SSL-Anforderungen pro virtuellem Server bewerten.

- Netzwerkleistung — Sie müssen die aggregierten, ausgehenden und internen Netzwerkeigenschaften bewerten. AWS Instance-Typen haben unterschiedliche Netzwerkeigenschaften (niedrig, mittel, hoch, bis zu X oder dediziert), die berücksichtigt werden müssen. Es gibt auch Beschränkungen dafür, wie viel Traffic eine einzelne Instance auswärts oder über eine direkte Verbindung senden kann.
- VIP-Dichte — Wenn Sie über eine größere Anzahl virtueller IP-Adressen (VIPs) verfügen, müssen Sie die Instanzbeschränkung auf die Anzahl der IP-Adressen berücksichtigen VIPs , die den Netzwerkschnittstellen zugeordnet werden können.
- Gleichzeitige Verbindung — Es gibt Flusslimits für die maximale Anzahl von Verbindungen, die die Instances unterstützen können.
- Sitzungsstatus — Verschiedene Anwendungen verwenden unterschiedliche Persistenztypen. Zustandsbehaftete und statusfreie Anwendungen ändern die verwendeten Methoden auf Shared State, was sich auf die Skalierung von In/Out-Vorgängen auswirken kann.

Auswahl des Instanztyps

F5 unterstützt mehrere Instance-Typen, und die Auswahl des zu verwendenden Instance-Typs kann eine komplexe Entscheidung sein. Für die meisten Migrationen `c5n.4xl` wird dies die gängigste Wahl sein, `c5n.2xl` da sie eine Mischung aus Netzwerkleistung, CPU-Dichte, Schnittstellendichte und der Anzahl der Instanzen bieten, die auf der IPs Instance unterstützt werden können. Das folgende Diagramm enthält Beispiele dafür, welche Instances auf der Grundlage der von Ihnen verwendeten F5-Produkte ausgewählt werden sollten.



Wichtige Entscheidungspunkte

Es gibt viele Aspekte der Migration, die berücksichtigt werden müssen. Bevor Sie jedoch mit der Migration Ihrer F5 BIG-IP-Workloads beginnen, sollten Sie sich die folgenden Fragen stellen, um den Migrationsprozess zu klären.

Wer sind die Benutzer Ihrer Anwendungen?

Beurteilen Sie, ob es sich dabei um interne Benutzer (die keine Elastic IP-Adresse durchqueren) oder um externe Benutzer (die eine Elastic IP-Adresse durchqueren) handelt. Wenn es sich bei den Benutzern um interne Benutzer handelt, prüfen Sie, ob die Anwendung DNS verwenden kann, um den Ausfall einer Availability Zone oder einer aktiven Bereitstellung zu beheben. Sie sollten auch überprüfen, ob Sie ein alternatives Entwurfsmuster verwenden müssen, das es einem Subnetz ermöglicht, sich über mehrere Availability Zones zu erstrecken.

Welche Teile Ihrer Anwendungen werden in die AWS Cloud migriert?

Beurteilen Sie, ob die gesamte Anwendung verschoben wird oder nur die Präsentationsebene. Sie sollten auch zusätzliche Abhängigkeiten in Bezug auf Sicherheit und DNS-Namespace berücksichtigen. Im Rahmen Ihrer Evaluierung müssen Sie ermitteln, welche Anforderungen die Netzwerktopologie stellen würde. Ermitteln Sie außerdem, was in einem Service Level Agreement (SLA) vorgeschrieben ist, falls ein Ereignis auf Availability Zone-, VPC- oder AWS Regionsebene eintritt.

Warum wird die Anwendung migriert?

Möglicherweise migrieren Sie Ihre Anwendung, weil Sie Rechenzentren schließen oder weil Sie mehr Elastizität wünschen. Beurteilen Sie, ob die Anwendung im Vergleich zu den gemeinsamen monolithischen Mustern, die in vielen Rechenzentren üblich sind, auf eine anwendungsspezifische Architektur migriert wird. Es lohnt sich auch zu überlegen, welche Modernisierungsmaßnahmen zusammen mit der Migration durchgeführt werden sollten.

Wohin wird die Anwendung migriert?

Beurteilen Sie, ob die Anwendung zu einer einzelnen VPC mit einer Availability Zone oder zwei Availability Zones migriert werden muss. Ermitteln Sie die Peer- oder Transit-VPC-Topologie sowie die Notwendigkeit von Bereitstellungen in mehreren Regionen. Diese werden sich auf das Design des Migrationsmusters auswirken.

