Amazon Web Services: Übersicht über die Sicherheitsprozesse

Juni 2014

(Die neueste Version dieses Dokuments finden Sie unter **http://aws.amazon.com/de/security/**.)

Inhalt

Amazon Web Services (AWS) bietet eine skalierbare Cloud Computing-Plattform mit hoher Verfügbarkeit und Zuverlässigkeit, die Kunden die Flexibilität bietet, eine Vielzahl von Anwendungen zu erstellen. Der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Daten unserer Kunden ist für AWS ebenso von großer Bedeutung, wie das Vertrauen der Kunden zu bewahren. In diesem Dokument sollen Fragen beantwortet werden, wie zum Beispiel „Wie hilft mir AWS beim Schutz meiner Daten?“. Insbesondere werden die physischen und betrieblichen Sicherheitsprozesse für die von AWS verwaltete Netzwerk- und Serverinfrastruktur, sowie servicespezifische Sicherheitsimplementierungen beschrieben.

Umgebung mit geteilter Verantwortung

Durch das Verschieben der IT-Infrastruktur in AWS entsteht ein Modell geteilter Verantwortung zwischen dem Kunden und AWS. Dieses gemeinsame Modell kann Sie im IT-Betrieb entlasten, da Komponenten vom Hostbetriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Anlagen, in denen der Betrieb der Services stattfindet, von AWS betrieben, verwaltet und gesteuert werden. Sie übernehmen wiederum die Verantwortung und Verwaltung für das Gastbetriebssystem (einschließlich der Updates und Sicherheitspatches), für andere zugehörige Anwendungssoftware sowie für die Konfiguration der von AWS bereitgestellten Sicherheitsgruppen-Firewall. Sie sollten die Services sorgfältig wählen, da Ihre Verantwortlichkeiten abhängig von den verwendeten Services, der Integration dieser Services in Ihre IT-Umgebung und den anwendbaren Gesetzen und Vorschriften unterschiedlich sind. Sie haben die Möglichkeit, die Sicherheit zu erhöhen bzw. strengere Compliance-Anforderungen zu erfüllen, indem Sie Technologien wie hostbasierte Firewalls, hostbasierte Angriffserkennung bzw. hostbasierten Angriffsschutz und Verschlüsselung verwenden.

Sicherheit der AWS Infrastruktur

AWS betreibt die Cloud-Infrastruktur, die Sie zur Bereitstellung verschiedener grundlegender Computerressourcen wie Datenverarbeitung und Datenpeicher benötigen. Die AWS-Infrastruktur enthält Anlagen, Netzwerk, Hardware und einen Teil der Betriebssoftware (z. B. Hostbetriebssystem, Virtualisierungssoftware usw.), welche die Bereitstellung und Verwendung dieser Ressourcen unterstützen. Die AWS-Infrastruktur wird gemäß empfohlener Vorgehensweisen und einer Reihe von Sicherheits-Compliance-Standards entwickelt und verwaltet. Als AWS-Kunde können Sie darauf vertrauen, dass Sie Ihre Webarchitektur auf einer der sichersten Computing-Infrastrukturen weltweit aufbauen.

AWS-Compliance-Programm

Mithilfe des AWS-Compliance-Programms können Kunden die zugrunde liegende robuste Sicherheitsstruktur nachvollziehen und dann ihre Compliance den branchenspezifischen und behördlichen Sicherheits- und Datenschutzanforderungen entsprechend optimieren. Die IT-Infrastruktur, die AWS für Kunden bereitstellt, wird nach Best Practices für die Sicherheit und einer Reihe von IT-Sicherheitsstandards entwickelt und verwaltet. Dazu gehören:

- SOC 1/SSAE 16/ISAE 3402 (früher SAS 70 Typ II)
- SOC 2
- SOC 3
- FISMA, DIACAP und FedRAMP
- PCI DSS Level 1
- ISO 27001
- ITAR

- FIPS 140-2

Außerdem können Kunden aufgrund der Flexibilität und Kontrollmöglichkeiten der AWS-Plattform Lösungen bereitstellen, die eine Reihe von branchenspezifischen Standards erfüllen. Dazu gehören:

- HIPAA
- Cloud Security Alliance (CSA)
- Motion Picture Association of America (MPAA)

AWS bietet Kunden bezüglich der IT-Kontrollumgebung umfangreiche Informationen in Form von Whitepapers, Berichten, Zertifizierungen, Akkreditierungen und anderen Nachweisen Dritter. Weitere Informationen dazu finden Sie im Whitepaper zu Risiko und Compliance auf der Website: http://aws.amazon.com/de/security/

Physische Sicherheit und Umgebungssicherheit

Die Rechenzentren von AWS sind hochmodern und wenden innovative architektonische und technische Ansätze an. Amazon verfügt über langjährige Erfahrung in Entwicklung, im Aufbau und im Betrieb groß angelegter Rechenzentren. Diese Erfahrung wurde in der AWS-Plattform und -Infrastruktur angewendet. AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht. Der physische Zugang wird sowohl im Umkreis der Anlage als auch an Zutrittspunkten zum Gebäude durch professionelles Sicherheitspersonal streng kontrolliert, das Videoüberwachung, Einbruchmeldeanlagen und andere elektronische Mittel verwendet. Autorisiertes Personal muss mindestens zweimal eine Zwei-Faktor-Authentifizierung durchlaufen, um Zutritt zu den Räumen des Rechenzentrums zu erlangen. Alle Besucher und Zeitarbeitskräfte müssen sich ausweisen, werden angemeldet und ständig von autorisiertem Personal begleitet.

Mitarbeitern und Zeitarbeitern wird der Zugang zu Rechenzentren nur gewährt, wenn hierfür eine legitime geschäftliche Notwendigkeit besteht. Sobald diese geschäftliche Notwendigkeit nicht mehr besteht, wird der Zugang sofort widerrufen, auch wenn die Person weiterhin bei Amazon oder Amazon Web Services beschäftigt ist. Jeder physische Zutritt von AWS-Mitarbeitern in die Rechenzentren wird routinemäßig protokolliert und geprüft.

Branderkennung und -bekämpfung

Es wurden Einrichtungen zur automatischen Branderkennung und -bekämpfung angebracht, um das Risiko zu verringern. Das Branderkennungssystem setzt Rauchsensoren in allen Rechenzentrumsumgebungen, in mechanischen und elektrischen Infrastrukturbereichen, Kühlräumen und Räumen für Generatoranlagen ein. Diese Bereiche werden entweder durch Wassersprinkler, vorgesteuerte und doppelt verriegelte Sprinklersysteme oder Gaslöschanlagen geschützt.

Strom

Die elektrischen Anlagen der Rechenzentren wurden so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können – und dies rund um die Uhr, sieben Tage die Woche. Uninterruptable Power Supply-Geräte (UPS, unterbrechungsfreie Stromversorgung) liefern im Fall eines Stromausfalls Notstrom an die kritischen Lasten der Anlage. Die Rechenzentren verfügen über Generatoren, welche Notstrom an die gesamte Anlage liefern können.

Klimatisierung und Temperatur

Eine Klimatisierung ist erforderlich, damit Server und andere Hardware eine konstante Betriebstemperatur beibehalten. Sie verhindert eine Überhitzung und verringert das Risiko von Service-Ausfällen. Die Rechenzentren sind so klimatisiert, dass die atmosphärischen Bedingungen im Optimalbereich bleiben. Personal und Systeme überwachen und steuern die richtige Temperatur und Luftfeuchtigkeit.

Verwaltung

AWS überwacht elektrische, mechanische und lebenserhaltende Systeme und Anlagen, sodass jegliche Probleme sofort erkannt werden. Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

Außerbetriebnahme von Speichergeräten

Wenn die Lebensdauer eines Speichergeräts zu Ende geht, führt AWS einen Prozess zur Außerbetriebnahme durch, der entwickelt wurde, damit Kundendaten nicht an unautorisierte Personen offengelegt werden. AWS wendet die in DoD 5220.22-M („National Industrial Security Program Operating Manual“) oder NIST 800-88 („Guidelines for Media Sanitization“) beschriebenen Techniken an, um Daten im Rahmen des Prozesses zur Außerbetriebnahme zu zerstören. Alle stillgelegten Magnetspeichergeräte werden entmagnetisiert und physisch den branchenüblichen Vorgehensweisen entsprechend zerstört.

Geschäftskontinuitätsverwaltung

Die Infrastruktur von Amazon weist ein hohes Maß an Verfügbarkeit auf und bietet Kunden Funktionen zur Bereitstellung einer stabilen IT-Architektur. AWS hat seine Systeme so entwickelt, dass sie System- oder Hardwareausfälle tolerieren, und Kunden nur minimale Auswirkungen zu spüren bekommen. Die Geschäftskontinuitätsverwaltung der Rechenzentren in AWS steht unter der Leitung der Infrastrukturgruppe von Amazon.

Verfügbarkeit

Rechenzentren werden in Clustern in verschiedenen Regionen der Welt errichtet. Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen.

AWS bietet Ihnen die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich z.B. in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonenkategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden.

Sie sollten die Architektur Ihrer AWS-Nutzung so erstellen, dass sie mehrere Regionen und Availability Zones umfasst. Durch das Verteilen von Anwendungen über mehrere Availability Zones bleibt die Architektur bei den meisten Ausfallarten, einschließlich Naturkatastrophen oder Systemausfällen, stabil.

Vorfallreaktion

Das Amazon-Team zur Verwaltung von Vorfällen wendet branchenübliche diagnostische Verfahren an, um die Behebung unternehmenskritischer Vorfälle voranzutreiben. Das Betriebspersonal bietet eine kontinuierliche Besetzung rund um die Uhr, sieben Tage die Woche und an 356 Tagen im Jahr, um Störfälle zu erkennen und deren Auswirkungen und Behebung zu verwalten.

Unternehmensweite Überprüfung durch die Geschäftsführung

Die Amazon-Gruppe für interne Prüfungen hat vor kurzem die Stabilitätspläne der AWS-Services überprüft. Sie werden ebenfalls regelmäßig von Mitgliedern der Geschäftsführung und des Prüfungsausschusses des Firmenvorstands überprüft.

Kommunikation

AWS hat verschiedene Methoden zur internen Kommunikation auf weltweiter Ebene implementiert, um Mitarbeiter dabei zu unterstützen, ihre jeweiligen Rollen und Verantwortlichkeiten zu verstehen und wichtige Vorfälle zeitgerecht zu kommunizieren. Zu diesen Methoden zählen Orientierungs- und Trainingsprogramme für neu eingestellte Mitarbeiter, regelmäßige Zusammenkünfte des Managements zur Besprechung von Updates zur Unternehmensleistung und anderen Themen, sowie elektronische Medien wie Videokonferenzen, E-Mails und das Posten von Informationen über das Amazon-Intranet.

AWS hat ebenfalls verschiedene Methoden der externen Kommunikation implementiert, um seine Kunden und die Community zu unterstützen. Es wurden Mechanismen eingerichtet, die das Kunden-Support-Team über Betriebsstörungen benachrichtigen, wenn durch diese die Nutzererfahrung der Kunden beeinträchtigt wird. Ein „Service Health Dashboard“ steht zur Verfügung, dass vom Kunden-Support-Team verwaltet wird, und in dem Kunden auf bestehende Probleme hingewiesen werden, die größere Auswirkungen auf sie haben könnten. Ein „Sicherheits- und Compliance-Zentrum“ wird bereitgestellt, damit Informationen zur Sicherheit und Compliance in AWS an einem Ort verfügbar sind. Sie können ebenfalls AWS-Support-Angebote abonnieren, die eine direkte Kommunikation mit dem Kunden-Support-Team und proaktive Meldungen zu sämtlichen Problemen umfassen, die eine Auswirkung auf Kunden haben könnten.

Netzwerksicherheit

Das AWS-Netzwerk wurde darauf ausgelegt, dass Sie die Sicherheits- und Stabilitätsebene Ihrem Bedarf entsprechend wählen können. Damit Sie geografisch gestreute, fehlertolerante Webarchitekturen mit Cloud-Ressourcen errichten können, hat AWS eine erstklassige Netzwerkinfrastruktur implementiert, die sorgfältig überwacht und verwaltet wird.

Sichere Netzwerkarchitektur

Netzwerkgeräte, einschließlich der Firewall und anderer Geräte zur Systemabgrenzung, wurden eingerichtet, um die Kommunikation an den äußeren Grenzen des Netzwerks und an wichtigen internen Grenzen innerhalb des Netzwerks zu überwachen und zu steuern. Diese Geräte zur Systemabgrenzung wenden Regelsätze, Access Control Lists (ACL, Zugriffskontrolllisten) und Konfigurationen an, um den Informationsfluss zu spezifischen Informationssystemdiensten zu regeln.

ACLs oder Datenflussrichtlinien werden auf jeder Schnittstelle eingerichtet und verwalten bzw. regeln dort den Datenfluss. ACL-Richtlinien werden vom Amazon-Team für Informationssicherheit genehmigt. Diese Richtlinien werden automatisch mithilfe des ACL-Verwaltungs-Tools von AWS übertragen, um zu gewährleisten, dass diese verwalteten Schnittstellen die neuesten ACLs umsetzen.

Sichere Zugriffspunkte

AWS hat eine beschränkte Anzahl von Zugriffspunkten zur Cloud an strategisch geeigneten Stellen platziert, damit eine umfassendere Überwachung der ein- und ausgehenden Kommunikation sowie des Netzwerkdatenverkehrs ermöglicht wird. Diese Kundenzugriffspunkte heißen API-Endpunkte und dienen dem sicheren HTTP-Zugriff (HTTPS), der Ihnen eine sichere Kommunikationssitzung mit Ihren Speicher- oder Datenverarbeitungs-Instanzen innerhalb von AWS ermöglicht. Um Kunden mit FIPS 140-2-Anforderungen zu unterstützen, werden die Amazon Virtual Private Cloud (VPN)-Endpunkte und die SSL-terminierenden Lastverteiler in der AWS GovCloud (USA) mithilfe von nach FIPS 140-2 Level 2 validierter Hardware betrieben.

Zusätzlich hat AWS Netzwerkgeräte implementiert, die für die Verwaltung der Schnittstellenkommunikation mit Internet Service Providern (ISPs, Internetdienstanbietern) vorgesehen sind. AWS verwendet eine redundante Verbindung zu mehr als einem Kommunikationsdienst an jeder mit dem Internet verbundene Stelle des AWS-Netzwerks. Jede dieser Verbindungen verfügt über eigene Netzwerkgeräte.

Übertragungsschutz

Sie können eine Verbindung mit einem AWS-Zugriffspunkt über HTTP oder HTTPS mit einem Secure Sockets Layer (SSL) erstellen, einem Verschlüsselungsprotokoll, das entwickelt wurde, um vor Abhörangriffen, Datenmanipulation oder Fälschung von Nachrichten zu schützen.

Für Kunden, die zusätzliche Ebenen an Netzwerksicherheit benötigen, bietet AWS die Amazon Virtual Private Cloud (VPC), die ein privates Subnetz innerhalb der AWS-Cloud bereitstellt, und die Verwendung eines IPsec Virtual Private Network (VPN)-Geräts ermöglicht, das einen verschlüsselten Tunnel zwischen dem Amazon-VPC und Ihrem Rechenzentrum herstellen kann. Weitere Informationen zu den Konfigurationsoptionen von VPC erhalten Sie im unten stehenden Abschnitt Amazon Virtual Private Cloud (Amazon VPC)-Sicherheit.

Unternehmenstrennung bei Amazon

Für den logischen Zugriff wird das AWS-Produktivnetzwerk vom Amazon-Unternehmensnetzwerk durch einen Reihe von Maßnahmen der Netzwerksicherheit- und -trennung abgegrenzt. AWS-Entwickler und Administratoren des Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, um diese zu verwalten, müssen ausdrücklich Zugriff über das AWS-Ticketing-System beantragen. Alle Anträge werden vom entsprechenden Service-Owner geprüft und genehmigt.

Zugelassenes AWS-Personal stellt dann eine Verbindung zum AWS-Netzwerk durch einen Bastions-Host her, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten einschränkt und alle Aktivitäten zur Sicherheitsüberprüfung protokolliert. Der Zugriff auf Bastions-Hosts erfordert für alle Benutzerkonten auf dem Host eine Authentifizierung durch einen öffentlichen SSH-Schlüssel. Weitere Informationen über den logischen Zugriff für AWS-Entwickler und -Administratoren finden Sie nachfolgend unter *AWS-Zugriff*.

Fehlertolerantes Design

Die Infrastruktur von Amazon weist ein hohes Maß an Verfügbarkeit auf und bietet Ihnen die Möglichkeit zur Bereitstellung einer stabilen IT-Architektur. AWS hat seine Systeme so entwickelt, dass sie System- oder Hardwareausfälle tolerieren, und Kunden nur minimale Auswirkungen zu spüren bekommen.

Rechenzentren werden in Clustern in verschiedenen *Regionen* der Welt errichtet. Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen.

AWS bietet Ihnen die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich in z.B. Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonenkategorisierungen). Zusätzlich zum Einsatz einer eigenständigen unterbrechungsfreien Stromversorgung und von Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden.

Sie sollten die Architektur Ihrer AWS-Nutzung so erstellen, dass sie mehrere Regionen und Availability Zones umfasst. Durch das Verteilen von Anwendungen über mehrere Availability Zones bleibt die Architektur bei den meisten Ausfallszenarien, einschließlich Naturkatastrophen oder Systemausfällen, stabil. Sie sollten jedoch standortabhängige Datenschutz- und Compliance-Anforderungen beachten, wie die EU-Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Daten zwischen Regionen werden nicht repliziert, außer dies wird proaktiv durch den Kunden durchgeführt. Kunden, die derartigen Anforderung an Datenplatzierung und Datenschutz unterliegen, richtlinienkonforme Umgebungen erstellen. Es ist zu beachten, dass sämtliche Kommunikation zwischen Regionen über die öffentliche Internetinfrastruktur erfolgt; daher sollten zum Schutz sensibler Daten entsprechende Verschlüsselungsmethoden angewendet werden.

Derzeit gibt es zehn Regionen: USA-Ost (Northern Virginia), USA-West (Oregon), USA-West (Nordkalifornien), AWS GovCloud (USA), EU (Irland), Asien-Pazifik (Singapur), Asien-Pazifik (Tokio), Asien-Pazifik (Sydney), Südamerika (São Paulo) und China (Peking).

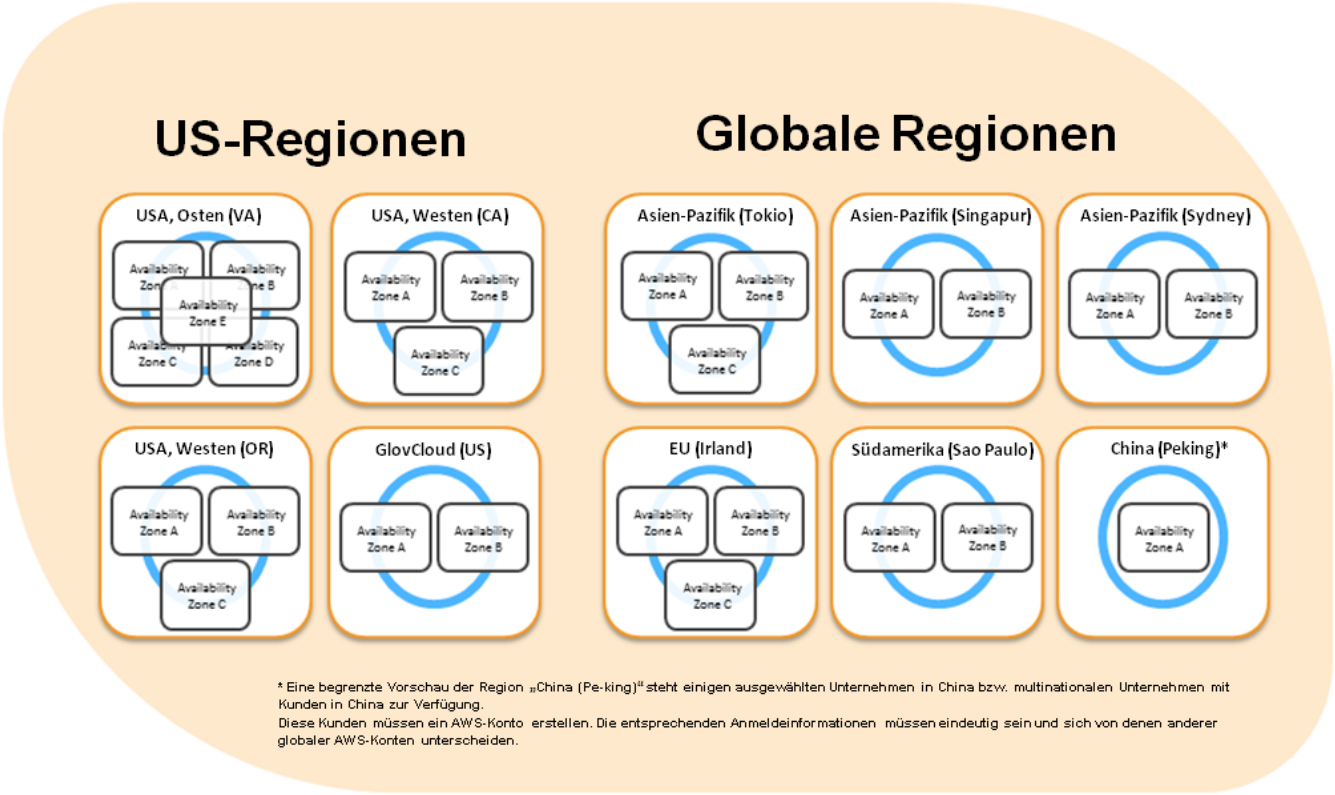


Abbildung 1: Regionen und Availability Zones

Beachten Sie, dass sich die Anzahl der Availability Zones ändern kann.

AWS GovCloud (USA) ist eine isolierte AWS-Region, die entwickelt wurde, damit US-Regierungsbehörden und Kunden Aufgaben in die Cloud verschieben können und bei der Erfüllung bestimmter behördlicher und Compliance-Anforderungen unterstützt werden. Mithilfe des AWS GovCloud (USA)-Frameworks können US-Regierungsbehörden und ihre Auftragnehmer die Anforderungen der U.S. International Traffic in Arms Regulations (ITAR) und des Federal Risk and Authorization Management Program (FedRAMP) erfüllen. AWS GovCloud (USA) hat eine „Agency Authorization to Operate (ATO)" vom US-Gesundheitsministerium erhalten und verwendet eine von FedRAMP autorisierte Third Party Assessment Organization (3PAO) für eine Reihe von AWS-Services.

Die AWS GovCloud (USA)-Region bietet dasselbe fehlertolerante Design wie andere Regionen mit zwei Availability Zones. Außerdem ist die AWS GovCloud (USA)-Region standardmäßig immer ein AWS Virtual Private Cloud (VPC)-Service, welcher ein abgetrennter Teil der AWS-Cloud ist und in dem Amazon EC2-Instanzen gestartet werden können, die private Adressen (RFC 1918) haben. Weitere Informationen über GovCloud erhalten Sie auf der AWS-Website: http://aws.amazon.com/govcloud-us/

Netzwerküberwachung und -schutz

AWS verwendet eine Vielzahl an automatisierten Überwachungssystemen, um ein hohes Maß an Leistung und Verfügbarkeit des Services zu bieten. AWS-Überwachungs-Tools wurden entwickelt, um ungewöhnliche oder unautorisierte Aktivitäten und Betriebsbedingungen an ein- und ausgehenden Kommunikationspunkten zu erkennen. Diese Werkzeuge überwachen Server- und Netzwerkauslastung, Port-Scanning-Aktivitäten, Anwendungsauslastung und unautorisierte Eindringversuche. Die Werkzeuge können benutzerdefinierte Schwellenwerte für Leistungsmetriken bei ungewöhnlichen Aktivitäten festlegen.

Systeme innerhalb von AWS sind umfassend zur Überwachung von wichtigen Betriebsmetriken ausgestattet. Alarme sind so konfiguriert, dass sie automatisch das Betriebs- und Verwaltungspersonal benachrichtigen, wenn die Frühwarnschwellen von wichtigen Betriebsmetriken überschritten werden. Ein Rufbereitschaftsplan ist vorhanden, damit jederzeit Personal verfügbar ist, um auf Betriebsprobleme zu reagieren. Dazu gehört ein Pager-System, das Alarme schnell und zuverlässig an das Betriebspersonal kommuniziert.

Vorfälle werden dokumentiert, um die Mitarbeiter des Betriebspersonals bei der Behandlung von Störfällen oder Problemen zu unterstützen und sie darüber zu informieren. Wenn die Lösung eines Problems eine Zusammenarbeit des Personals erfordert, kommt ein Konferenzsystem zum Einsatz, das Kommunikations- und Protokollierungsfunktionen unterstützt. Geschulte Konferenzleiter unterstützen Kommunikation und Fortschritt bei der Behandlung von Betriebsproblemen, die eine Zusammenarbeit erfordern. Nach jedem größeren Betriebsproblem werden Nachbesprechungen einberufen, und zwar unabhängig davon, ob das Problem externe Beeinträchtigungen verursacht hat. Dokumente zu den Fehlerursachen werden ausgearbeitet, sodass die zugrunde liegende Ursache erfasst wird und in Zukunft Präventivmaßnahmen ergriffen werden können. Die Implementierung von Präventivmaßnahmen wird bei den wöchentlichen Betriebsversammlungen nachverfolgt.

AWS-Sicherheitsüberwachungs-Werkzeuge sind bei der Erkennung mehrerer Arten von Denial of Service (DoS)-Angriffen behilflich, einschließlich Distributed Flooding und Software-/Logic-Angriffe. Bei Erkennung von DoS-Angriffen wird der AWS-Vorfallreaktionsprozess gestartet. Zusätzlich zu den DoS-Präventions-Tools schützen redundante Telekommunikationsanbieter in den einzelnen Regionen sowie zusätzliche Kapazitäten vor dem Risiko von DoS-Angriffen.

Das AWS-Netzwerk bietet maßgeblichen Schutz vor gängigen Netzwerksicherheitsproblemen und Sie können weitere Schutzmaßnahmen implementieren. Im Folgenden sind einige Beispiele aufgeführt:

- **Distributed Denial Of Service (DDoS)-Angriffe:** Die API-Endpunkte in AWS werden auf einer großen, das gesamte Internet umspannenden, hochkarätigen Infrastruktur betrieben, in das die Fachkompetenz von Ingenieuren eingeflossen ist, die Amazon zum weltweit größten Online-Händler gemacht hat. Es werden proprietäre DDoS-Risikovermeidungstechniken angewendet. Außerdem sind die Netzwerke von AWS mehrfach über eine Reihe von Anbietern vernetzt, um einen vielfältigen Internetzugriff zu ermöglichen.
- **Man in the Middle (MITM)-Angriffe:** Alle AWS-APIs sind über SSL-geschützte Endpunkte verfügbar, die eine Serverauthentifizierung bereitstellen. Amazon EC2-AMIs generieren automatisch neue SSH-Hostzertifikate beim ersten Systemstart und protokollieren sie dann in der Konsole der Instanz. Sie können dann die sicheren APIs verwenden, um die Konsole aufzurufen und auf die Hostzertifikate vor ihrer ersten Protokollierung in die Instanz zugreifen. Wir empfehlen, SSL für alle Interaktionen mit AWS zu verwenden.
- **IP Spoofing:** Amazon EC2-Instanzen können keinen manipulierten („spoofed“) Netzwerkverkehr senden. Die von AWS gesteuerte, hostbasierte Firewall-Infrastruktur gestattet einer Instanz nicht, Datenverkehr mit einer anderen Quell-IP oder MAC-Adresse als der eigenen zu senden.

- **Port-Scanning:** Unautorisierte Port-Scans von Amazon EC2-Kunden sind ein Verstoß gegen die AWS Acceptable Use Policy. Verstöße gegen die AWS Acceptable Use Policy werden ernst genommen und jeder gemeldete Verstoß wird untersucht. Kunden können einen Verdacht auf Missbrauch über die auf unserer Website aufgeführten Kontakte melden: http://aws.amazon.com/contact-us/report-abuse/. Wenn AWS unautorisiertes Port-Scanning erkennt, wird dieses gestoppt und blockiert. Port-Scans von Amazon EC2-Instanzen sind im Allgemeinen ineffektiv, da standardmäßig alle eingehenden Ports der Amazon EC2-Instanzen geschlossen sind und nur von Ihnen geöffnet werden können. Eine strenge Verwaltung von Sicherheitsgruppen kann die Bedrohung von Port-Scans weiter vermindern. Wenn Sie die Sicherheitsgruppe so konfigurieren, dass sie Datenverkehr von einer beliebigen Quelle zu einem bestimmten Port zulässt, wird dieser Port anfällig für Port-Scans. In diesen Fällen müssen Sie entsprechende Sicherheitsmaßnahmen treffen, um Überwachungsdienste, die möglicherweise für deren Anwendung wesentlich sind, vor der Erkennung durch einen unautorisierten Port-Scan zu schützen. Beispielsweise muss ein Webserver offensichtlich den Port 80(HTTP) für die Außenwelt geöffnet haben und der Administrator dieses Servers ist für die Sicherheit der HTTP-Serversoftware, wie zum Beispiel Apache, zuständig. Möglicherweise müssen Sie eine Genehmigung zur Durchführung von Schwachstellen-Scans anfordern, um Ihre spezifischen Compliance-Anforderungen zu erfüllen. Diese Scans müssen auf Ihre eigenen Instanzen beschränkt sein und dürfen nicht gegen die AWS Acceptable Use Policy verstoßen. Eine Vorabgenehmigung für diese Arten von Scans kann durch Einreichen einer Anfrage über folgende Website angefordert werden: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest
- **Packet-Sniffing durch andere Kunden:** Eine virtuelle Instanz, die im Promiscuous-Modus ausgeführt wird, kann keinen Datenverkehr empfangen oder „sniffen“, der für eine andere virtuelle Instanz bestimmt ist. Obwohl Sie Schnittstellen in den Promiscuous-Modus versetzen können, liefert der Hypervisor keinen Datenverkehr, der nicht an sie adressiert ist. Nicht einmal zwei virtuelle Instanzen, deren Besitzer derselbe Kunde ist und die sich auf demselben physischen Host befinden, können ihren Datenverkehr gegenseitig abhören. Angriffe wie ARP-Cache-Poisoning funktionieren nicht innerhalb von Amazon EC2 und Amazon VPC. Auch wenn Amazon EC2 weitreichenden Schutz davor bietet, dass ein Kunde unabsichtlich oder absichtlich die Daten eines anderen aufruft, sollten Sie sensiblen Datenverkehr standardmäßig verschlüsseln.

Zusätzlich zur Überwachung werden regelmäßige Schwachstellen-Scans mit verschiedenen Tools auf dem Host-Betriebssystem, der Webanwendung und den Datenbanken in der AWS-Umgebung durchgeführt. AWS-Sicherheitsteams abonnieren des Weiteren Newsfeeds zu den entsprechenden Anbieterfehlern und überwachen proaktiv die Websites der Anbieter und andere relevante Quellen auf neue Patches. AWS-Kunden können ebenfalls Probleme an AWS über die Website „Berichte zu Schwachstellen“ melden: http://aws.amazon.com/security/vulnerability-reporting/

AWS-Zugriff

Das AWS-Produktivnetzwerk ist vom Amazon-Unternehmensnetzwerk getrennt und erfordert separate Anmeldeinformationen für den logischen Zugriff. Das Amazon-Unternehmensnetzwerk verwendet Benutzer-IDs, Passwörter und Kerberos, während das AWS-Produktivnetzwerk eine SSH public-key Authentifizierung mit einem Bastions-Host erfordert.

AWS-Entwickler und Administratoren des Amazon-Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, müssen ausdrücklich Zugriff über das AWS-Zugriffsverwaltungssystem beantragen. Alle Anträge werden von der jeweils zuständigen Person geprüft und genehmigt.

Kontoüberprüfung und -überwachung

Konten werden alle 90 Tage überprüft; wenn die Freigabe nicht ausdrücklich erneut erteilt wird, wird der Zugriff auf die Ressource automatisch gesperrt. Der Zugriff wird ebenfalls automatisch gesperrt, wenn ein Mitarbeiterdatensatz im Personalverwaltungssystem von Amazon geschlossen wird. Windows- und UNIX-Konten werden deaktiviert und das Zugriffsverwaltungssystem von Amazon entfernt den Benutzer aus allen Systemen.

Anforderungen für Zugriffsänderungen werden im Auditprotokoll des Zugriffsverwaltungssystems von Amazon erfasst. Wenn sich die Funktion eines Mitarbeiters ändert, muss der Fortbestand der Zugriffsrechte ausdrücklich genehmigt werden, anderenfalls wird der Zugriff automatisch gesperrt.

Hintergrundüberprüfungen

AWS hat formale Richtlinien und Verfahren erstellt, um Mindeststandards für den logischen Zugriff auf die AWS-Plattform und Infrastruktur-Hosts festzulegen. AWS führt gesetzlich zulässige Überprüfungen auf kriminelle Vergangenheit durch. Dies ist ein Bestandteil der Prüfungsprozesse vor der Einstellung eines Mitarbeiters, welche im angemessenen Verhältnis zur Position und zur Berechtigungsstufe des Mitarbeiters durchgeführt werden. Die Richtlinien bestimmen ebenfalls die funktionellen Verantwortlichkeiten für die Verwaltung von logischem Zugriff und Sicherheit.

Richtlinie zu Anmeldeinformationen

AWS-Sicherheit hat eine Richtlinie zu Anmeldeinformationen mit den erforderlichen Konfigurationen und Ablaufintervallen festgelegt. Passwörter müssen komplex sein und alle 90 Tage geändert werden.

Grundsätze für ein sicheres Design

Beim Entwicklungsprozess von AWS wurden Best Practices für die Entwicklung von sicherer Software angewendet. Sie umfassen formale Designprüfungen durch das AWS-Sicherheitsteam, Bedrohungsmodelle und die Durchführung einer Risikobewertung. Werkzeuge zur Analyse von statischem Code werden als Teil des standardmäßigen Erstellungsprozesses ausgeführt und die gesamte bereitgestellte Software wird wiederholten Penetrationstests unterzogen, welche von sorgfältig ausgewählten Branchenexperten durchgeführt werden. Unsere Prüfungen zur Bewertung des Sicherheitsrisikos beginnen während der Planungsphase und werden bis zum Start des laufenden Betriebs weitergeführt.