Überblick über die Migration auf hoher Ebene

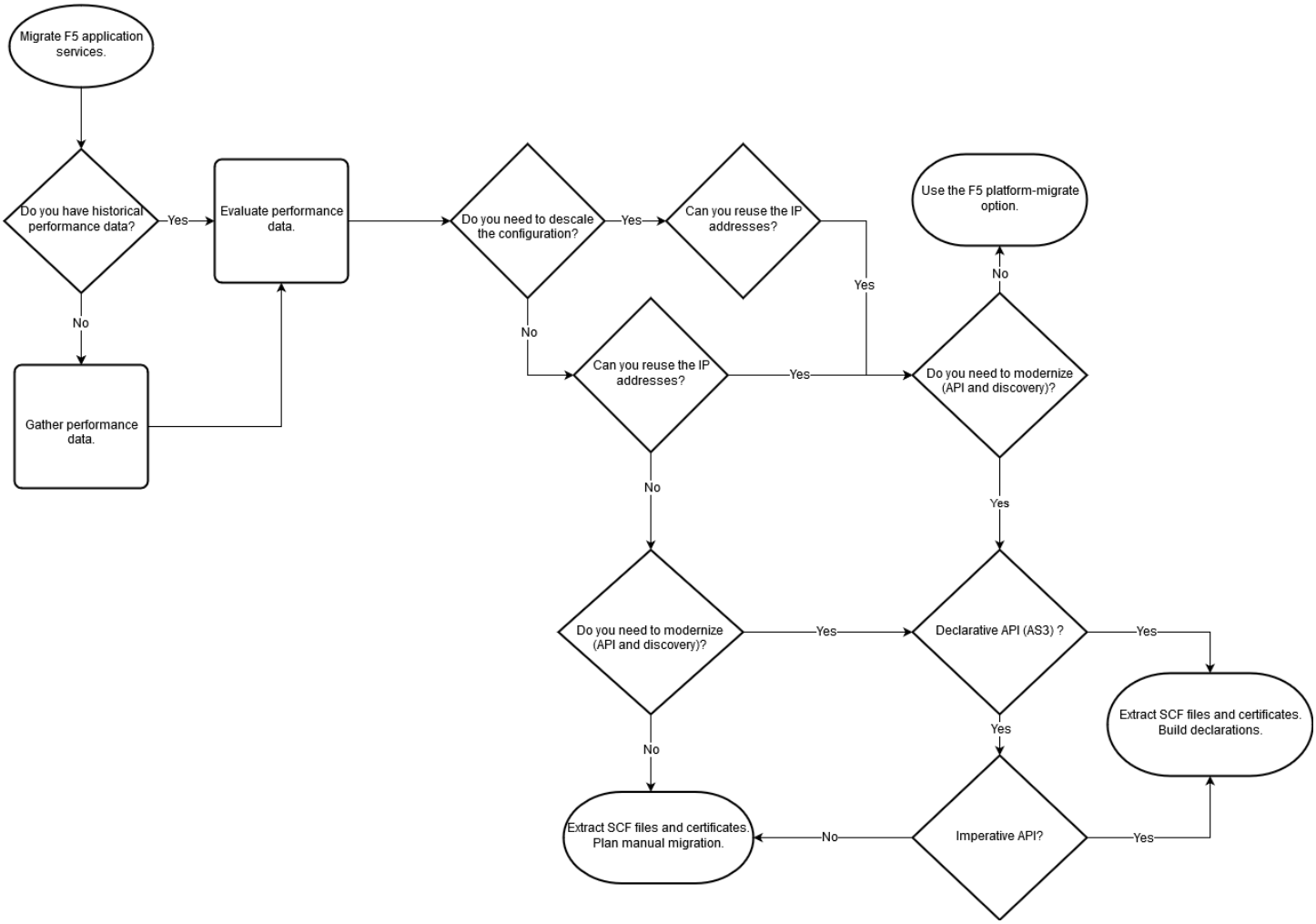
Bevor Sie mit der Migration beginnen, ist es hilfreich, den gesamten Prozess von einer übergeordneten Ebene aus zu gestalten. Im Folgenden finden Sie ein Beispiel für die Schritte, die Sie ergreifen könnten, um einen F5 BIG-IP-Workload in die Cloud zu migrieren. AWS Ausführlichere Schritte und Prozesse für eine F5 BIG-IP-Migration finden Sie im Muster Migrieren Sie einen F5 BIG-IP-Workload zu F5 BIG-IP VE in der Cloud. AWS

1. Stellen Sie die erforderliche Anzahl von auf der Grundlage Ihrer individuellen Anforderungen bereit. VPCs Dies kann manuell oder mithilfe eines Tools wie AWS Landing Zone automatisiert werden.
2. Evaluieren Sie die aktuellen F5-Lizenzen, Nutzungen und Konfigurationen.
3. Evaluieren Sie öffentliche und interne Anwendungen.
4. Evaluieren Sie aktuelle F5-Konfigurationen.