Änderungsverwaltung

Routinemäßige Änderungen, Änderungen aufgrund von Notfällen und Konfigurationsänderungen an der bestehenden AWS-Infrastruktur werden gemäß den Branchennormen für ähnliche Systeme autorisiert, protokolliert, getestet, genehmigt und dokumentiert. Updates der Infrastruktur von AWS werden so durchgeführt, dass die Auswirkungen auf die Kunden und deren Nutzung der Services minimal sind. AWS kommuniziert entweder per E-Mail oder über das „AWS – Service Health Dashboard“ (http://status.aws.amazon.com/) mit den Kunden, wenn die Nutzung des Services möglicherweise beeinträchtigt wird.

Software

AWS wendet einen systematischen Ansatz zur Verwaltung von Änderungen an. Änderungen, die Auswirkungen auf Kunden haben, werden gründlich überprüft, getestet, genehmigt und effizient kommuniziert. Der Änderungsverwaltungsprozess von AWS wurde so entwickelt, dass unbeabsichtigte Service-Unterbrechungen vermeiden und die Integrität des Services gegenüber dem Kunden gewahrt wird. In Produktionsumgebungen bereitgestellte Änderungen werden wie folgt behandelt:

- Überprüfung: Es ist eine Überprüfung der technischen Aspekte einer Änderung durch Kollegen erforderlich.
- Tests: Angewendete Änderungen werden getestet, um sicherzustellen, dass sie erwartungsgemäß funktionieren und die Leistung nicht beeinträchtigen.
- Genehmigung: Alle Änderungen müssen autorisiert werden, um den erforderlichen Überblick sowie Kenntnisse über Auswirkungen auf das Unternehmen zu erhalten.

Änderungen werden normalerweise phasenweise in die Produktion eingeführt, beginnend mit den Bereichen, in denen sie die geringsten Auswirkungen haben. Bereitstellungen werden an einem Einzelsystem getestet und sorgfältig überwacht, damit Beeinträchtigungen ausgewertet werden können. Service-Owner verfügen über eine Reihe konfigurierbarer Metriken zum Messen der Funktionsfähigkeit der Upstream-Abhängigkeiten des Services. Diese Metriken werden sorgfältig durch Schwellenwerte und Alarme überwacht. Rollback-Verfahren werden im Change Management-Ticket (CM, Änderungsverwaltung) dokumentiert.

Wenn möglich, werden Änderungen während regelmäßiger Änderungsfenster geplant. Notfalländerungen an Produktionssystemen, die Abweichungen von den Standardverfahren der Änderungsverwaltung erfordern, werden einem Vorfall zugeordnet und dementsprechend protokolliert und genehmigt.

AWS führt in regelmäßigen Abständen Selbstüberprüfungen von wichtigen Services durch, um die Qualität zu überwachen, hohe Standards aufrechtzuerhalten und eine fortlaufende Verbesserung des Änderungsverwaltungsprozesses zu ermöglichen. Es werden sämtliche Ausnahmen analysiert, um die zugrunde liegende Ursache zu ermitteln, und es werden die entsprechenden Maßnahmen ergriffen, damit die Änderung die Compliance-Anforderungen erfüllt. Falls erforderlich wird ein Rollback der Änderung durchgeführt. Es werden dann Maßnahmen ergriffen, um den Prozess oder das Problem zu behandeln bzw. wiederherzustellen.

Infrastruktur

Das Amazon-Team für Unternehmensanwendungen entwickelt und verwaltet Software, um IT-Prozesse für UNIX-/Linux-Hosts in den Bereichen Bereitstellung von Drittanbieter-Software, intern entwickelte Software und Konfigurationsverwaltung zu automatisieren. Das Infrastrukturteam unterhält und betreibt das Framework der UNIX-/Linux-Konfigurationsverwaltung und widmet sich dabei der Hardware-Skalierbarkeit, Verfügbarkeit, Überprüfung und Sicherheitsverwaltung. Durch die zentrale Verwaltung von Hosts mithilfe von automatisierten Prozessen zur Änderungsverwaltung kann Amazon seine Ziele der hohen Verfügbarkeit, Reproduzierbarkeit, Skalierbarkeit, Sicherheit und Notfallwiederherstellung erreichen. System- und Netzwerkingenieure überwachen fortlaufend den Status dieser automatisierten Tools und überprüfen dabei Berichte, um auf Hosts zu reagieren, die ihre Konfiguration und Software nicht erhalten haben oder nicht aktualisieren konnten.

Intern entwickelte Software zur Konfigurationsverwaltung wird installiert, wenn neue Hardware bereitgestellt wird. Diese Tools werden auf allen UNIX-Hosts ausgeführt. Dadurch wird überprüft, ob sie angemessen konfiguriert sind und ob die Software den Standards entsprechend installiert ist, die dem Host aufgrund seiner Rolle zugewiesen wurden. Diese Software zur Konfigurationsverwaltung unterstützt ebenfalls die regelmäßige Aktualisierung von Paketen, die bereits auf dem Host installiert sind. Nur zugelassenes Personal, das über den Berechtigungs-Service autorisiert wurde, kann sich an den Zentralservern zur Konfigurationsverwaltung anmelden.

Sicherheitsfunktionen von AWS-Konten

AWS bietet eine Reihe von Möglichkeiten zur Identifizierung und zum sicheren Zugriff auf Ihr AWS-Konto. Eine vollständige Liste der von AWS unterstützten Anmeldeinformationen befindet sich auf der Seite mit den Sicherheitsanmeldeinformationen unter „Mein Konto“. AWS bietet außerdem zusätzliche Sicherheitsoptionen, durch die Sie Ihr AWS-Konto weiter schützen und den Zugriff steuern können: AWS Identity and Access Management (AWS IAM), Schlüsselverwaltung und -rotation, temporäre Sicherheitsanmeldeinformationen und Multi-Factor Authentication (MFA).

AWS Identity and Access Management (AWS IAM)

IAM AWS ermöglicht die Erstellung mehrerer Benutzer und die Verwaltung der Berechtigungen der einzelnen Benutzer innerhalb Ihres AWS-Kontos. Ein Benutzer ist eine Identität (innerhalb eines AWS-Kontos) mit eindeutigen Sicherheitsanmeldeinformationen, die zum Zugriff auf AWS-Services verwendet werden können. Durch AWS IAM ist das Teilen von Passwörtern oder Schlüsseln nicht mehr erforderlich und es ist einfach, den Zugriff eines Benutzers je nach Bedarf zu aktivieren oder zu deaktivieren.

AWS IAM ermöglicht die Implementierung von Best Practices für die Sicherheit, wie das Prinzip der geringsten Rechte, bei dem jeder Benutzer innerhalb Ihres AWS-Kontos eindeutige Anmeldeinformationen erhält und Benutzer nur zur Durchführung ihrer Arbeit eine Berechtigung zum Zugriff auf AWS-Services und erforderliche Ressourcen erhalten. AWS IAM ist standardmäßig sicher und neue Benutzer haben keinen Zugriff auf AWS, bis die Berechtigungen ausdrücklich erteilt wurden.

AWS IAM ist auch in AWS Marketplace integriert, sodass Sie steuern können, wer in Ihrem Unternehmen die von Marketplace angebotene Software und die angebotenen Services abonnieren kann. Da das Abonnieren bestimmter Software in Marketplace eine EC2-Instanz zur Ausführung der Software startet, ist dies eine wichtige Zugriffssteuerungsfunktion. Durch die Verwendung von AWS IAM zur Kontrolle des Zugriffs auf AWS Marketplace können AWS-Kontoinhaber die Nutzungs- und Software-Kosten außerdem bis ins Detail steuern.

Mit AWS IAM können Sie die Verwendung Ihrer Anmeldeinformationen für AWS-Konten minimieren. Wenn Sie AWS IAM-Benutzerkonten erstellen, sollten alle Interaktionen mit AWS-Services und -Ressourcen unter Verwendung von Sicherheitsanmeldeinformationen für AWS IAM-Benutzer erfolgen. Weitere Informationen über AWS IAM erhalten Sie auf der AWS-Website: http://aws.amazon.com/iam/

Rollen

Eine *IAM-Rolle* verwendet temporäre Sicherheitsanmeldeinformationen, damit Sie den Zugriff an Benutzer oder Services delegieren können, die normalerweise keinen Zugriff auf Ihre AWS-Ressourcen haben. Eine Rolle ist ein Satz von Berechtigungen für bestimmte AWS-Ressourcen, wobei diese Berechtigungen nicht mit einem bestimmten IAM-Benutzer oder einer bestimmten IAM-Gruppe verknüpft sind. Eine autorisierte Entität (z. B. Mobilbenutzer, EC2-Instanz) nimmt eine Rolle an und erhält temporäre Sicherheitsanmeldeinformationen zur Authentifizierung für die in der Rolle definierten Ressourcen. Temporäre Sicherheitsanmeldeinformationen bieten verbesserte Sicherheit aufgrund ihrer kurzen Lebensdauer (die Standardlebensdauer beträgt zwölf Stunden) und der Tatsache, dass sie nach Ablauf nicht mehr wiederverwendet werden können. Dies kann besonders nützlich sein, wenn in bestimmten Situationen eingeschränkter, kontrollierter Zugriff erteilt werden muss.

- **Zugriff für verbundene(nicht AWS) Benutzer:** Verbundene (federated) Benutzer sind Benutzer (oder Anwendungen), die über keine AWS-Konten verfügen. Mit Rollen können Sie ihnen für begrenzte Zeit Zugriff auf Ihre AWS-Ressourcen gewähren. Dies ist hilfreich, wenn Sie nicht AWS-Benutzern Zugriff gewähren, die Sie mit einem externen Service authentifizieren können, z. B. Microsoft Active Directory, LDAP oder Kerberos. Die temporären AWS-Anmeldeinformationen werden mit Rollen verwendet und stellen einen Identitätsverbund zwischen AWS- und nicht AWS-Benutzern in Ihrem Unternehmensidentitäts- und Autorisierungssystem bereit.

  Wenn Ihr Unternehmen SAML 2.0 (Security Assertion Markup Language 2.0) unterstützt, können Sie eine Vertrauensbasis zwischen Ihrem Unternehmen als Identitätsanbieter (IdP, Identidy Provider) und anderen Unternehmen schaffen, die als Service-Anbieter fungieren. Sie können AWS als Service-Anbieter konfigurieren und Ihren Benutzern mithilfe von SAML ein verbundenes Single-Sign-on (SSO) auf die AWS Management Console oder verbundenen Zugriff zum Aufrufen der AWS-APIs zur Verfügung stellen.

  Rollen sind ebenfalls hilfreich, wenn Sie eine mobile oder webbasierte Anwendung erstellen, die auf AWS-Ressourcen zugreift. AWS-Ressourcen benötigen Sicherheitsanmeldeinformationen für Programmanforderungen. Sie sollten jedoch keine Langzeit-Sicherheitsanmeldeinformationen in Ihre Anwendung integrieren, da die Benutzer der Anwendung auf diese zugreifen können und eine Rotation schwierig sein kann. Stattdessen sollten Sie Benutzern gestatten, sich in Ihrer Anwendung mit dem Login von Amazon, Facebook oder Google anzumelden und dann mithilfe dieser Authentifizierungsinformationen eine Rolle übernehmen und temporäre Sicherheitsanmeldeinformationen erhalten.
- **Kontoübergreifender Zugriff:** Für Unternehmen, die mehrere AWS-Konten zur Verwaltung ihrer Ressourcen verwenden, können Sie Rollen einrichten, um Benutzern, die über Berechtigungen in einem Konto verfügen, Zugriff auf die Ressourcen in einem anderen Konto zu gewähren. Für Unternehmen mit Personal, das nur selten Zugriff auf die Ressourcen in einem anderen Konto benötigt, gewährleistet die Verwendung von Rollen, dass die Anmeldeinformationen nur temporär und bei Bedarf bereitgestellt werden.
- **Anwendungen, die auf Amazon EC2-Instanzen ausgeführt werden und auf AWS-Ressourcen zugreifen müssen:** Wenn eine Anwendung auf einer Amazon EC2-Instanz ausgeführt wird und Anforderungen nach AWS-Ressourcen wie z.B. Amazon S3-Buckets oder eine Amazon DynamoDB-Tabelle stellen muss, benötigt sie Sicherheitsanmeldeinformationen. Die Verwendung von Rollen statt der Erstellung eigener IAM-Konten für jede Anwendung auf jeder Instanz kann für Kunden eine beträchtliche Zeitersparnis bedeuten, wenn sie eine große Anzahl von Instanzen oder eine dynamisch skalierte Flotte verwalten, die AWS-Auto Scaling verwendet.

Temporäre Anmeldeinformationen bestehen aus einem Sicherheitstoken, einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Um einem Benutzer temporären Zugriff auf bestimmte Ressourcen zu gewähren, teilen Sie diesem temporäre Sicherheitsanmeldeinformationen zu. Wenn der Benutzer Ihre Ressourcen aufruft, übergibt er das Token und die Zugriffsschlüssel-ID und unterzeichnet die Anforderung mit dem geheimen Zugriffsschlüssel. Das Token funktioniert nicht mit anderen Zugriffsschlüsseln. Wie der Benutzer das Token übergibt hängt von der API und der Version des AWS-Produkts ab, das der Benutzer aufruft. Weitere Informationen über temporäre Sicherheitsanmeldeinformationen erhalten Sie auf der AWS-Website: http://docs.amazonwebservices.com/STS

Die Verwendung von temporären Sicherheitsanmeldeinformationen bedeutet zusätzliche Sicherheit, da Sie keine Langzeit-Anmeldeinformationen für temporäre Benutzer verwalten oder verteilen müssen. Außerdem werden temporäre Anmeldeinformationen automatisch in die Ziel-Instanz geladen, sodass sie nicht auf eine unsichere Art eingebettet werden müssen, zum Beispiel im Code. Temporäre Anmeldeinformationen rotieren oder ändern sich mehrmals täglich automatisch, ohne dass Sie etwas unternehmen müssen, und sie sind standardmäßig sicher gespeichert.

Weitere Informationen über die Verwendung von IAM-Rollen zur automatischen Bereitstellung von Schlüsseln auf EC2-Instanzen finden Sie in der Anleitung *Verwendung von IAM* auf der AWS-Website: http://docs.amazonwebservices.com/IAM

AWS Multi-Factor Authentication (AWS MFA)

AWS Multi-Factor Authentication (AWS MFA) ist eine zusätzliche Sicherheitsschicht für den Zugriff auf AWS-Services. Wenn Sie diese optionale Funktion aktivieren, müssen Sie zusätzlich zu den standardmäßigen Anmeldeinformationen für Benutzername und Passwort einen sechsstelligen Einmal-Code eingeben, bevor Zugriff auf Ihre AWS-Kontoeinstellungen oder AWS-Services und -Ressourcen gewährt wird. Sie erhalten diesen Einmal-Code von einem Authentifizierungsgerät, das sich physisch in Ihrem Besitz befindet. Dies wird Multi-Factor Authentication genannt, da vor Gewährung des Zugriffs mehr als ein Authentifizierungsfaktor überprüft wird: ein Passwort (etwas, das Sie wissen) und der genaue Code von Ihrem Authentifizierungsgerät (etwas, das Sie besitzen). Sie können MFA-Geräte sowohl für Ihr AWS-Konto als auch für Benutzer aktivieren, die Sie mit AWS IAM in Ihrem AWS-Konto erstellt haben. Des Weiteren fügen Sie MFA-Schutz für den kontoübergreifenden Zugriff auf AWS-Konten hinzu. Dies ist erforderlich, wenn Sie einem Benutzer, den Sie in einem AWS-Konto erstellt haben, die Verwendung einer IAM-Rolle zum Zugriff auf die Ressourcen eines anderen AWS-Kontos gestatten möchten. Sie können als weitere Sicherheitsebene einrichten, dass der Benutzer vor Annahme der Rolle MFA verwenden muss.

AWS MFA unterstützt die Verwendung von Hardware-Token und virtuellen MFA-Geräten. Virtuelle MFA-Geräte verwenden dieselben Protokolle wie physische MFA-Geräte, können jedoch auf jedem mobilen Hardware-Gerät ausgeführt werden, einschließlich einem Smartphone. Ein virtuelles MFA-Gerät bedient sich einer Software-Anwendung, die dem Time-Based One-Time Password (TOTP)-Standard entsprechende sechsstellige Authentifizierungscodes erstellt, wie in RFC 6238 beschrieben. Die meisten virtuellen MFA-Anwendungen ermöglichen das Hosten von mehr als einem virtuellen MFA-Gerät und sind daher praktischer als Hardware-MFA-Geräte. Sie sollten jedoch beachten, dass eine virtuelle MFA auch auf einem weniger sicheren Gerät wie einem Smartphone ausgeführt werden kann und daher möglicherweise nicht dieselbe Sicherheitsebene wie ein Hardware-MFA-Gerät bietet.

Sie können außerdem die MFA-Authentifizierung für AWS-Service-APIs erzwingen, um eine zusätzliche Schutzschicht für weitreichende oder privilegierte Aktionen wie das Beenden von Amazon EC2-Instanzen oder das Lesen sensibler, in Amazon S3 gespeicherter Daten bereitzustellen. Dies können Sie durch Hinzufügen einer MFA-Authentifizierungsanforderung zu einer IAM-Zugriffsrichtlinie einrichten. Diese Zugriffsrichtlinien können IAM-Benutzern, IAM-Gruppen oder Ressourcen angefügt werden, die Access Control Lists (ACL, Zugriffskontrolllisten) wie Amazon S3-Buckets, SQS-Warteschlangen und SNS-Themen unterstützen.