5. Bewerten Sie die Anforderungen an Größe und IP-Adresse und wählen Sie die erforderliche Anzahl und den Typ von F5 und AWS Instanzen aus.
6. Identifizieren Sie, welche Migrationsstrategie eingesetzt werden soll. Zum Beispiel Lift and Shift, Lift, Shift und Modernisieren oder Hybrid.
7. Evaluieren und identifizieren Sie das DNS-Design.
8. Beurteilen Sie, wie der Datenverkehr an die Anwendung weitergeleitet wird, wenn sie sowohl vor Ort als auch in der AWS Cloud vorhanden ist.
9. Führen Sie erste Bereitstellungen von F5-Instanzen mithilfe AWS CloudFormation von Vorlagen durch.
10. Passen Sie Bereitstellungen mit zusätzlichen elastischen Netzwerkschnittstellen und Routing-Tabellen an, um die Topologieanforderungen zu erfüllen.
11. Richten Sie Elastic IP-Adressen an Ihre eigenen IP-Adressen IPs oder an die Verwaltung IPs aus und planen Sie die Zuordnung von Elastic IP zu virtueller IP (VIP).
12. Erstellen Sie sekundäre Adressen auf elastischen Netzwerkschnittstellen für VIPs.
13. Wenden Sie sekundäre Adressen in der AWS Cloud an.
14. Ordnen Sie Elastic IP-Adressen der sekundären Adresse für zu VIPs.
15. Rufen Sie Konfigurationen ab und stellen Sie eine Liste der zu verschiebenden Objekte zusammen.
16. Stellen Sie die Konfigurationen auf F5 BIG-IP bereit.
17. Ordnen Sie die sekundären Adressen zu. VIPs
18. Testen Sie den Verkehr.
19. Testen Sie den Failover.
20. Wenn Sie einen Hybrid erstellen, stellen Sie sicher, dass Sie das System in F5 DNS integrieren.

> **Important**
>
> Zugriff auf die AWS API-Endpunkte ist erforderlich. Für eine hohe Verfügbarkeit innerhalb oder zwischen Availability Zones sind auch NAT- oder Elastic-IP-Adressen erforderlich.

Das folgende Diagramm zeigt den allgemeinen Prozessablauf für eine F5 BIG-IP-Migration.


Migrate F5 application services.
Do you have historical performance data?
Yes
No
Evaluate performance data.
Gather performance data.
Do you need to descale the configuration?
Yes
No
Can you reuse the IP addresses?
Yes
No
Can you reuse the IP addresses?
Yes
No
Use the F5 platform-migrate option.
Do you need to modernize (API and discovery)?
Yes
No
Do you need to modernize (API and discovery)?
Yes
No
Declarative API (AS3) ?
Yes
Yes
Extract SCF files and certificates. Build declarations.
Imperative API?
Yes
No
Extract SCF files and certificates. Plan manual migration.

Daten migrieren

Bei allen Migrationen muss eine Konfiguration wiederholt und der Abhängigkeitsbaum erstellt werden. Wenn Sie eine einzige Konfigurationsdatei verwenden, wird das alles für Sie erledigt. Wenn Sie die TMSH-API verwenden, müssen Sie den Abhängigkeitsbaum iterieren und erstellen. In den folgenden Abschnitten werden die verschiedenen Optionen und Konfigurationen beschrieben, die bei der Migration eines F5 BIG-IP-Workloads verfügbar sind.

Themen

Migration einer vollständigen Konfiguration

Bei diesem Ansatz übernehmen Sie eine Konfiguration aus einem vorhandenen System und migrieren sie auf ein neues System. Bei diesem Vorgang werden eine bestehende Konfiguration, IP-Adressen, Zertifikate, Schlüssel, Passphrasen und Anmeldeinformationen kopiert.

Der Hauptgrund für die Migration einer gesamten Konfiguration ist ein like-for-like Systemaustausch, z. B. ein Hardware-Upgrade oder eine RMA. In der Regel gelten diese Konzepte nicht für die AWS Cloud.

Sie können UCS- oder SCF-Dateien verwenden, um eine vollständige Konfiguration zu migrieren. Die folgenden Tabellen bieten einen Überblick über die Vor- und Nachteile ihrer Verwendung.

Verwenden Sie eine UCS- oder QKView-Datei

Vorteile	Nachteile
Alle Dateien werden als ein einziges Archiv verschoben.	Der Hauptanwendungsfall für die Verwendun g einer UCS-Datei wäre der Austausch eines ausgefallenen Geräts. Das Archiv enthält