Es ist einfach, Hardware-Token von einem teilnehmenden Drittanbieter oder virtuelle MFA-Anwendungen von einem AppStore zu erhalten und über die AWS-Website für die Verwendung einrichten. Weitere Informationen über AWS MFA erhalten Sie auf der AWS-Website: http://aws.amazon.com/mfa/

Schlüsselverwaltung und Rotation

Aus denselben Gründen, weshalb Passwörter häufig geändert werden sollen, empfiehlt ASW eine regelmäßige Rotation von Zugriffsschlüsseln und Zertifikaten. Damit Sie dies ohne potenzielle Beeinträchtigung der Verfügbarkeit Ihrer Anwendung tun können, unterstützt AWS mehrere gleichzeitige Zugriffsschlüssel und Zertifikate. Mit dieser Funktion können Sie Zugriffsschlüssel und Zertifikate regelmäßig und ohne Ausfallzeiten der Anwendung in und aus dem Betrieb rotieren lassen. So kann das Risiko verlorener oder nicht mehr vertrauenswürdiger Zugriffsschlüssel und Zertifikate verringert werden. Die AWS IAM-API ermöglicht die Rotation der Zugriffsschlüssel für Ihr AWS-Konto sowie für Benutzer, die mit AWS IAM unter ihren jeweiligen AWS-Konten erstellt wurden.

AWS Trusted Advisor-Sicherheitsprüfungen

Der Kunden-Support von AWS Trusted Advisor überwacht nicht nur die Leistung und Stabilität der Cloud, sondern auch ihre Sicherheit. Trusted Advisor überprüft Ihre AWS-Umgebung und gibt Empfehlungen ab, wenn eventuell Möglichkeiten bestehen, Geld zu sparen, die Systemleistung zu verbessern oder Sicherheitslücken zu schließen. Er liefert Benachrichtigungen zu den am häufigsten auftretenden Fehlern bei Sicherheitskonfigurationen. Zu diesen Fehlern gehören das Offenlassen von Ports, das Sie anfällig für Hacking und unautorisierte Zugriffe macht, keine IAM-Konten für interne Benutzer zu erstellen, der Öffentlichkeit Zugriff zu S3-Buckets zu gestatten oder MFA nicht in Ihrem AWS-Stammkonto zu verwenden. Der AWS Trusted Advisor-Service steht AWS-Kunden zur Verfügung, die AWS Support der Kategorien Business oder Enterprise beziehen.

Servicespezifische Sicherheit bei AWS

Sicherheitsvorkehrungen sind nicht nur in alle Schichten der AWS-Infrastruktur integriert, sondern auch in alle Services, die auf dieser Infrastruktur verfügbar sind. AWS-Services wurden auf effizientes und sicheres Zusammenspiel mit allen AWS-Netzwerken und Plattformen ausgelegt. Jeder Service bietet umfassende Sicherheitsfunktionen, damit Sie sensible Daten und Anwendungen schützen können.

Sicherheit bei Amazon Elastic Compute Cloud (Amazon EC2)

Die Amazon Elastic Compute Cloud (EC2) ist eine Hauptkomponente der ‚Infrastructure as a Service' (IaaS) von Amazon, die eine dynamische Rechenkapazität mithilfe von Server-Instanzen in AWS-Rechenzentren bereitstellt. Amazon EC2 wurde entwickelt, um web-scaleComputing zu vereinfachen, indem Sie bei nur minimalem Aufwand Kapazitäten erwerben und konfigurieren können. Sie erstellen und starten *Instanzen,* welche eine Kombination aus Hard- und Software sind.

Mehrere Sicherheitsebenen

Die Sicherheit innerhalb von Amazon EC2 wird auf mehreren Ebenen bereitgestellt: dem Operating System (OS, Betriebssystem) der Host-Plattform, dem OS der virtuellen Instanz oder Gast-OS, einer Firewall und signierten API-Aufrufen. Jedes dieser Elemente baut auf den Funktionen der anderen auf. Das Ziel ist, zu verhindern, dass die in Amazon EC2 enthaltenen Daten durch unautorisierte Systeme oder Benutzer abgefangen werden. Ein weiteres Ziel ist es, Amazon EC2-Instanzen bereitzustellen, die möglichst sicher sind, ohne auf die von den Kunden geforderte Flexibilität bei der Konfiguration zu verzichten.

Hypervisor

Amazon EC2 verwendet derzeit eine hochgradig angepasste Version des Xen-Hypervisors und nutzt die Paravirtualisierung (für Linux-Gäste). Da paravirtualisierte Gäste auf den Hypervisor angewiesen sind, um Operationen zu unterstützen, die normalerweise privilegierten Zugriff erfordern, verfügt das Gast-OS über keinen höheren Zugriff auf die CPU. Die CPU bietet vier separate Privilegienmodi: 0-3, auch *Ringe genannt.* Ring 0 ist am privilegiertesten und 3 am wenigsten privilegiert. Das Host-OS wird in Ring 0 ausgeführt. Das Gast-OS wird jedoch nicht in Ring 0 ausgeführt, wie bei den meisten Betriebssystemen, sondern im weniger privilegierten Ring 1. Anwendungen werden im am wenigsten privilegierten Ring 3 ausgeführt. Diese explizite Virtualisierung der physischen Ressourcen führt zu einer klaren Trennung zwischen Gast und Hypervisor und einer zusätzlichen Sicherheitstrennung zwischen den beiden.

Instanz-Isolierung

Verschiedene Instanzen, die auf derselben physischen Maschine ausgeführt werden, sind durch den Xen-Hypervisor voneinander isoliert. Amazon ist in der Xen-Community aktiv und daher über die aktuellen Entwicklungen informiert. Außerdem befindet sich die AWS-Firewall innerhalb der Hypervisor-Ebene, nämlich zwischen der physischen Netzwerkoberfläche und der virtuellen Oberfläche der Instanz. Alle Pakete müssen diese Ebene durchlaufen. Daher haben die Nachbarn einer Instanz genauso wenig Zugriff auf diese Instanz wie beliebige andere Hosts im Internet und können daher so behandelt werden, als ob sie sich auf getrennten physischen Hosts befinden. Das physische RAM wird mithilfe ähnlicher Mechanismen getrennt.

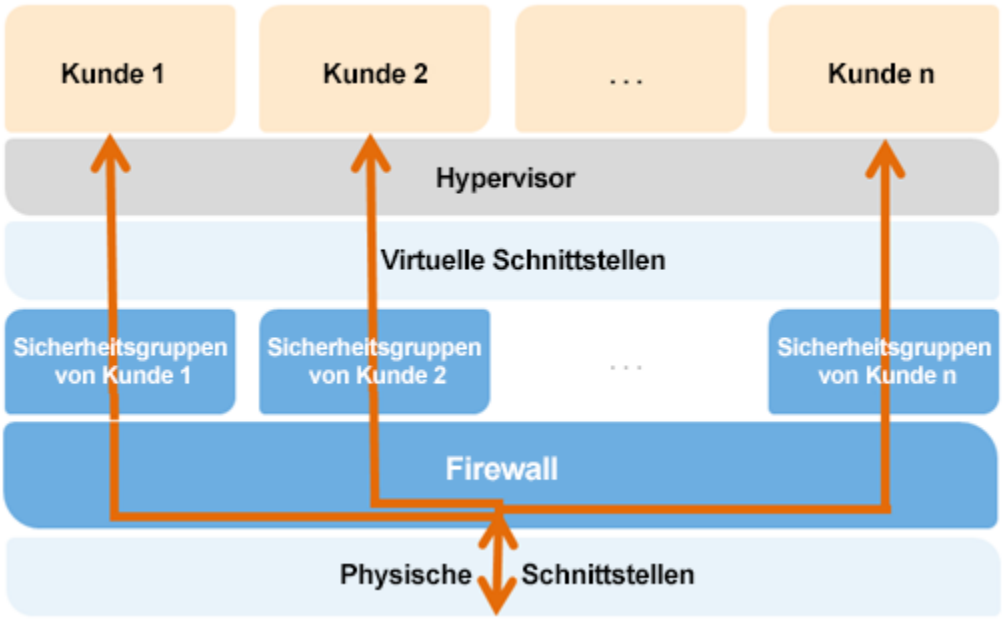


Abbildung 2: Mehrere Sicherheitsebenen von Amazon EC2

Kunden-Instanzen haben keinen Zugriff auf Rohdatenträger. Ihnen werden stattdessen virtualisierte Datenträger präsentiert. Die AWS-eigene Datenträgervirtualisierungsebene setzt jeden Speicherblock automatisch zurück, der von einem Kunden neu verwendet wird, sodass die Daten eines Kunden nie unabsichtlich einem anderen zugänglich gemacht werden. Außerdem wird Gästen zugewiesener Arbeitsspeicher vom Hypervisor gelöscht (auf Null gesetzt), wenn er wieder freigegeben wird. Der Arbeitsspeicher gelangt nicht in den Pool mit freiem Arbeitsspeicher, der für neue Zuweisungen verfügbar ist, bis die Rücksetzung des Arbeitsspeichers erfolgt ist.

AWS empfiehlt Kunden, ihre Daten durch entsprechende Maßnahmen weiter zu schützen. Eine übliche Lösung besteht darin, ein verschlüsseltes Dateisystem auf dem virtualisierten Datenträger auszuführen.

Host-Betriebssystem: Administratoren, für die eine geschäftliche Notwendigkeit zum Zugriff auf die Management-Ebene besteht, müssen die Multi-Factor Authentication verwenden, um Zugriff auf speziell erstellte Administrations-Hosts zu erlangen. Diese Administrations-Hosts sind Systeme, die speziell zum Schutz der Management-Ebene der Cloud entwickelt, erstellt, konfiguriert und gehärtet wurden. Jeder Zugriff wird protokolliert und geprüft. Sobald für einen Mitarbeiter keine geschäftliche Notwendigkeit für den Zugriff auf die Management-Ebene mehr besteht, können die Privilegien und der Zugriff auf diese Hosts und relevanten Systeme widerrufen werden.

Gastbetriebssystem: Virtuelle Instanzen werden zur Gänze von Ihnen, dem Kunden, gesteuert. Sie haben vollständigen Root-Zugriff oder administrative Kontrolle über Konten, Services und Anwendungen. AWS verfügt über keine Zugriffsrechte auf Ihre Instanzen oder das Gast-OS. AWS empfiehlt, einen Grundstock von Best Practices für die Sicherheit umzusetzen, um den Zugriff nur durch das Passwort für Ihre Gast-Betriebssysteme zu deaktivieren und den Zugriff auf Ihre Instanzen nur über eine Form der Multi-Factor Authentication zuzulassen (oder zumindest Zugriff über zertifikatbasiertes SSH Version
2). Außerdem sollten Sie einen Mechanismus zur Privilegieneskalation mit Protokollierung für jeden Benutzer einsetzen. Wenn das Gast-OS beispielsweise Linux ist, sollten Sie nach dem Härten Ihrer Instanz das zertifikatbasierte SSHv2 zum Zugriff auf die virtuelle Instanz verwenden, den Root-Fernzugriff deaktivieren, die Befehlszeilenprotokollierung verwenden und den Befehl „sudo“ für die Privilegieneskalation verwenden. Sie sollten Ihre eigenen Schlüsselpaare generieren, um zu gewährleisten, dass sie eindeutig sind und nicht an andere Kunden oder AWS weitergegeben werden.

AWS unterstützt ebenfalls das Secure Shell (SSH)-Netzwerkprotokoll, mit dem Sie sich sicher bei Ihren UNIX- bzw. Linux EC2-Instanzen anmelden können. Die bei AWS verwendete SSH-Authentifizierung erfolgt über ein öffentliches und privates Schlüsselpaar, um das Risiko von unautorisiertem Zugriff auf Ihre Instanz zu verringern. Sie können auch eine Remote-Verbindung zu Ihren Windows-Instanzen herstellen, indem Sie das Remote Desktop Protocol (RDP) und ein für Ihre Instanz generiertes RDP-Zertifikat verwenden.

Außerdem können Sie die Aktualisierungs- und Patch-Vorgänge Ihres Gast-OS einschließlich der Sicherheitsaktualisierungen steuern. Von Amazon bereitgestellte Windows- und Linux-basierte AMIs werden regelmäßig mit den neuesten Patches aktualisiert. Wenn Sie keine Daten oder Anpassungen in Ihren laufenden AMI-Instanzen von Amazon speichern müssen, können Sie die neuen Instanzen einfach mit der aktualisierten AMI neu starten. Außerdem werden Aktualisierungen für das Amazon Linux AMI über die yum-Repositorien von Amazon Linux bereitgestellt.

Firewall: Amazon EC2 bietet eine vollständige Firewall-Lösung. Diese obligatorische Firewall für eingehende Verbindungen ist standardmäßig im deny-all-Modus und Amazon EC2-Kunden müssen die Ports, die für den eingehenden Datenverkehr benötigt werden, ausdrücklich öffnen. Der Datenverkehr kann anhand eines Protokolls, eines Service-Ports und anhand der Quell-IP-Adresse (einzelne IP-Adresse oder Classless Inter-Domain Routing (CIDR)-Block) beschränkt werden.

Die Firewall kann in Gruppen konfiguriert werden, sodass verschiedene Klassen von Instanzen unterschiedlichen Regeln unterliegen. Denken Sie zum Beispiel an den Fall einer traditionellen dreistufigen Webanwendung. In der Gruppe für die Webserver wäre der Port 80 (HTTP) und/oder der Port 443 (HTTPS) offen zum Internet. In der Gruppe für die Anwendungsserver kann nur die Webservergruppe auf den Port 8000 (anwendungsspezifisch) zugreifen. In der Gruppe für die Datenbankserver wäre der Port 3306 (MySQL) nur für die Anwendungsservergruppe geöffnet. Alle drei Gruppen würden administrativen Zugriff auf Port 22 (SSH) gestatten, jedoch nur aus dem Unternehmensnetzwerk des Kunden. Hochsichere Anwendungen können mit diesem expressiven Mechanismus bereitgestellt werden. Sehen Sie sich das Diagramm unten an:

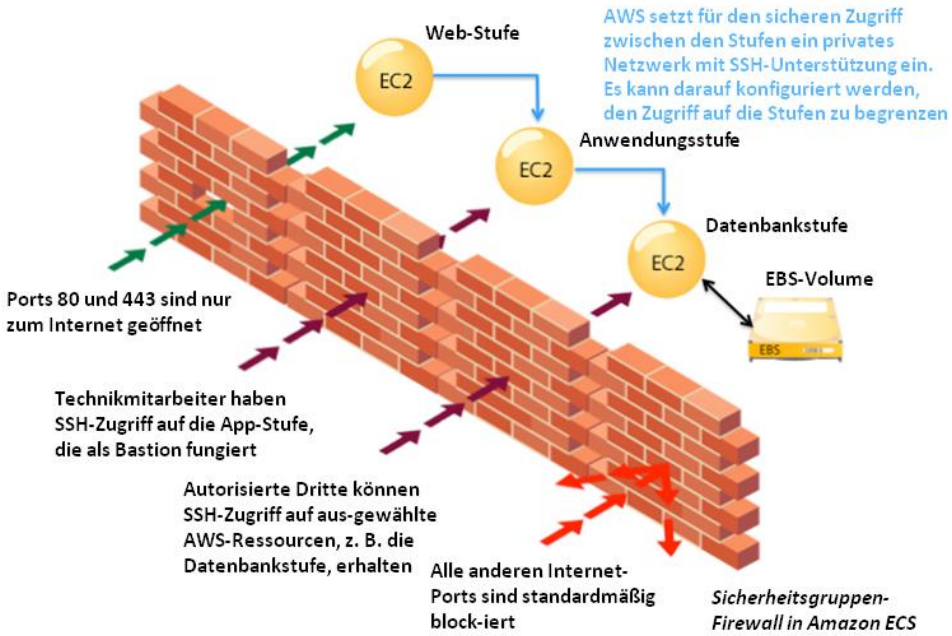


Abbildung 3: Sicherheitsgruppen-Firewall in Amazon EC2

Die Firewall wird nicht über das Gast-OS gesteuert. Sie erfordert stattdessen Ihr X.509-Zertifikat und den Schlüssel zur Autorisierung von Änderungen, wodurch eine weitere Sicherheitsschicht hinzugefügt wird. AWS unterstützt die Möglichkeit, differenzierten Zugang zu verschiedenen Verwaltungsfunktionen der Instanzen und der Firewall zu gewähren. So können Sie mehr Sicherheit durch Aufgabentrennung implementieren. Das von der Firewall geschaffene Sicherheitsniveau hängt davon ab, welche Ports Sie öffnen, wie lange und für welchen Zweck. Im Standardzustand wird sämtlicher eingehender Datenverkehr blockiert. Sie sollten bei der Erstellung und Sicherung Ihrer Anwendungen sorgfältig planen, welche Ports Sie öffnen. Eine fundierte Datenverkehrsverwaltung und Sicherheitsgestaltung sind nach wie vor für jede Instanz einzeln erforderlich. Mit AWS können Sie zusätzliche Filter pro Instanz mit hostbasierten Firewalls wie IPtables oder die Windows Firewall und VPNs anwenden. Dadurch kann der ein- und ausgehende Datenverkehr eingeschränkt werden.

API-Zugriff: API-Aufrufe, um Instanzen zu starten und zu beenden, Firewall-Parameter zu ändern und andere Funktionen auszuführen, werden alle mit Ihrem geheimen Amazon-Zugriffsschlüssel signiert. Dabei handelt es sich entweder um den geheimen Zugriffsschlüssel des AWS-Kontos oder um den geheimen Zugriffsschlüssel eines mit AWS IAM erstellten Benutzers. Ohne Zugriff auf Ihren geheimen Zugriffsschlüssel können keine Amazon EC2 API-Aufrufe in Ihrem Namen ausgeführt werden. Darüber hinaus können API-Aufrufe mit SSL verschlüsselt werden, um die Vertraulichkeit zu wahren. Amazon empfiehlt, immer SSL-geschützte API-Endpunkte zu verwenden.

Berechtigungen: Mit AWS IAM können Sie außerdem kontrollieren, welche APIs von einem Benutzer aufgerufen werden dürfen.

Sicherheit beiElastic Block Storage (Amazon EBS)

Mit Elastic Block Storage (EBS) von Amazon können Sie Speichereinheiten von 1 GB bis 1 TB erstellen, die als Festplattensubsysteme von Amazon EC2-Instanzen dienen können. Diese Speichereinheiten verhalten sich wie unformatierte Block-Geräte mit vom Nutzer vergebenen Gerätenamen und einer Block-Geräte-Oberfläche. Sie können ein Dateisystem auf den Amazon EBS-Volumes erstellen oder sie auf jede beliebige Art verwenden wie Sie ein Block-Gerät (so wie eine Festplatte) verwenden würden. Der Zugriff auf Amazon EBS-Volumes ist auf das AWS-Konto, mit dem das Volume erstellt wurde, sowie auf die Benutzer im AWS-Konto beschränkt, die mit AWS IAM erstellt wurden, sofern diesen Zugriff auf die EBS-Operationen gewährt wurde. Daher sind alle anderen AWS-Konten und Benutzer nicht berechtigt, das Volume aufzurufen oder darauf zuzugreifen.

In Amazon EBS-Volumes gespeicherte Daten werden redundant an mehreren physischen Standorten abgelegt. Dies erfolgt im Rahmen des normalen Betriebs dieser Services und ohne Zusatzkosten. Die Amazon EBS-Replik wird innerhalb derselben Availability Zone gespeichert und nicht über mehrere Zonen hinweg. Daher wird dringend empfohlen, regelmäßige Snapshots auf Amazon S3 durchzuführen, um eine langfristige Datenhaltbarkeit zu erreichen. Für Kunden, die komplexe Transaktionsdatenbanken mit EBS erstellt haben, ist es empfehlenswert, Sicherungen über das Datenbankverwaltungssystem an Amazon S3 durchzuführen, damit Prüfpunkte für verteilte Transaktionen und Logs erstellt werden können. AWS führt keine Sicherungen von Daten durch, die auf virtuellen Festplatten gehalten werden, die an laufende Instanzen auf Amazon EC2 angehängt sind.

Sie können die Snapshots von Amazon EBS-Volumes anderen AWS-Konten öffentlich zur Verfügung stellen und diese als Basis für die Erstellung Ihrer eigenen Volumes verwenden. Durch Teilen der Snapshots von Amazon EBS-Volumes erlangen andere AWS-Konten keine Berechtigung zum Ändern oder Löschen des ursprünglichen Snapshots, da diese Berechtigung ausdrücklich dem AWS-Konto vorbehalten ist, in dem das Volume erstellt wurde. Ein EBS-Snapshot ist eine Ansicht eines gesamten EBS-Volumes auf Blockebene. Beachten Sie, dass Daten, die nicht im Dateisystem auf dem Volume sichtbar sind, zum Beispiel gelöschte Dateien, auf dem EBS-Snapshot zu sehen sein können. Wenn Sie geteilte Snapshots erstellen möchten, sollten Sie dies sorgfältig tun. Wenn ein Volume sensible Daten enthalten hat oder Dateien daraus gelöscht wurden, sollte ein neues EBS-Volume erstellt werden. Die Daten, die im geteilten Snapshot enthalten sein sollen, sollten auf das neue Volume kopiert werden. Der Snapshot wird dann vom neuen Volume erstellt.

Amazon EBS-Volumes werden Ihnen als unformatierte Block-Geräte dargestellt, die vor ihrer Freigabe zur Verwendung gelöscht wurden. Das Löschen findet unmittelbar vor der erneuten Verwendung statt, damit Sie sichergehen können, dass der Löschvorgang abgeschlossen wurde. Wenn Sie Verfahren anwenden, die erfordern, dass alle Daten unter Verwendung einer bestimmten Methode gelöscht werden, wie zum Beispiel die in DoD 5220.22-M („National Industrial Security Program Operating Manual“) oder NIST 800-88 („Guidelines for Media Sanitization“) dargestellten Methoden, können Sie dies mit Amazon EBS umsetzen. Sie sollten vor der Entfernung des Volumes einen speziellen Löschvorgang durchführen, der Ihren festgelegten Anforderungen entspricht.

Die Verschlüsselung von sensiblen Daten ist im Allgemeinen Best Practice. AWS bietet die Möglichkeit zur Verschlüsselung von EBS-Volumes und deren Snapshots mit AES-256. Die Verschlüsselung findet auf den Servern statt, auf denen die EC2-Instanzen betrieben werden, so dass die Verschlüsselung der Daten auch beim Transport zwischen EC2-Instanzen und EBS Storage gewährleistet ist. Damit dies effizient und mit niedriger Latenz durchgeführt werden kann, steht die EBS-Verschlüsselungsfunktion nur auf den leistungsstärkeren Instanz-Typen von EC2 zur Verfügung (z. B. M3, C3, R3, G2).

Sicherheit bei „Amazon Elastic Load Balancing“

Amazon Elastic Load Balancing wird zur Verwaltung des Datenverkehrs auf einer Gesamtheit von Amazon EC2-Instanzen verwendet und verteilt den Datenverkehr auf Instanzen über alle Availability Zones innerhalb einer Region. Elastic Load Balancing kombiniert die Vorteile eines lokalen Load Balancers mit mehreren Sicherheitsvorteilen:

- Elastic Load Balancing übernimmt die Aufgabe der Ver- und Entschlüsselung anstelle der Amazon EC2-Instanzen und erledigt diese zentral auf dem Load Balancer.
- Elastic Load Balancing bietet Clients einen einzigen Kontaktpunkt und kann auch als erste Verteidigungslinie gegen Angriffe auf Ihr Netzwerk dienen.
- Bei Verwendung in Amazon VPC unterstützt Elastic Load Balancing die Erstellung und Verwaltung von Sicherheitsgruppen, die dem Elastic Load Balancing zugeordnet sind, um weitere Netzwerk- und Sicherheitsoptionen zur Verfügung zu stellen.
- Elastic Load Balancing unterstützt eine Ende-zu-Ende Datenverkehrsverschlüsselung mithilfe von TLS (zuvor SSL) auf Netzwerken, die sichere HTTP (HTTPS)-Verbindungen verwenden. Wenn TLS verwendet wird, kann das TLS-Serverzertifikat, das zum Terminieren von Client-Verbindungen verwendet wird, zentral auf dem Load Balancer verwaltet werden, statt auf jeder einzelnen Instanz.

HTTPS/TLS verwendet einen geheimen Langzeitschlüssel zur Generierung eines Kurzzeit-Sitzungsschlüssels, der zwischen Server und Browser verwendet wird, um die verschlüsselte Nachricht zu erstellen. Amazon Elastic Load Balancing konfiguriert Ihren Load Balancer mit einem vordefinierten Satz an Verschlüsselungsoptionen, der für die TLS-Aushandlung verwendet wird, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wird. Der vordefinierte Satz an Verschlüsselungsoptionen ist mit vielen verschiedenen Clients kompatibel und verwendet komplexe Verschlüsselungsalgorithmen. Manche Kunden haben jedoch möglicherweise Anforderungen, nur bestimmte Verschlüsselungen und Protokolle (z. B. PCI, SOX usw.) von Clients zuzulassen, um sicherzustellen, dass die Standards erfüllt werden. In diesen Fällen bietet Amazon Elastic Load Balancing Optionen zur Auswahl verschiedener TLS-Protokoll- und Verschlüsselungskonfigurationen. Sie können die Optionen zur Verschlüsselung abhängig von Ihren spezifischen Anforderungen aktivieren oder deaktivieren.

Um zu gewährleisten, dass neuere und komplexere Chiffrensammlungen bei der Einrichtung einer sicheren Verbindung verwendet werden, können Sie den Load Balancer so konfigurieren, dass dieser die letzte Entscheidung bei der Auswahl der Chiffrensammlung im Zuge der Aushandlung zwischen Client und Server trifft. Wenn die Option „Server Order Preference“ (Präferenz für die Serverreihenfolge) aktiviert ist, wählt der Load Balancer eine Chiffrensammlung basierend auf der Priorisierung des Servers und nicht der des Client. Dadurch haben Sie mehr Kontrolle über den Grad der Sicherheit von Verbindungen zwischen Clients und Ihrem Load Balancer.

Um einen noch besseren Schutz der Vertraulichkeit Ihrer Kommunikation zu gewährleisten, verwendet der Elastic Load Balancer von Amazon den Standard „Perfect Forward Secrecy“. Dieser nutzt flüchtige Sitzungsschlüssel, die nirgendwo gespeichert werden. Dadurch wird die Entschlüsselung von erfassten Daten verhindert, auch wenn der geheime Langzeitschlüssel nicht mehr vertrauenswürdig sein sollte.

Amazon Elastic Load Balancing ermöglicht Ihnen die Identifikation der ursprünglichen IP-Adresse eines Clients, der eine Verbindung mit Ihren Servern herstellt, und zwar unabhängig davon, ob Sie HTTPS- oder TCP-Load Balancing verwenden. Normalerweise gehen die Verbindungsinformationen des Client wie IP-Adresse und Port verloren, wenn Proxyanforderungen über einen Load Balancer gesendet werden. Der Grund hierfür ist, dass der Load Balancer Anforderungen für den Client an den Server sendet und es daher so aussieht, als ob Ihr Load Balancer der anfragende Client wäre. Es ist nützlich, die ursprüngliche IP-Adresse des Client zu kennen, wenn Sie weitere Informationen über Besucher Ihrer Anwendungen benötigen, um Verbindungsstatistiken zu erstellen, Datenverkehrsprotokolle zu analysieren oder Whitelists mit IP-Adressen zu verwalten.

Die Zugriffsprotokolle von Amazon Elastic Load Balancing enthalten Informationen über jede HTTP- und TCP-Anforderung, die von Ihrem Load Balancer verarbeitet wurde. Dazu gehört auch die IP-Adresse und der Port des anfragenden Clients, die Backend-IP-Adresse der Instanz, welche die Anforderung verarbeitet hat, die Größe der Anforderung und die Reaktion darauf sowie die tatsächliche Anforderungszeile des Clients (zum Beispiel: GET http://www.example.com: 80/HTTP/1.1). Alle an den Load Balancer gesendeten Anforderungen werden protokolliert. Dazu gehören auch Anfragen, die nicht bis zu den Backend-Instanzen übertragen wurden.

Sicherheit bei Auto Scaling

Mit Auto Scaling können Sie die Amazon EC2-Kapazität mithilfe definierter Bedingungen nach oben oder unten anpassen. So wird die verwendete Anzahl von Amazon EC2-Instanzen bei Nachfragespitzen automatisch nach oben angepasst, um die Leistung sicherzustellen, und bei geringer Nachfrage zur Senkung der Kosten nach unten korrigiert.

Wie bei allen AWS-Services müssen alle Anforderungen, die an die Steuer-API des Auto Scaling-Service gesendet werden, authentifiziert werden, sodass nur authentifizierte Nutzer auf den Service zugreifen und ihn verwalten können. Anforderungen werden mit einer HMAC-SHA1-Signatur versehen, die aus der Anforderung und dem privaten Schlüssel des Benutzers berechnet wird. Anmeldeinformationen an neue EC2-Instanzen zu vergeben, die mit Auto Scaling gestartet wurden, kann für große oder dynamisch skalierte Flotten von Instanzen eine Herausforderung darstellen. Um diesen Prozess zu vereinfachen, können Sie *Rollen* in IAM verwenden, sodass alle neuen Instanzen, die mit einer Rolle gestartet werden, die Anmeldeinformationen automatisch erhalten. Beim Starten einer EC2-Instanz mit einer IAM-Rolle werden der Instanz temporäre AWS-Sicherheitsanmeldeinformationen mit den von der Rolle festgelegten Berechtigungen sicher zugewiesen und der Anwendung über den Amazon EC2-Instanz-Metadaten-Service zur Verfügung gestellt. Der Metadaten-Service stellt vor Ablauf der aktuell aktiven Anmeldeinformationen neue temporäre Sicherheitsanmeldeinformationen bereit, sodass immer gültige Anmeldeinformationen für die Instanz vorliegen. Darüber hinaus werden die temporären Sicherheitsanmeldeinformationen zur Verbesserung der Sicherheit mehrmals am Tag automatisch gewechselt. Sie können den Zugriff auf den Auto Scaling-Service außerdem kontrollieren, indem Sie mit AWS IAM Benutzer unter Ihrem AWS-Konto erstellen und steuern, welche Auto Scaling APIs von diesen Benutzern aufgerufen werden dürfen. Weitere Informationen zur Verwendung von Rollen beim Starten von Instanzen erhalten Sie im Amazon EC2-Benutzerhandbuch auf der AWS-Website:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM

Amazon Virtual Private Cloud-(Amazon VPC-)Sicherheit

Normalerweise wird jeder gestarteten Amazon EC2-Instanz eine öffentliche IP-Adresse im Amazon EC2-Adressbereich per Zufallsprinzip zugewiesen. Mit Amazon VPC können Sie einen isolierten Teil der AWS Cloud erstellen und Amazon EC2-Instanzen starten, die private (RFC 1918) Adressen in dem von Ihnen ausgewählten Bereich enthalten (z. B. 10.0.0.0/16). Sie können Subnetze innerhalb der VPC definieren, indem Sie ähnliche Instanzen basierend auf dem IP-Adressbereich gruppieren und dann Routing und Sicherheit einrichten, um den ein- und ausgehenden Datenverkehr der Instanzen und Subnetze zu kontrollieren.

AWS bietet verschiedene VPC-Architekturvorlagen mit Konfigurationen, die verschiedene Stufen des öffentlichen Zugriffs bereitstellen:

- **VPC mit nur einem öffentlichen Subnetz:** Ihre Instanzen werden in einem privaten, isolierten Bereich der AWS Cloud mit direkter Internetverbindung ausgeführt. Mit Netzwerk-ACLs und Sicherheitsgruppen kann der ein- und ausgehende Netzwerkdatenverkehr Ihrer Instanzen streng kontrolliert werden.
- **VPC mit öffentlichen und privaten Subnetzen:** Diese Konfiguration enthält nicht nur ein öffentliches Subnetz, sondern außerdem ein privates Subnetz, dessen Instanzen nicht vom Internet aus kontaktierbar sind. Instanzen im privaten Subnetz können über das öffentliche Subnetz mit Network Address Translation (NAT) ausgehende Verbindungen mit dem Internet herstellen.
- **VPC mit öffentlichen und privaten Subnetzen und Hardware-VPN-Zugriff:** Diese Konfiguration umfasst zusätzlich eine IPsec VPN-Verbindung zwischen der Amazon VPC und dem Rechenzentrum, wodurch das Rechenzentrum effektiv auf die Cloud erweitert wird. Außerdem wird direkter Zugriff auf das Internet für Subnetz-Instanzen in der Amazon VPC bereitgestellt. In dieser Konfiguration installieren die Kunden ein VPN-Gerät im Rechenzentrum ihres Unternehmens hinzugefügt.
- **VPC nur mit privatem Subnetz und Hardware-VPN-Zugriff:** Die Instanzen werden in einem privaten, isolierten Bereich der AWS-Cloud mit einem privaten Subnetz ausgeführt, dessen Instanzen nicht vom Internet aus kontaktierbar sind. Sie können dieses private Subnetz über einen IPsec VPN-Tunnel mit dem Unternehmensrechenzentrum verbinden.

Außerdem können Sie zwei VPCs mithilfe einer privaten IP-Adresse verbinden. So können die Instanzen der beiden VPCs miteinander kommunizieren, als befänden sie sich in demselben Netzwerk. Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen VPCs oder mit einer VPC in einem anderen AWS-Konto innerhalb einer Region herstellen.

Zu den Sicherheitsfunktionen in der Amazon VPC zählen Sicherheitsgruppen, Netzwerk-ACLs, Routing-Tabellen und externe Gateways. Jede dieser Funktionen leistet einen Beitrag zu einem sicheren, isolierten Netzwerk, das durch selektives Aktivieren des direkten Internetzugriffs oder eine private Verbindung mit einem anderen Netzwerk erweitert werden kann. Amazon EC2-Instanzen, die mit einer Amazon VPC ausgeführt werden, profitieren von allen unten beschriebenen Vorteilen in Bezug auf Hostbetriebssystem, Gastbetriebssystem, Hypervisor, Instanz-Isolation und Schutz vor Packet Sniffing. VPC-Sicherheitsgruppen müssen jedoch speziell für Amazon VPC erstellt werden. Amazon EC2-Sicherheitsgruppen funktionieren innerhalb Ihrer Amazon VPC nicht. Außerdem verfügen Amazon VPC-Sicherheitsgruppen gegenüber Amazon EC2-Sicherheitsgruppen über zusätzliche Funktionen. Hierzu zählt beispielsweise die Fähigkeit, die Sicherheitsgruppe nach dem Starten der Instanz zu ändern, und die Fähigkeit, jedes Protokoll mit einer Standardprotokollnummer (statt nur TCP, UDP oder ICMP) anzugeben.