Vorteile	Nachteile
	gerätespezifische Informationen, die dazu führen könnten, dass der F5 BIG-IP-Workload nicht erreichbar ist.
Lokale Benutzerkonten werden beibehalten. Wenn sie in Ihr Active Directory integriert sind, bleibt die Konfiguration erhalten.	Wenn Sie eine Verzeichnisintegration konfiguriert haben, haben Sie möglicherweise Zugriffsprobleme. Wenn Sie keinen Zugriff auf die Benutzerkennwörter haben, haben Sie möglicherweise auch Zugriffsprobleme.
Alle virtuellen Serverkonfigurationen werden beibehalten.	Möglicherweise müssen Sie die IP-Adressen des Geräts, der virtuellen Server und der Poolmitglieder bearbeiten.
Die Dateistruktur wird beibehalten.	Sie müssen wissen, welche Dateien bearbeitet werden müssen.
	Dieser Vorgang ist komplexer als ein SCF oder ein object-by-object Umzug.
	Erhöhtes Fehlerrisiko, einschließlich einer erneuten Bereitstellung oder der Möglichkeit, dass die Konfiguration nicht geladen werden kann.
	Konzipiert für Workflows zum Austausch ganzer Systeme.

Verwenden Sie eine SCF-Datei

Vorteile	Nachteile
Erzeugt eine Textdatei der Konfiguration.	Änderungen sind erforderlich, da die Datei gerätespezifische Eigenschaften enthält, die sich auf den Zugriff auswirken können, wenn die Datei einfach geladen wird.

Vorteile	Nachteile
Leicht editierbar in jedem Unix- oder Linux-Texteditor.	Sie müssen die Konfiguration und die Dateistruktur verstehen, um die Änderungen vornehmen zu können.
Die Konfigurationsdatei hat die richtige Reihenfolge der Ladevorgänge.	Sie müssen wissen, welche Teile der Datei entfernt werden müssen, um zu verhindern, dass gerätespezifische Konfigurationen überschrieben werden.
Sie können leicht Objekte finden, die migriert werden sollen.	

Eine Teilkonfiguration migrieren

Wenn Sie sich für die Migration einer Teilkonfiguration entscheiden, verwenden Sie entweder eine TMSH- oder eine SCF-Datei als Ausgangspunkt. Sie müssen auch nach den Objekten suchen, die Sie verschieben möchten, und sie in der richtigen Reihenfolge kompilieren. In der folgenden Tabelle werden die Vor- und Nachteile der Migration einer Teilkonfiguration beschrieben.

Vorteile	Nachteile
Konfigurationen können analysiert und im Laufe der Arbeit Korrekturen vorgenommen werden.	Kenntnisse über F5-Objekte und Dateistrukturen sind erforderlich. Sie müssen auch in der Lage sein, iRules zu lesen.
Konfigurationsänderungen können gebündelt werden.	Die Migration benötigt Zeit.
Einfachere Behebung von Problemen beim Laden der Konfiguration.	Das Bearbeiten der Dateien oder das Extrahieren der Informationen kann zeitaufwändig sein.
Geringeres Risiko, vom Gerät ausgesperrt zu werden.	
Es ist einfacher, die Konfiguration in eine geeignete Topologie zu verschieben.	

Vorteile	Nachteile
Es ist einfacher, Administratorpartitionen zu adressieren und Domänen weiterzuleiten, da es sich um eine Flatfile handelt.	
Die Flatfile-Struktur ermöglicht die Verwendung von Linux-Texttools, wenn Sie IP-Adressen programmgesteuert suchen und ersetzen möchten.	