Jede Amazon VPC ist ein individuelles, isoliertes Netzwerk innerhalb der Cloud. Der Netzwerkdatenverkehr innerhalb jeder Amazon VPC wird von allen anderen Amazon VPCs isoliert. Beim Erstellen wählen Sie einen IP-Adressbereich für jede Amazon VPC aus. Sie können ein Internet-Gateway, ein virtuelles privates Gateway oder beides erstellen und hinzufügen, um externe Konnektivität unter Beachtung der unten aufgeführten Kontrollmechanismen herzustellen.

API-Zugriff: Aufrufe, um Amazon VPCs zu erstellen und zu löschen, Routing, Sicherheitsgruppe und Netzwerk-ACL-Parameter zu ändern und andere Funktionen auszuführen, werden alle mit Ihrem geheimen Amazon-Zugriffsschlüssel signiert. Dabei handelt es sich entweder um den geheimen Zugriffsschlüssel des AWS-Kontos oder um den Schlüssel eines mit AWS IAM erstellten Benutzers. Ohne Zugriff auf Ihren geheimen Zugriffsschlüssel können keine Amazon VPC API-Aufrufe in Ihrem Namen ausgeführt werden. Darüber hinaus können API-Aufrufe mit SSL verschlüsselt werden, um die Vertraulichkeit zu wahren. Amazon empfiehlt, immer SSL-geschützte API-Endpunkte zu verwenden. Mit AWS IAM können Kunden außerdem kontrollieren, welche APIs von einem neu erstellten Benutzer aufgerufen werden dürfen.

Subnetze und Routing-Tabellen: Sie erstellen ein oder mehrere Subnetze innerhalb jeder Amazon VPC. Jede in der Amazon VPC gestartete Instanz wird mit einem Subnetz verbunden. Herkömmliche Layer 2-Sicherheitsangriffe, einschließlich MAC-Spoofing und ARP-Spoofing, werden blockiert.

Jedes Subnetz in einer Amazon VPC ist mit einer Routing-Tabelle verknüpft und der gesamte Netzwerkdatenverkehr, der das Subnetz verlässt, wird von der Routing-Tabelle verarbeitet, um das Ziel zu bestimmen.

Firewall (Sicherheitsgruppen): Wie Amazon EC2 unterstützt Amazon VPC eine vollständige Firewall-Lösung, mit der der ein- und ausgehende Datenverkehr einer Instanz gefiltert werden kann. Mit der Standardgruppe ist eingehende Kommunikation von anderen Mitgliedern derselben Gruppe und ausgehende Kommunikation zu einem beliebigen Ziel möglich. Der Datenverkehr kann anhand eines IP-Protokolls, eines Service-Ports und der Quell-/Ziel-IP-Adresse (einzelne IP-Adresse oder Classless Inter-Domain Routing-(CIDR-)Block) beschränkt werden.

Die Firewall wird nicht über das Gastbetriebssystem kontrolliert. Sie kann nur über den Aufruf von Amazon VPC APIs geändert werden. AWS unterstützt die Möglichkeit, differenzierten Zugang zu verschiedenen Verwaltungsfunktionen der Instanzen und der Firewall zu gewähren. So können Sie mehr Sicherheit durch Aufgabentrennung implementieren. Das von der Firewall geschaffene Sicherheitsniveau hängt davon ab, welche Ports Sie öffnen, wie lange und für welchen Zweck. Eine fundierte Datenverkehrsverwaltung und Sicherheitsgestaltung sind nach wie vor für jede Instanz einzeln erforderlich. Mit AWS können Sie zusätzliche Filter pro Instanz mit hostbasierten Firewalls wie IPtables oder die Windows Firewall anwenden.

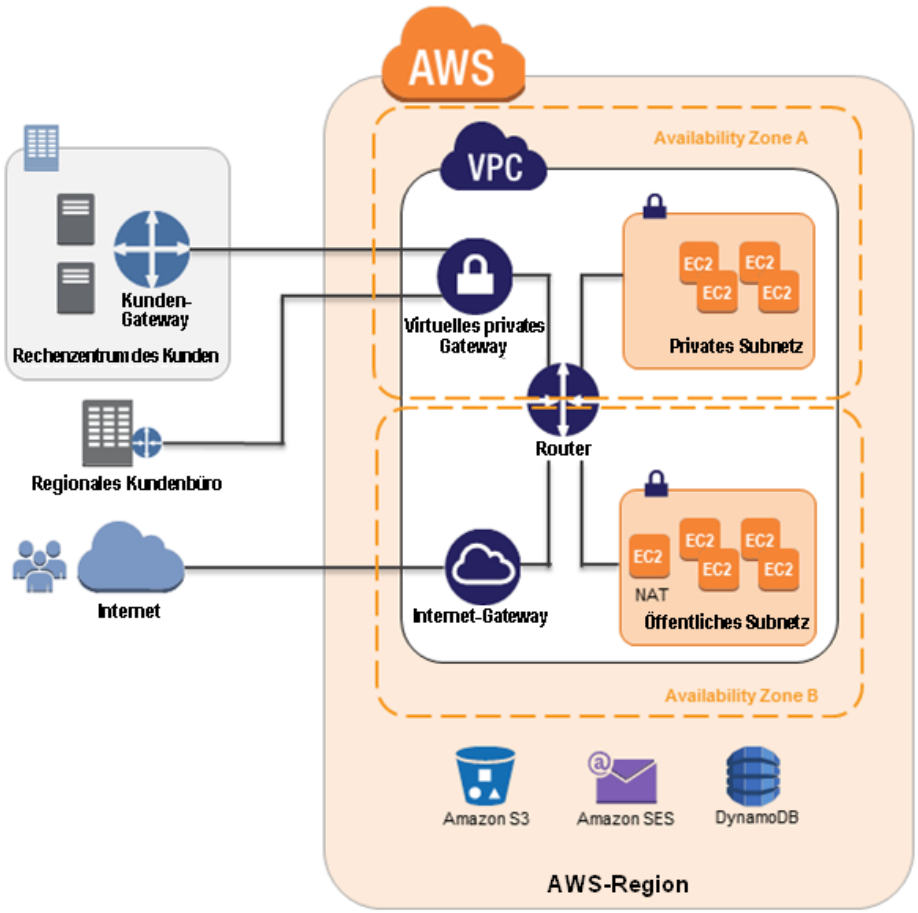


Abbildung 4: Amazon VPC-Netzwerkarchitektur

Netzwerkzugriffskontrolllisten: Um die Amazon VPC um eine Sicherheitsschicht zu erweitern, können Sie Netzwerkzugriffskontrolllisten konfigurieren. Hierbei handelt es sich um zustandslose Datenverkehrsfilter, die auf den gesamten ein- und ausgehenden Datenverkehr eines Subnetzes in der Amazon VPC angewendet werden. Diese Zugriffskontrolllisten können hierarchische Regeln enthalten, mit denen der Datenverkehr anhand des IP-Protokolls, des Service-Ports und der Quell-/Ziel-IP-Adresse zugelassen oder abgelehnt wird.

Netzwerkzugriffskontrolllisten werden ebenso wie Sicherheitsgruppen über Amazon VPC APIs verwaltet. So wird eine zusätzliche Sicherheitsschicht hinzugefügt und mehr Sicherheit durch Aufgabentrennung ermöglicht. Im Diagramm unten wird dargestellt, wie die oben genannten Kontrollmechanismen interagieren , um flexible Netzwerktopologien bei gleichzeitiger vollständiger Kontrolle des Datenflusses zu ermöglichen.

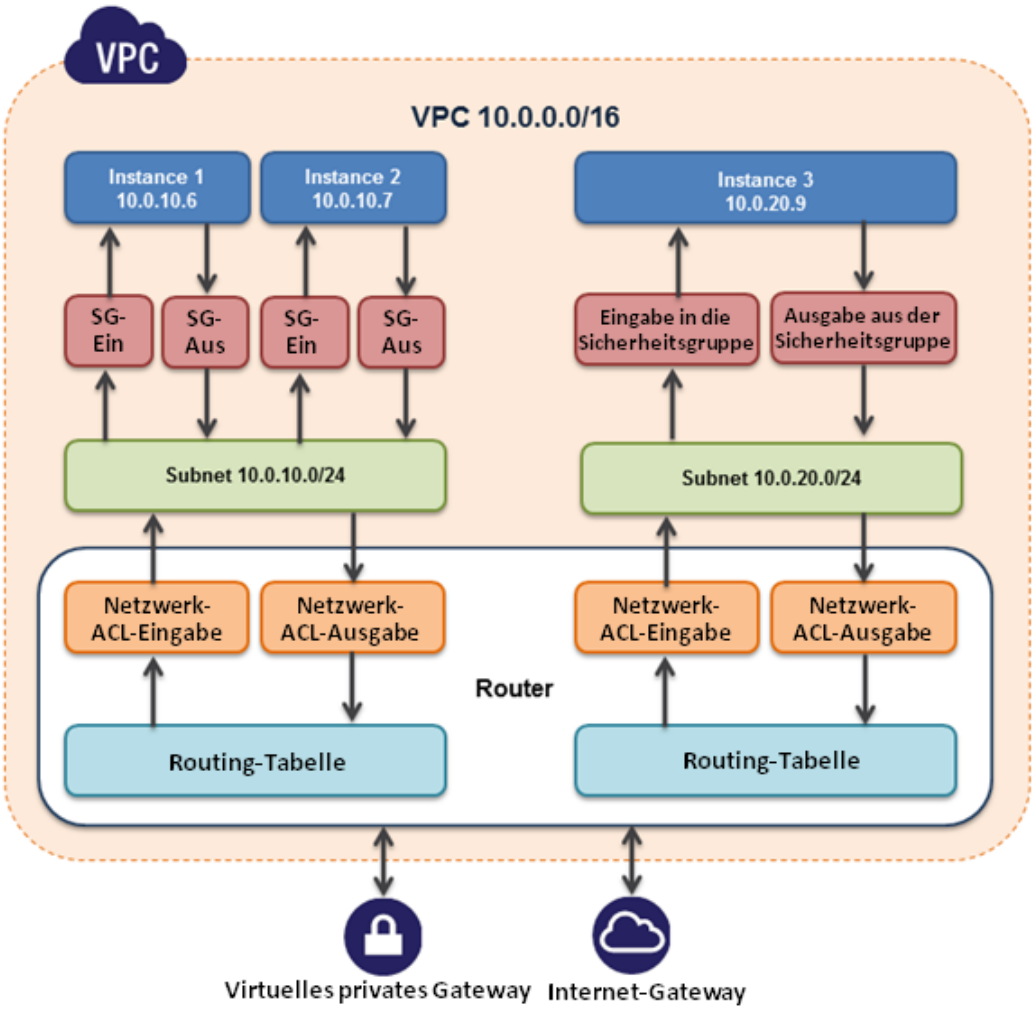


Abbildung 5: Flexible Netzwerktopologien

Virtuelles privates Gateway: Ein virtuelles privates Gateway ermöglicht eine private Verbindung zwischen der Amazon VPC und einem anderen Netzwerk. Der Datenverkehr innerhalb jedes einzelnen virtuellen privaten Gateways wird vom Datenverkehr in allen anderen virtuellen privaten Gateways isoliert. Sie können VPN-Verbindungen mit dem virtuellen privaten Gateway über die Gateway-Geräte an Ihrem Standort herstellen. Jede Verbindung wird durch einen vorinstallierten Schlüssel in Verbindung mit der IP-Adresse des kundenseitigen Gateway-Geräts gesichert.

Internet-Gateway: Ein Internet-Gateway kann mit einer Amazon VPC verbunden werden, um die direkte Verbindung Konnektivität mit Amazon S3, anderen AWS-Services und dem Internet zu ermöglichen. Jede Instanz, die diesen Zugriff erfordert, muss entweder über eine entsprechend verknüpfte Elastic IP-Adresse verfügen oder den Datenverkehr über eine NAT-Instanz weiterleiten. Außerdem werden Netzwerkrouten konfiguriert (siehe oben), um den Datenverkehr an das Internet-Gateway weiterzuleiten. AWS stellt Referenz-NAT AMIs zur Verfügung, mit denen Sie Netzwerkprotokollierung, Deep Packet Inspection, Filter auf Anwendungsebene oder andere Sicherheitskontrollen nutzen können.

Dieser Zugriff kann nur über den Aufruf von Amazon VPC APIs geändert werden. AWS unterstützt die Möglichkeit, differenzierten Zugang zu verschiedenen Verwaltungsfunktionen der Instanzen und des Internet-Gateway zu gewähren. So können Sie mehr Sicherheit durch Aufgabentrennung implementieren.

Dedicated Instances: Innerhalb einer VPC können Sie Amazon EC2-Instanzen starten, die auf Ebene der Host-Hardware physisch isoliert sind (d. h., sie werden auf Single-Tenant-Hardware ausgeführt). Eine Amazon VPC kann mit "dedicated tenancy" erstellt werden, sodass alle Instanzen, die in der Amazon VPC gestartet werden, diese Funktion verwenden (d.h. auf dedizierter Hardware ausgeführt werden). Alternativ kann eine Amazon VPC mit "default tenancy " erstellt werden, wobei Sie dann "dedicated tenancy" für bestimmte in der VPC gestartete Instanzen einstellen können.

Elastic Network Interfaces: Jede Amazon EC2-Instanz verfügt über eine Standardnetzwerkschnittstelle, der eine private IP-Adresse im Amazon VPC-Netzwerk zugewiesen ist. Sie können eine zusätzliche Netzwerkschnittstelle, eine sogenannte elastische Netzwerkschnittstelle (Elastic Network Interface, ENI) erstellen und jeder Amazon EC2-Istance in der Amazon VPC hinzufügen, und zwar insgesamt zwei Netzwerkschnittstellen pro Instanz. Es ist nützlich, einer Instanz mehr als eine Netzwerkschnittstelle anzufügen, wenn Sie ein Management-Netzwerk erstellen, Netzwerk- und Sicherheitsanwendungen in der Amazon VPC verwenden oder Dual Homed-Instanzen mit Aufgaben /Rollen in verschiedenen Subnetzen erstellen möchten. Die Attribute einer ENI, einschließlich privater IP-Adresse, Elastic IP-Adressen und MAC-Adresse, folgen der ENI, wenn sie einer Instanz hinzugefügt oder von ihr getrennt und einer anderen Instanz hinzugefügt werden. Weitere Informationen über Amazon VPC erhalten Sie auf der AWS-Website: http://aws.amazon.com/de/vpc/

Zusätzliche Netzwerkzugriffskontrolle mit der EC2-VPC

Wenn Sie Instanzen in einer Region starten, in der Sie vor dem Start der neuen EC2-VPC-Funktion (auch als Standard-VPC bezeichnet) durch AWS noch keine Instanzen in Betrieb hatten, werden alle Instanzen automatisch in einer verwendungsbereiten Standard-VPC bereitgestellt. Sie können entweder zusätzliche VPCs erstellen oder VPCs für Instanzen in Regionen erstellen, in denen Sie vor der Einführung von EC2-VPC bereits Instanzen in Betrieb hatten.

Wenn Sie später eine VPC anhand einer normalen VPC erstellen, geben Sie einen CIDR-Block an, erstellen Subnetze, geben Routing und Sicherheit für diese Subnetze ein und stellen ein Internet-Gateway oder eine NAT-Instanz bereit, wenn eines der Subnetze Zugriff auf das Internet haben sollen. Wenn Sie EC2-Instanzen in einer EC2-VPC starten, werden diese Einstellungen größtenteils automatisch vorgenommen. Wenn Sie eine Instanz in einer Standard-VPC mit EC2-VPC starten, werden folgende Vorgänge zur Einrichtung ausgeführt:

- Erstellen eines Standardsubnetzes in jeder Availability Zone
- Erstellen eines Internet-Gateways und Herstellen einer Verbindung mit der Standard-VPC
- Erstellen einer Routing-Haupttabelle für Ihre Standard-VPC mit einer Regel, die den gesamten für das Internet bestimmten Datenverkehr an das Internet-Gateway sendet
- Erstellen einer Standardsicherheitsgruppe und Verknüpfen dieser Gruppe mit Ihrer Standard-VPC
- Erstellen einer Standardnetzwerkzugriffskontrollliste (ACL) und Verknüpfen mit Ihrer Standard-VPC
- Verknüpfen der DHCP-Standardoptionen für Ihr AWS-Konto mit Ihrer Standard-VPC

Die Standard-VPC hat nicht nur einen eigenen privaten IP-Bereich, sondern in einer Standard-VPC gestartete EC2-Instanzen können eine öffentliche IP-Adresse erhalten.

In der folgenden Tabelle werden die Unterschiede zwischen Instanzen zusammengefasst, die in EC2-Classic gestartet werden, Instanzen, die in einer Standard-VPC gestartet werden, und Instanzen, die in einer nicht standardmäßigen VPC gestartet werden.