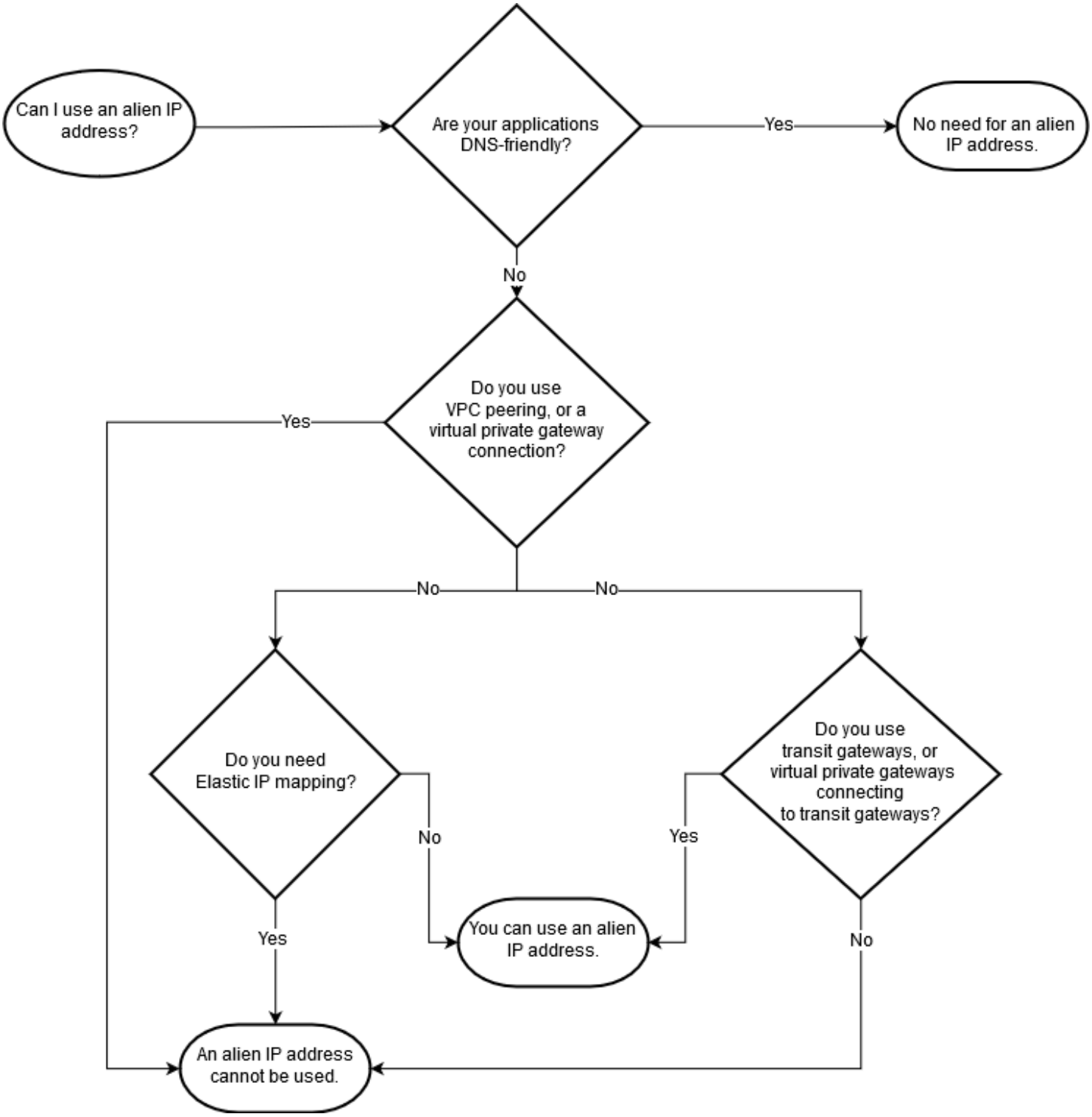
Bereitstellungen mit hoher Dichte ohne Elastic IPs

Wenn Sie Bereitstellungen mit hoher Dichte benötigen, können Sie anhand der Leistungskennzahlen arbeiten, ohne dass Elastic für diese Anwendungen erforderlich ist. IPs Dies wird als „Alien-IP“ bezeichnet.

Eine Alien-IP ist ein Netzwerk oder ein Subnetzbereich, der sich außerhalb des VPC-CIDR-Blocks befindet und dem F5 virtuelle Dienste zuordnet. Alien-IP-Adressen funktionieren nicht in allen Szenarien, können aber für eine hohe Dichte an virtuellen Servern verwendet werden. Bevor eine Alien-IP verwendet werden kann, sind die folgenden Ressourcen erforderlich.

- Ein Subnetz zum Hosten der Anwendungen
- Eine F5 BIG-IP-Bereitstellung mit einer Cloud-Failover-Erweiterung zur Verwaltung der Routen
- Eine Route in den Routentabellen, die AWS auf die elastischen Netzwerkschnittstellen verweist

Die Verwendung fremder IP-Adressen hat Auswirkungen darauf VPCs, wie Sie VPCs sich mit anderen verbinden und wie Sie sich mit Ihren Rechenzentren VPCs verbinden können. Anhand des folgenden Diagramms können Sie feststellen, ob eine fremde IP-Adresse erforderlich ist.



Verbindung zwischen Ihren VPCs

Die folgenden Tabellen zeigen die wichtigsten Überlegungen, wenn Sie Ihre miteinander verbinden. VPCs

Sicherheits-VPC mit VPC-Peering		Sicherheits-VPC mit AWS Transit Gateway		Sicherheits-VPC mit VPN-Verbindung	
Vorteile	Nachteile	Vorteile	Nachteile	Vorteile	Nachteile
• Einfach und schnell einzurichten • Einfaches Routing • Hohe Redundanz • Hohe Bandbreite	• Unterstützt nur Traffic aus VPC-zugewiesenen CIDR-Bereichen • Eine Sicherheitsinspektion kann nicht eingefügt werden zwischen VPCs • Die Verwaltung im großen Maßstab ist komplex (alle sind es point-to-point)	• Einfach einzurichten • Flexibles Routing ohne SNAT • Hohe Redundanz • Hohe Bandbreite • Einfach und in großem Maßstab zu verwalten	• Routing ist komplexer (VPC-Routentabellen und AWS Transit Gateway Gateway-Routentabellen) • Komplexe Topologie zum Einfügen einer Sicherheitsinspektion dazwischen VPCs	• Flexibles Routing ohne SNAT • Einfaches Einfügen einer Sicherheitsinspektion zwischen VPCs	• Niedrige Bandbreite • Komplexes, herstellerspezifisches, abhängiges Failover • Umfangreiches Management ist komplex (alle sind) point-to-point