Merkmal	EC2-Classic	EC2-VPC (Standard-VPC)	Normale VPC
Öffentliche IP-Adresse	Die Instanz empfängt eine öffentliche IP-Adresse.	Die in einem Standardsubnetz gestartete Instanz empfängt standardmäßig eine öffentliche IP-Adresse, sofern beim Start keine andere Einstellung festgelegt wurde.	Die Instanz empfängt standardmäßig keine öffentliche IP-Adresse, sofern beim Start keine andere Einstellung festgelegt wurde.
Private IP-Adresse	Die Instanz empfängt bei jedem Start eine private IP-Adresse aus dem EC2-Classic-Bereich.	Die Instanz empfängt eine statische private IP-Adresse aus dem Adressbereich Ihrer Standard-VPC.	Die Instanz empfängt eine statische private IP-Adresse aus dem Adressbereich Ihrer VPC.
Mehrere private IP-Adressen	Wir wählen eine einzelne IP-Adresse für Ihre Instanz aus. Mehrere IP-Adressen werden nicht unterstützt.	Sie können Ihrer Instanz mehrere private IP-Adressen zuweisen.	Sie können Ihrer Instanz mehrere private IP-Adressen zuweisen.
Elastic IP-Adresse	Die Zuordnung einer EIP zu Ihrer Instanz wird getrennt, wenn Sie sie anhalten.	Die Zuordnung einer EIP zu Ihrer Instanz bleibt bestehen, wenn Sie sie anhalten.	Die Zuordnung einer EIP zu Ihrer Instanz bleibt bestehen, wenn Sie sie anhalten.
DNS-Hostnamen	DNS-Hostnamen werden standardmäßig aktiviert.	DNS-Hostnamen werden standardmäßig aktiviert.	DNS-Hostnamen werden standardmäßig deaktiviert.
Sicherheitsgruppe	Eine Sicherheitsgruppe kann auf Sicherheitsgruppen verweisen, die zu anderen AWS-Konten gehören.	Eine Sicherheitsgruppe kann nur auf Sicherheitsgruppen für Ihre VPC verweisen.	Eine Sicherheitsgruppe kann nur auf Sicherheitsgruppen für Ihre VPC verweisen.
Sicherheitsgruppenzuweisung	Sie müssen Ihre Instanz beenden, um die zugehörige Sicherheitsgruppe zu ändern.	Sie können die Sicherheitsgruppe Ihrer laufenden Instanz ändern.	Sie können die Sicherheitsgruppe Ihrer laufenden Instanz ändern.
Sicherheitsgruppenregeln	Sie können nur Regeln für eingehenden Datenverkehr hinzufügen.	Sie können Regeln für ein- und ausgehenden Datenverkehr hinzufügen.	Sie können Regeln für ein- und ausgehenden Datenverkehr hinzufügen.
Tenancy	Die Instanz wird auf gemeinsam genutzter Hardware ausgeführt. Sie können eine Instanz nicht auf dedizierter Hardware ausführen.	Sie können die Instanz auf gemeinsam genutzter Hardware oder auf dedizierter Hardware ausführen.	Sie können die Instanz auf gemeinsam genutzter Hardware oder auf dedizierter Hardware ausführen.

Hinweis: Sicherheitsgruppen für Instanzen in EC2-Classic unterscheiden sich geringfügig von Sicherheitsgruppen für Instanzen in EC2-VPC. Sie können beispielsweise Regeln für eingehenden Datenverkehr für EC2-Classic hinzufügen. Zur EC2-VPC können Sie hingegen Regeln sowohl für ein- als auch ausgehenden Datenverkehr hinzufügen. In EC2-Classic können Sie die Sicherheitsgruppen, die einer Instanz nach deren Start zugewiesen sind, nicht ändern. In der EC2-VPC ist dies möglich. Darüber hinaus können Sie die Sicherheitsgruppen, die Sie zur Verwendung mit EC2-Classic mit Instanzen in Ihrer VPC erstellt haben, nicht nutzen. Sie müssen Sicherheitsgruppen speziell zur Verwendung mit Instanzen in Ihrer VPC erstellen. Die Regeln, die Sie für eine Sicherheitsgruppe für eine VPC erstellen, können nicht auf eine Sicherheitsgruppe für EC2-Classic verweisen und umgekehrt.

Sicherheit bei AWS Direct Connect

Mit AWS Direct Connect können Sie eine direkte Verknüpfung zwischen Ihrem internen Netzwerk und einer AWS-Region mit einer dedizierten Verbindung mit hohem Durchsatz bereitstellen. So lassen sich möglicherweise die Netzwerkkosten reduzieren, den Durchsatz erhöhen oder eine konsistentere Netzwerkfunktion schaffen. Mit dieser dedizierten Verbindung können Sie dann virtuelle Schnittstellen direkt zur AWS-Cloud (z. B. zu Amazon EC2 und Amazon S3) und zu Amazon VPC erstellen.

Mit Direct Connect umgehen Sie Internetprovider in Ihrem Netzwerkpfad. Sie können innerhalb der Anlage, in der sich der AWS Direct Connect-Standort befindet, Rackspace erwerben und Ihre Geräte in unmittelbarer Nähe bereitstellen. Nach der Bereitstellung können Sie diese Geräte über ein Cross-Connect mit AWS Direct Connect verbinden. Jeder AWS Direct Connect-Standort ermöglicht eine Konnektivität mit der geografisch nächstgelegenen AWS-Region sowie in den USA Zugriff auf andere Regionen. Sie können beispielsweise eine einzelne Verbindung mit einem AWS Direct Connect-Standort in den USA bereitstellen und sie für den Zugriff auf öffentliche AWS-Services in allen US-Regionen und AWS GovCloud (US) verwenden.

Mithilfe von VLANs nach Industriestandard 802.1q kann die dedizierte Verbindung in mehrere virtuelle Schnittstellen partitioniert werden. So können Sie dieselbe Verbindung für den Zugriff auf öffentliche Ressourcen wie Objekte verwenden, die in Amazon S3 mit öffentlichem IP-Adressbereich gespeichert sind, und auf private Ressourcen wie Amazon EC2-Instanzen, die innerhalb einer Amazon VPC mit einem privaten IP-Adressbereich ausgeführt werden. Dabei wird die Netzwerktrennung der öffentlichen und privaten Umgebungen beibehalten.

Für Amazon Direct Connect muss das Border Gateway Protocol (BGP) mit einer Autonomous System Number (ASN) verwendet werden. Verwenden Sie zum Erstellen einer virtuellen Schnittstelle einen kryptografischen MD5-Schlüssel, um Nachrichten zu autorisieren. MD5 erstellt einen verschlüsselten Hash mit Ihrem geheimen Schlüssel. Sie können einen BGP MD5-Schlüssel automatisch von AWS generieren lassen oder einen eigenen beschaffen.

Sicherheit bei Amazon Simple Storage Service (Amazon S3)

Mit Amazon Simple Storage Service (S3) können Sie Daten jederzeit und überall im Web hochladen und abrufen. Amazon S3 speichert Daten als *Objekte* in *Buckets*. Ein Objekt kann jede Art von Datei sein: eine Textdatei, ein Foto, ein Video usw. Wenn Sie eine Datei zu Amazon S3 hinzufügen, können Sie Metadaten in die Datei einbeziehen und Berechtigungen für den Dateizugriff festlegen. Für jeden Bucket können Sie den Zugriff steuern (welche Benutzer Objekte im Bucket erstellen, löschen und auflisten können), Zugriffsprotokolle für den Bucket und seine Objekte anzeigen und die geografische Region wählen, in der Amazon S3 den Bucket und seinen Inhalt speichert.

Datenzugriff

Der Zugriff auf die in Amazon S3 gespeicherten Daten wird standardmäßig beschränkt. Nur Bucket- und Objektbesitzer haben Zugriff auf Amazon S3-Ressourcen, die sie erstellen (Bucket-/Objektbesitzer ist der AWS-Kontoinhaber, nicht der Benutzer, der den Bucket bzw. das Objekt erstellt hat). Es gibt mehrere Möglichkeiten, den Zugriff auf Buckets und Objekte zu kontrollieren:

- **Identity and Access Management (IAM)-Richtlinien:** Mit AWS IAM können Organisationen mit vielen Mitarbeitern mehrere Benutzer für ein einzelnes AWS-Konto erstellen und diese verwalten. IAM-Richtlinien werden den Benutzern zugeordnet und ermöglichen eine zentrale Kontrolle der Berechtigungen für Benutzer in Ihrem AWS-Konto, um auf Buckets oder Objekte zuzugreifen. Mit IAM-Richtlinien können Sie nur *Benutzern innerhalb Ihres eigenen AWS-Kontos* Zugriffsberechtigung für Ihre Amazon S3-Ressourcen erteilen.

- **Netzwerkzugriffskontrolllisten (ACLs):** In Amazon S3 können Sie mit ACLs für Benutzergruppen Lese- oder Schreibzugriff auf Buckets oder Objekte vergeben. Mit ACLs können Sie nur *anderen AWS-Konten* (keinen bestimmten Benutzern) Zugriff auf Ihre Amazon S3-Ressourcen erteilen.
- **Bucket-Richtlinien:** Mit Bucket-Richtlinien in Amazon S3 können Berechtigungen für einige oder alle Objekte in einem Bucket hinzugefügt oder abgelehnt werden. Richtlinien können Benutzern, Gruppen oder Amazon S3-Buckets zugeordnet werden, was eine zentrale Berechtigungsverwaltung ermöglicht. Mit Bucket-Richtlinien können Sie Benutzern innerhalb Ihres eigenen AWS-Kontos *oder* anderen AWS-Konten Zugriffsberechtigung für Ihre Amazon S3-Ressourcen erteilen.

Art der Zugriffskontrolle	Kontrolle auf AWS-Kontoebene?	Kontrolle auf Benutzerebene?
IAM-Richtlinien	Nein	Ja
ACLs	Ja	Nein
Bucket-Richtlinien	Ja	Ja

Sie können den Zugriff auf spezifische Ressourcen basierend auf bestimmten Bedingungen beschränken. Sie können den Zugriff beispielsweise basierend auf dem Zeitpunkt der Anforderung (Datumsbedingung), auf der Tatsache, ob die Anforderung mit SSL gesendet wurde (boolesche Bedingung), auf der IP-Adresse des Anforderers (IP-Adressbedingung) oder basierend auf der Client-Anwendung des Anforderers (String-Bedingung) einschränken. Zur Festlegung dieser Bedingungen verwenden Sie *Richtlinienschlüssel*. Weitere Informationen über aktionsspezifische Richtlinienschlüssel, die in Amazon S3 verfügbar sind, finden Sie im Amazon Simple Storage Service Developer Guide.

Mit Amazon S3 können Entwickler auch die *Authentifizierung anhand der Abfragezeichenfolge* (*Query String Authentication*) verwenden. Mit dieser Authentifizierung können Amazon S3-Objekte über URLs geteilt werden, die für einen vordefinierten Zeitraum gültig sind. Die Authentifizierung anhand der Abfragezeichenfolge ist nützlich, um HTTP- oder Browserzugriff auf Ressourcen zu erteilen, für die normalerweise eine Authentifizierung erforderlich ist. Die Abfrage wird durch die Signatur in der Abfragezeichenfolge gesichert.

Datenübertragung

Um maximale Sicherheit zu erreichen, können Sie Daten in Amazon S3 über die SSL-verschlüsselten Endpunkte hoch- bzw. herunterladen. Die verschlüsselten Endpunkte sind sowohl über das Internet als auch innerhalb von Amazon EC2 zugänglich, sodass die Daten innerhalb von AWS sowie zu und von Quellen außerhalb von AWS sicher übertragen werden.

Datenspeicher

Amazon S3 bietet mehrere Optionen zum Schutz von ruhenden Daten. Für Kunden, die eigene kryptografische Schlüssel vorziehen, kann eine Clientverschlüsselungsbibliothek wie der Amazon S3 Encryption Client verwendet werden, um die Daten vor dem Hochladen auf Amazon S3 zu verschlüsseln. Alternativ können Sie Amazon S3 Server Side Encryption (SSE) verwenden, wenn die Verwaltung der kryptografischen Schlüssel über Amazon S3 erfolgen soll. Mit Amazon S3 SSE können Sie Daten beim Hochladen verschlüsseln. Dazu müssen Sie einfach beim Schreiben des Objekts einen zusätzlichen Anforderungs-Header hinzufügen. Die Entschlüsselung geschieht automatisch, wenn die Daten abgerufen werden.

Hinweis: Metadaten, die in das Objekt einbezogen werden können, werden nicht verschlüsselt. Daher empfiehlt AWS, keine vertraulichen Informationen in S3-Metadaten zu integrieren.

Amazon S3 SSE verwendet 256-Bit Advanced Encryption Standard (AES-256), eine der stärksten Blockverschlüsselungen, die verfügbar sind. Mit Amazon S3 SSE wird jedes geschützte Objekt mit einem eindeutigen kryptografischen Schlüssel verschlüsselt. Dieser Objektschlüssel wird dann mit einem regelmäßig rotierten Hauptschlüssel verschlüsselt. Amazon S3 SSE bietet zusätzliche Sicherheit, indem die verschlüsselten Daten und kryptografischen Schlüssel in verschiedenen Hosts gespeichert werden. Mit Amazon S3 SSE können Sie außerdem Verschlüsselungsanforderungen durchsetzen. Sie können beispielsweise Bucket-Richtlinien erstellen und anwenden, die festlegen, dass nur verschlüsselte Daten in Ihre Buckets hochgeladen werden können.

Zur langfristigen Speicherung können Sie die Inhalte Ihrer S3-Buckets im Archiv-Service von AWS, Glacier, archivieren. Daten können in bestimmten Intervallen in Glacier übertragen werden. Dazu werden Lebenszyklusregeln in S3 erstellt, die beschreiben, welche Objekte zu welchen Zeiten in Glacier archiviert werden sollen. Im Rahmen Ihrer Datenverwaltungsstrategie können Sie außerdem angeben, wie lange S3 warten soll, bis die in S3 übertragenen Objekte gelöscht werden.

Wenn ein Objekt aus Amazon S3 gelöscht wird, wird die Entfernung der Zuordnung des öffentlichen Namens zum Objekt sofort gestartet und im Allgemeinen innerhalb einiger Sekunden im gesamten verteilten System verarbeitet. Sobald die Zuordnung entfernt ist, besteht kein Remotezugriff mehr auf das gelöschte Objekt. Der zugrunde liegende Speicherbereich wird dann vom System wiederverwendet.

Datenhaltbarkeit und -zuverlässigkeit

Amazon S3 ist auf eine Haltbarkeit von 99,999999999 % und Verfügbarkeit von Objekten von 99,99 % pro Jahr ausgelegt. Objekte werden redundant auf mehreren Geräten über mehrere Einrichtungen einer Amazon S3-Region gespeichert. Zur Unterstützung der Haltbarkeit werden durch die Amazon S3-Vorgänge PUT und COPY Kundendaten in mehreren Anlagen synchron gespeichert, bevor SUCCESS zurückgegeben wird. Nach dem Speichern unterstützt Amazon S3 die Haltbarkeit der Objekte, indem verloren gegangene Redundanz schnell ermittelt und behoben wird. Amazon S3 überprüft außerdem regelmäßig die Integrität der gespeicherten Daten anhand von Prüfsummen. Wenn eine Beschädigung festgestellt wird, wird diese mit den redundanten Daten behoben. Darüber hinaus kalkuliert Amazon S3 Prüfsummen im gesamten Netzwerkdatenverkehr, um beim Speichern oder Abrufen von Daten eine Beschädigung von Datenpaketen zu erkennen.

Amazon S3 bietet einen weiteren Schutz durch Versionierung. Mit Versionierung können Sie jede Version eines jeden in einem Amazon S3-Bucket gespeicherten Objekts beibehalten, abrufen und wiederherstellen. Daten lassen sich dank Versionierung nach unbeabsichtigten Benutzeraktionen und Anwendungsfehlern leicht wiederherstellen. Standardmäßig wird durch Anforderungen die zuletzt geschriebene Version abgerufen. Ältere Versionen eines Objekts können abgerufen werden, indem die entsprechende Version in der Anforderung angegeben wird. Sie können Versionen zudem mithilfe der MFA Delete-Funktion von Amazon S3 Versionierung schützen. Sobald diese Funktion für ein S3-Bucket aktiviert wurde, muss jede Anforderung zur Löschung einer Version einen sechsstelligen Code und die Seriennummer des Multi-Faktor Authentication-Geräts enthalten.

Zugriffsprotokolle

Ein Amazon S3-Bucket kann so konfiguriert werden, dass der Zugriff auf den Bucket und die darin enthaltenen Objekte protokolliert werden. Das Zugriffsprotokoll enthält Details über jede Zugriffsanforderung, einschließlich Anforderungstyp, angeforderte Ressource, IP des Anforderers sowie Uhrzeit und Datum der Anforderung. Wenn die Protokollierung für ein Bucket aktiviert ist, werden Protokolldatensätze regelmäßig in Protokolldateien kumuliert und an den angegebenen Amazon S3-Bucket geliefert.

Cross-Origin Resource Sharing (CORS)

AWS-Kunden, die S3 zum Hosten statischer Webseiten oder zum Speichern von Objekten verwenden, die von anderen Webseiten genutzt werden, können Inhalt sicher laden, indem sie einen S3-Bucket konfigurieren, um ursprungsübergreifende Anforderungen zu ermöglichen. Moderne Browser verwenden die Same Origin-Richtlinie, um JavaScript oder HTML5 zu blockieren, sodass keine Anforderungen zum Laden von Inhalten von einer anderen Website oder Domain zugelassen werden. So wird sichergestellt, dass kein schädlicher Inhalt von einer weniger seriösen Quelle (wie bei Cross-Site-Scripting-Angriffen) geladen wird. Wenn die Cross-Origin Resource Sharing (CORS)-Richtlinie aktiviert ist, kann auf Komponenten wie in einem S3-Bucket gespeicherte Webschriftarten und Bilder von externen Webseiten, Formatvorlagen und HTML5-Anwendungen sicher verwiesen werden.