Client (sendet SYN)	AWS Transit Gateway	VPC-Peering	VPN zwischen VPCs	Lösungsübersicht und mögliche Bedenken
Internet oder AWS Direct Connect Service in einer einzelnen VPC mit einem öffentlichen oder privaten Subnetz.	N/A	–	N/A	Der Datenverkehr durchquert das Internet-Gateway oder das virtuelle Gateway — es muss nicht mehr als die VPC-Grenze überschreiten. VPC fungiert als entworfene Stub-Netzwerke. Der eingehende Datenverkehr erfolgt von lokalen Standorten in die AWS Cloud (AWS Direct Connect, VPN).
Internet oder AWS Direct Connect in einer VPC mit Clients in einer anderen VPCs (z. B. Poolmitglieder in einer anderen VPC), kein SNAT.	Ja	Nein	Ja	AWS Transit Gateway oder VPNs lassen Sie zu, dass der Datenverkehr den VPC-Peering-Filter umgeht, den nur von VPC zugewiesene Benutzer passieren CIDRs können. VPN-Lösungen werden eingeschränkt sein. Kein gleichwertiges Multi-Path-Routing (ECMP) (nur eine einzige Route) und keine Bandbreite (etwa 1,2 GB-Sekunden pro Tunnel, im Allgemeinen nur ein Tunnel).
Internet oder AWS Direct Connect zu einem Dienst in einer VPC mit Kunden in einer anderen VPCs (z. B. Poolmitglieder in einer	Ja (aber nicht erforderlich)	Ja	Ja (aber nicht erforderlich)	Da die Verbindung zwischen den Verbindungen den VPCs Datenverkehr von VPC zuweist CIDRs, funktioniert jeder. VPN-Lösungen werden eingeschränkt sein. Kein ECMP (nur eine einzige Route) und keine Bandbreite (etwa 1,2 GB-Sekunden pro Tunnel, im Allgemeinen nur ein Tunnel).

Client (sendet SYN)	AWS Transit Gateway	VPC-Peering	VPN zwischen VPCs	Lösungsübersicht und mögliche Bedenken
anderen VPC), mit SNAT.				
Innerhalb der VPC für den Betrieb in derselben VPC.	N/A	–	N/A	Der gesamte Verkehr ist auf eine einzige VPC beschränkt. Eine Zusammenschaltung ist nicht erforderlich.
Innerhalb einer VPC zu einer Service-VPC. Der Dienst befindet sich in der Ziel-VPC CIDR.	Ja (aber nicht erforderlich)	Ja	Ja (aber nicht erforderlich)	Da die Verbindung zwischen den Verbindungen den VPCs Datenverkehr von VPC zuweist CIDRs, funktioniert jeder.
Innerhalb einer VPC zu einer Service-VPC. Der Service liegt außerhalb des VPC-CIDR-Bereichs.	Ja	Nein	Ja	Da die Verbindung zwischen den Verbindungen den VPCs Datenverkehr von VPC zuweist CIDRs, funktioniert jeder. VPN-Lösungen werden eingeschränkt sein. Kein ECMP (nur eine einzige Route) und keine Bandbreite (etwa 1,2 GB-Sekunden pro Tunnel, im Allgemeinen nur ein Tunnel).
Innerhalb einer einzelnen VPC zu einem Internetdienst.	N/A	–	N/A	Der Datenverkehr stammt von einem von der VPC zugewiesenen CIDR. Wenn Elastic IP-, NAT- oder Routentabellenkonstrukte inline sind, fließt der Verkehr.

Client (sendet SYN)	AWS Transit Gateway	VPC-Peering	VPN zwischen VPCs	Lösungsübersicht und mögliche Bedenken
Innerhalb einer VPC zu einem Internetdienst, Routing über eine Sicherheits- oder Inspektions-VPC.	Ja	Nein	Ja	Da die Verbindung zwischen den Datenverkehr von außerhalb eines von VPCs der VPC zugewiesenen CIDR-Bereichs empfängt, kann VPC-Peering nicht verwendet werden. VPN-Lösungen werden eingeschränkt sein. Kein ECMP (nur eine einzige Route) und keine Bandbreite (etwa 1,2 GB-Sekunden pro Tunnel, im Allgemeinen nur ein Tunnel).

Verbindung zu Ihrer Infrastruktur herstellen AWS

Die folgende Tabelle zeigt die wichtigsten Überlegungen, die Sie bei der Verbindung mit Ihrer neuen AWS Infrastruktur während einer F5 BIG-IP-Migration berücksichtigen sollten.

Methode der Konnektivität	Unterstützung für das Routing-Protokoll	Bandbreitenbeschränkungen	Endpunkt-IP-Adressierung (öffentlich, privat oder beides)	Support für Alien-Adressraum	Multi-VPC-Unterstützung für eine Verbindung	Unterstützung für mehrere Regionen
Internet	N/A	Sie stellen eine Verbindung her AWS, 5 GB-Sekunden pro	Öffentlich	Nein	Ja	Ja

Methode der Konnektivität	Unterstützung für das Routing-Protokoll	Bandbreitenbeschränkungen	Endpunkt-IP-Adressierung (öffentlich, privat oder beides)	Support für Alien-Adressraum	Multi-VPC-Unterstützung für eine Verbindung	Unterstützung für mehrere Regionen
		ausgehender Instanz				
VPN - VPC	Statisch, BGP	IPsec Grenzwerte (etwa 1,2 GB-Sekunden pro Tunnel)	Privat	Ja (Sie müssen einen zusätzlichen IPsec Tunnel vom F5 BIG-IP in der VPC zum virtuellen Gateway einrichten, das mit der VPC verbunden ist).	Nein	Nein
VPN und AWS Transit Gateway	Statisch, BGP	IPsec Grenzwerte (etwa 1,2 GB-Sekunden pro Tunnel)	Privat	Ja	Ja	Nein (wenn das Transit-Gateway erweitert wird, wird es beeinträchtigt)

Methode der Konnektivität	Unterstützung für das Routing-Protokoll	Bandbreitenbeschränkungen	Endpunkt-IP-Adressierung (öffentlich, privat oder beides)	Support für Alien-Adressraum	Multi-VPC-Unterstützung für eine Verbindung	Unterstützung für mehrere Regionen
AWS Direct Connect - VPC	Statisch, BGP	AWS Direct Connect Limits (unterstützt Bonding), einzelne Instanzen sind auf 5 GB-Sekunden begrenzt	beides	Nein	Nein	Nein
AWS Direct Connect - Gateway	Statisch, BGP	AWS Direct Connect Limits (unterstützt Bonding), einzelne Instanzen sind auf 5 GB-Sekunden begrenzt	beides	Nein	Ja	Ja

Methode der Konnektivität	Unterstützung für das Routing-Protokoll	Bandbreitenbeschränkungen	Endpunkt-IP-Adressierung (öffentlich, privat oder beides)	Support für Alien-Adressraum	Multi-VPC-Unterstützung für eine Verbindung	Unterstützung für mehrere Regionen
AWS Direct Connect gateway - AWS Transit Gateway (auf mehrere AWS Regionen beschränkt)	Statisch, BGP	AWS Direct Connect Limits (unterstützt Bonding), einzelne Instanzen sind auf 5 GB-Sekunden begrenzt	Mündliche Bestätigung durch das AWS Architektenteam	Ja	Ja	Beschränkt auf mehrere Regionen

Ressourcen

F5-Dokumentation

- F5 Cloud Failover-Erweiterung
- F5-Telemetrie-Streaming
- F5-Topologielabor
- F5 Application Services auf AWS: ein Überblick (Video)
- Benutzerhandbuch für die F5 Application Services 3-Erweiterung
- F5 Devcentral GitHub
- F5 iControl REST-Wiki
- F5-Übersicht über einzelne Konfigurationsdateien (11.x - 15.x)
- F5-Whitepapers
- Überblick über die Option „Plattform-Migrate“ für das UCS-Archiv
- Wissenszentrum für die F5 BIG-IP Cloud Edition

AWS Ressourcen

- F5 im Marketplace AWS
- F5 BIG-IP VE aktiviert: Schnellstart AWS

AWS Partner

- F5 an AWS

Verwandte Anleitungen und Muster

- Migrieren Sie einen F5 BIG-IP-Workload zu F5 BIG-IP VE in der Cloud AWS

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	16. November 2020

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance verwendet. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-kompatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2 Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung in der AWS Migrationsstrategie finden Sie im Operations Integration Guide. AIOps

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den

öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Cloud-Einführung (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für die erfolgreiche Umstellung auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue

Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, sogenannte bösartige Bots, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Exzellenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition eines CCo E, Einrichtung eines Betriebsmodells)

- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oderBitbucket Cloud. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD is commonly described as a pipeline. CI/CDkann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil

der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen historischer Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto

wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, wie z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, die Sie verwenden, um Ausfallzeiten und Datenverluste aufgrund einer Katastrophe zu minimieren. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration. Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter Was ist elektronischer Datenaustausch.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen

Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.
- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit,

Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

Eingabeaufforderung mit wenigen Klicks

Bereitstellung einer kleinen Anzahl von Beispielen, die die Aufgabe und das gewünschte Ergebnis veranschaulichen, bevor das LLM aufgefordert wird, eine ähnliche Aufgabe auszuführen. Bei dieser Technik handelt es sich um eine Anwendung des kontextbezogenen Lernens, bei der Modelle anhand von Beispielen (Aufnahmen) lernen, die in Eingabeaufforderungen eingebettet sind. Bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, kann die Eingabeaufforderung mit wenigen Handgriffen effektiv sein. Siehe auch Zero-Shot Prompting.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

Ein großes neuronales Deep-Learning-Netzwerk, das mit riesigen Datensätzen generalisierter und unbeschrifteter Daten trainiert wurde. FMs sind in der Lage, eine Vielzahl allgemeiner Aufgaben zu erfüllen, z. B. Sprache zu verstehen, Text und Bilder zu generieren und Konversationen in natürlicher Sprache zu führen. Weitere Informationen finden Sie unter Was sind Foundation-Modelle.

G

generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mit einer einfachen Textaufforderung neue Inhalte und Artefakte wie Bilder, Videos, Text und Audio erstellen können. Weitere Informationen finden Sie unter Was ist Generative KI.

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

goldenes Bild

Ein Snapshot eines Systems oder einer Software, der als Vorlage für die Bereitstellung neuer Instanzen dieses Systems oder dieser Software verwendet wird. In der Fertigung kann ein Golden Image beispielsweise zur Bereitstellung von Software auf mehreren Geräten verwendet werden und trägt zur Verbesserung der Geschwindigkeit, Skalierbarkeit und Produktivität bei der Geräteherstellung bei.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dazu beiträgt, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Unternehmenseinheiten zu regeln (OUs). Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Holdout-Daten

Ein Teil historischer, beschrifteter Daten, der aus einem Datensatz zurückgehalten wird, der zum Trainieren eines Modells für maschinelles Lernen verwendet wird. Sie können Holdout-Daten verwenden, um die Modellleistung zu bewerten, indem Sie die Modellvorhersagen mit den Holdout-Daten vergleichen.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS Security Reference Architecture empfiehlt, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr und Inspektion einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer

schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

industrielles Internet der Dinge (T) IIo

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Weitere Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in demselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit des Modells für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten

und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

großes Sprachmodell (LLM)

Ein Deep-Learning-KI-Modell, das anhand einer riesigen Datenmenge vorab trainiert wurde. Ein LLM kann mehrere Aufgaben ausführen, z. B. Fragen beantworten, Dokumente zusammenfassen, Text in andere Sprachen übersetzen und Sätze vervollständigen. Weitere Informationen finden Sie unter Was sind. LLMs

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der

Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Dienst, der über genau definierte Kanäle kommuniziert APIs und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren mithilfe von Lightweight über eine klar definierte Schnittstelle. APIs Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementierung von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Siehe Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während

der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Einen Trail für eine Organisation erstellen.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS Security Reference Architecture empfiehlt die Einrichtung Ihres Netzwerkkontos mit eingehendem und ausgehendem Datenverkehr sowie Inspektion, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe

Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

Ein systemtechnischer Ansatz, der den Datenschutz während des gesamten Entwicklungsprozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und deren Subdomains innerhalb einer oder mehrerer VPCs Domains antworten

soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Diese Steuerelemente scannen Ressourcen, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

schnelle Verkettung

Verwendung der Ausgabe einer LLM-Eingabeaufforderung als Eingabe für die nächste Aufforderung, um bessere Antworten zu generieren. Diese Technik wird verwendet, um eine komplexe Aufgabe in Unteraufgaben zu unterteilen oder um eine vorläufige Antwort iterativ zu verfeinern oder zu erweitern. Sie trägt dazu bei, die Genauigkeit und Relevanz der Antworten eines Modells zu verbessern und ermöglicht detailliertere, personalisierte Ergebnisse.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen,

den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

LAPPEN

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

Ein systemtechnischer Ansatz, der die Sicherheit während des gesamten Entwicklungsprozesses berücksichtigt.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als

detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer EC2 Amazon-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Steuerung der Berechtigungen für alle Konten in einer Organisation in ermöglicht AWS Organizations. SCPs Definieren Sie Leitplanken oder legen Sie Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können sie SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Dienste oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, während Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb

genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

Systemaufforderung

Eine Technik, mit der einem LLM Kontext, Anweisungen oder Richtlinien zur Verfügung gestellt werden, um sein Verhalten zu steuern. Systemaufforderungen helfen dabei, den Kontext festzulegen und Regeln für Interaktionen mit Benutzern festzulegen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der Dokumentation unter Was ist ein Transit-Gateway. AWS Transit Gateway

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen

finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs , die es Ihnen ermöglicht, den Verkehr mithilfe privater IP-Adressen weiterzuleiten. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems beeinträchtigt.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur gilt als unveränderlich.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zero-Shot-Aufforderung

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein

vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Prompting.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.