Sicherheit bei AWS Glacier

Ebenso wie Amazon S3 bietet der Amazon Glacier-Service einen kostengünstigen, sicheren und haltbaren Speicher. Während S3 jedoch für schnelles Abrufen konzipiert ist, dient Glacier als Archiv-Service für Daten, auf die nicht oft zugegriffen wird und für die Abrufzeiten von mehreren Stunden geeignet sind.

Amazon Glacier speichert Dateien als *Archive* in *Vaults*. Archive können beliebige Daten wie ein Foto, Video oder Dokument sein und ein oder mehrere Dateien enthalten. Sie können eine unbegrenzte Anzahl von Archiven in einem einzelnen Vault speichern und bis zu 1.000 Vaults pro Region erstellen. Jedes Archiv kann bis zu 40 TB Daten enthalten.

Daten-Upload

Um Daten in Amazon Glacier-Vaults zu übertragen, können Sie ein Archiv in einem einzigen Upload-Vorgang oder einem mehrteiligen Vorgang hochladen. In einem Upload-Vorgang können Archive mit einer Größe von bis zu 4 GB hochgeladen werden. Kunden können jedoch bessere Ergebnisse erzielen, wenn sie die API für den mehrteiligen Upload verwenden, um Archive mit einer Größe von mehr als 100 MB hochladen. Mit der API für den mehrteiligen Upload können Sie große Archive bis zu einer Größe von rund 40.000 GB hochladen. Die API für den mehrteiligen Upload soll den Upload-Vorgang für größere Archive verbessern, da die Teile unabhängig, in einer beliebigen Reihenfolge und parallel hochgeladen werden können. Wenn bei einem mehrteiligen Upload ein Fehler auftritt, müssen Sie lediglich den betroffenen Teil und nicht das gesamte Archiv erneut hochladen.

Wenn Sie Daten auf Glacier hochladen, müssen Sie einen Struktur-Hash ("tree hash") berechnen und mit hochladen. Glacier gleicht den Hash mit den Daten ab, um sicherzustellen, dass sie auf dem Weg nicht verändert wurden. Ein Struktur-Hash wird generiert, indem ein Hash für jedes megabytegroße Datensegment berechnet wird und die Hashes dann in Form eines Baums kombiniert werden, um stetig wachsende aneinanderhängende Datensegmente darzustellen.

Alternativ zum mehrteiligen Upload können Kunden mit sehr großen Uploads auf Amazon Glacier die Daten stattdessen mit dem AWS Import/Export-Service übertragen. Der AWS Import/Export-Service ermöglicht die Übertragung großer Datenmengen in AWS durch Nutzung von portablen Speichergeräten als Transportmittel. AWS überträgt Ihre Daten von den Speichergeräten mithilfe des internen Hochgeschwindigkeitsnetzwerks von Amazon unter Umgehung des Internets.

Sie können S3 auch so einrichten, dass Daten in bestimmten Intervallen auf Glacier übertragen werden. Sie können Lebenszyklusregeln in S3 erstellen, die beschreiben, welche Objekte in Glacier archiviert werden sollen und zu welchem Zeitpunkt. Sie können außerdem angeben, wie lange S3 warten soll, bis die in S3 übertragenen Objekte gelöscht werden.

Um eine noch höhere Sicherheit zu erreichen, können Sie Daten in Amazon Glacier über die SSL-verschlüsselten Endpunkte hoch- bzw. herunterladen. Die verschlüsselten Endpunkte sind sowohl über das Internet als auch innerhalb von Amazon EC2 zugänglich, sodass die Daten innerhalb von AWS sowie zu und von den Quellen außerhalb von AWS sicher übertragen werden.

Datenabruf

Für das Abrufen von Archiven von Amazon Glacier muss ein Abrufauftrag eingeleitet werden, der im Allgemeinen in 3 bis 5 Stunden abgeschlossen ist. Sie können dann über HTTP GET-Anforderungen auf die Daten zugreifen. Die Daten bleiben 24 Stunden verfügbar.

Sie können ein gesamtes Archiv oder einzelne Dateien aus einem Archiv abrufen. Wenn Sie nur einen Teil eines Archivs abrufen möchten, können Sie den Bereich des Archivs, der die entsprechenden Dateien enthält, in einer Abrufanforderung angeben oder Sie können mehrere Abrufanforderungen einleiten, die jeweils einen Bereich für eine oder mehrere Dateien angeben. Außerdem können Sie die Anzahl der abgerufenen Vault-Inventarelemente begrenzen, indem Sie nach einem Archiverstellungsdatum filtern oder die Anzahl der Elemente beschränken. Mit hilfe des Sruktur-Hash des Gesamtarchives können sie Beim Abrufen von Teilen Ihres Archivs unabhängig von der ausgewählten Methode, die angegebene Prüfsumme verwenden, um die Integrität der Dateien sicherzustellen.

Datenspeicher

Amazon Glacier verschlüsselt die Daten automatisch mit AES-256 und speichert sie dauerhaft in unveränderbarer Form. Amazon Glacier ist auf eine durchschnittliche Jahreshaltbarkeit von 99,999999999 % pro Archiv ausgelegt. Jedes Archiv wird in mehreren Anlagen und Geräten gespeichert. Im Gegensatz zu herkömmlichen Systemen, die eine aufwendige Datenüberprüfung und manuelle Reparatur erfordern, führt Glacier regelmäßige, systematische Datenintegritätsprüfungen durch und ist für eine automatische Selbst-Reparatur konzipiert.

Datenzugriff

Nur Ihr Konto hat Zugriff auf Ihre Daten in Amazon Glacier. Um den Zugriff auf Ihre Daten in Amazon Glacier zu kontrollieren, können Sie mithilfe von AWS IAM festlegen, welche Benutzer innerhalb Ihres Kontos für Vorgänge auf dem jeweiligen Vault berechtigt sind.

Sicherheit bei AWS Storage Gateway

Der AWS Storage Gateway-Service verbindet Ihre Softwareanwendung vor Ort mit dem cloudbasierten Speicher, um eine nahtlose und sichere Integration zwischen Ihrer IT-Umgebung und der Speicherinfrastruktur von AWS herzustellen. Mit dem Service können Sie Daten in den skalierbaren, zuverlässigen und sicheren S3-Speicher-Service hochladen, um ein kosteneffizientes Backup und eine schnelle Notfallwiederherstellung zu ermöglichen.

AWS Storage Gateway sichert externe Daten in Amazon S3 in Form von Amazon EBS-Snapshots. Amazon S3 speichert diese Snapshots redundant auf mehreren Geräten in verschiedenen Anlagen und ermittelt und behebt dabei verloren gegangene Redundanz. Der Amazon EBS-Snapshot stellt eine Zeitpunktsicherung bereit, die vor Ort wiederhergestellt oder dazu verwendet werden kann, neue Amazon EBS-Volumes zu instanziieren. Die Daten werden innerhalb einer von Ihnen angegebenen Region gespeichert.

AWS Storage Gateway bietet drei Optionen:

- **Gateway-Stored Volumes (die Cloud dient als Sicherung)**: Bei dieser Option werden Ihre Volume-Daten lokal gespeichert und dann in Amazon S3 übertragen, wo sie in redundanter, verschlüsselter Form gespeichert werden und in Form von Elastic Block Storage (EBS)-Snapshots verfügbar gemacht werden. Wenn Sie dieses Modell verwenden, ist der lokale Speicher primär und stellt Zugriff auf ihren gesamten Datensatz mit niedriger Latenz bereit. Der Cloud-Speicher dient als Sicherung.
- **Gateway-Cached Volumes (die Cloud ist primär)**: Bei dieser Option werden die Volume-Daten in Amazon S3 verschlüsselt gespeichert, wobei sie innerhalb des Unternehmensnetzwerks über eine iSCSI-Schnittstelle

sichtbar sind. Daten, auf die zuletzt zugegriffen wurde, werden lokal zwischengespeichert, um lokalen Zugriff mit niedriger Latenz zu ermöglichen. Wenn Sie dieses Modell verwenden, ist der Cloud-Speicher zwar primär, doch Sie erhalten Zugriff mit niedriger Latenz auf Ihren aktiven Arbeitssatz in den lokalen zwischengespeicherten Volumes.

- **Gateway-Virtual Tape Library (VTL)**: Bei dieser Option können Sie ein Gateway-VTL mit bis zu 10 virtuellen Bandlaufwerken pro Gateway, einem Medienwechsler und bis zu 1500 virtuellen Bandkassetten konfigurieren. Jedes virtuelle Bandlaufwerk reagiert auf den SCSI-Befehlssatz, sodass Ihre vorhandenen lokalen Sicherungsanwendungen (entweder von Festplatte auf Band oder von Festplatte auf Festplatte und auf Band) unverändert funktionieren.

Unabhängig davon, welche Option Sie auswählen, werden die Daten asynchron von Ihrer lokalen Speicherhardware auf AWS über SSL übertragen. Die Daten werden in Amazon S3 mit dem Advanced Encryption Standard (AES) 256, einem Verschlüsselungsstandard mit symmetrischem Schlüssel unter Verwendung von kryptografischen Schlüsseln mit einer Länge von 256-Bit, verschlüsselt gespeichert. Das AWS Storage Gateway lädt nur Daten hoch, die geändert wurden, und minimiert so die über das Internet gesendete Datenmenge.

Das AWS Storage Gateway wird als virtuelle Maschine (VM) ausgeführt, die Sie auf einem Host in Ihrem Rechenzentrum einrichten, auf der VMware ESXi Hypervisor v 4.1 oder v 5 oder Microsoft Hyper-V ausgeführt wird (Sie laden die VMware-Software während der Einrichtung herunter). Das Gateway kann auch mit einem Gateway-AMI innerhalb von EC2 ausgeführt werden. Während des Installations- und Konfigurationsprozesses können Sie bis zu 12 Stored Volumes, 20 Cached Volumes oder 1500 virtuelle Bandkassetten pro Gateway erstellen. Nach der Installation wird jedes Gateway automatisch Aktualisierungen und Patches herunterladen, installieren und verteilen. Diese Aktivität findet während eines Wartungsfensters statt, das Sie für jedes Gateway gesondert festlegen können.

Das iSCSI-Protokoll unterstützt die Authentifizierung zwischen Targets und Initiatoren über CHAP (Challenge-Handshake Authentication Protocol). CHAP bietet Schutz gegen Man-in-the-Middle- und Playback-Angriffe, indem die Identität eines iSCSI-Initiators als für den Zugriff auf ein Volume-Target authentifiziert regelmäßig verifiziert wird. Zum Einrichten von CHAP müssen Sie das Protokoll sowohl in der AWS Storage Gateway-Konsole als auch in der iSCSI-Initiatorsoftware konfigurieren, die Sie zum Verbinden mit dem Target verwenden.

Nachdem Sie die AWS Storage Gateway VM eingerichtet haben, müssen Sie das Gateway über die AWS Storage Gateway-Konsole aktivieren. Durch den Aktivierungsprozess wird Ihr Gateway mit Ihrem AWS-Konto verknüpft. Sobald Sie diese Verbindung herstellen, können Sie fast alle Funktionen Ihres Gateways über die Konsole verwalten. Bei der Aktivierung geben Sie die IP-Adresse Ihres Gateways an, benennen das Gateway, identifizieren die AWS-Region, in der die Snapshot-Sicherungen gespeichert werden sollen, und geben die Zeitzone für das Gateway an.

AWS Import/Export-Sicherheit

AWS Import/Export ist eine einfache, sichere Methode für die physische Übertragung großer Datenmengen in den AWS S3-, EBS- oder Glacier-Speicher. Dieser Service wird in der Regel von Kunden mit Daten von über 100 GB und/oder langsamen Verbindungsgeschwindigkeiten verwendet, da die Übertragungsraten über das Internet in diesen Fällen sehr niedrig wären. Mit AWS Import/Export bereiten Sie ein portables Speichergerät vor, das Sie an einen sicheren AWS-Standort versenden. AWS überträgt die Daten vom Speichergerät über das interne Hochgeschwindigkeitsnetzwerks von Amazon unter Umgehung des Internets. Umgekehrt können Daten auch aus AWS auf ein portables Speichergerät exportiert werden.

Wie alle anderen AWS-Services erfordert auch AWS Import/Export-Service, dass Sie Ihr Speichergerät sicher identifizieren und authentifizieren. In diesem Fall senden Sie einen Auftrag an AWS, die den Amazon S3-Bucket, die Amazon EBS-Region, die AWS-Zugriffsschlüssel-ID und die Absenderadresse enthält. Anschließend erhalten Sie eine

eindeutige Auftrags-ID, eine digitale Signatur zum Authentifizieren Ihres Geräts und eine AWS-Adresse, an die das Speichergerät zu versenden ist. Für Amazon S3 legen Sie die Signaturdatei im Stammverzeichnis des Geräts ab. Für Amazon EBS bringen Sie den Signaturbarcode an der Außenseite des Geräts an. Die Signaturdatei wird nur zur Authentifizierung verwendet und nicht auf S3 oder EBS hochgeladen.

Für Übertragungen auf S3 geben die Kunden die spezifischen Buckets an, in die die Daten geladen werden sollen, und stellen sicher, dass das entsprechende Konto Schreibberechtigung für die Buckets hat. Sie sollten außerdem die Zugriffskontrollliste angeben, die auf jedes Objekt, das auf S3 geladen wird, anzuwenden ist.

Für Übertragungen in EBS geben Sie die Zielregion für den EBS-Importvorgang an. Wenn das Speichergerät unter der maximalen Volume-Größe von 1 TB liegt oder dieser entspricht, werden die Inhalte direkt in einen Amazon EBS-Snapshot geladen. Überschreitet die Kapazität des Speichergeräts 1 TB, wird ein Geräte-Image im angegebenen Amazon S3-Log-Bucket gespeichert. Sie können dann ein RAID von Amazon EBS-Volumes mit Software wie Logical Volume Manager erstellen und das Image aus Amazon S3 auf dieses neue Volume kopieren.

Zur Erhöhung der Sicherheit können Sie die Daten auf Ihrem Gerät vor dem Versand an AWS verschlüsseln. Für S3-Daten unterstützt der AWS Import/Export die Verschlüsselung mit TrueCrypt. Für EBS- und Glacier-Daten können Sie eine beliebige Verschlüsselungsmethode auswählen. AWS entschlüsselt Ihre S3-Daten vor dem Import mit dem TrueCrypt-Passwort, das Sie in Ihrem Importmanifest angeben. EBS- und Glacier-Daten werden vor dem Import nicht entschlüsselt, werden jedoch verschlüsselt gespeichert. Die folgende Tabelle enthält eine Zusammenfassung der Verschlüsselungsoptionen für die einzelnen Import-/Export-Auftragstypen.

Import in Amazon S3		
Quelle	Ziel	Ergebnis
• Dateien in einem Gerätedateisystem • Daten vor dem Versand des Geräts mit TrueCrypt verschlüsseln	• Objekte in einem vorhandenen Amazon S3-Bucket • AWS entschlüsselt die Daten vor dem Importieren.	• Ein Objekt pro Datei • AWS löscht Ihr Speichergerät nach jedem Importauftrag vor dem Versand.
Export von Amazon S3		
Quelle	Ziel	Ergebnis
• Objekte in einem oder mehreren Amazon S3-Buckets • Passwort angeben, mit dem AWS die Daten verschlüsselt	• Dateien auf dem Speichergerät • AWS formatiert das Gerät. • AWS kopiert die Daten in einen verschlüsselten Dateicontainer auf dem Gerät.	• Eine Datei pro Objekt • AWS verschlüsselt die Daten vor dem Versand. • TrueCrypt wird zum Verschlüsseln der Dateien verwendet.

Import in Amazon Glacier		
Quelle	Ziel	Ergebnis
• Gesamtes Gerät • Die Daten mit einer Verschlüsselungsmethode Ihrer Wahl vor dem Versand verschlüsseln	• Ein Archiv in einem vorhandenen Amazon Glacier-Vault • AWS entschlüsselt das Gerät nicht.	• Das Geräte-Image wird als einzelnes Archiv gespeichert. • AWS löscht Ihr Speichergerät nach jedem Importauftrag vor dem Versand.
Import in Amazon EBS (Gerätekapazität < 1 TB)		
Quelle	Ziel	Ergebnis
• Gesamtes Gerät • Die Daten mit einer Verschlüsselungsmethode Ihrer Wahl vor dem Versand verschlüsseln	• Ein Amazon EBS-Snapshot • AWS entschlüsselt das Gerät nicht.	• Das Geräte-Image wird als einzelner Snapshot gespeichert. • Wenn das Gerät verschlüsselt war, ist auch das Image verschlüsselt. • AWS löscht Ihr Speichergerät nach jedem Importauftrag vor dem Versand.
Import in Amazon EBS (Gerätekapazität > 1 TB)		
Quelle	Ziel	Ergebnis
• Gesamtes Gerät • Die Daten mit einer Verschlüsselungsmethode Ihrer Wahl vor dem Versand verschlüsseln	• Mehrere Objekte in einem vorhandenen Amazon S3-Bucket • AWS entschlüsselt das Gerät nicht.	• Das Geräte-Image wird auf mehrere Snapshots von 1 TB aufgeteilt und die Teile werden als Objekte im S3-Bucket gespeichert, der in der Manifestdatei angegeben ist. • Wenn das Gerät verschlüsselt war, ist auch das Image verschlüsselt. • AWS löscht Ihr Speichergerät nach jedem Importauftrag vor dem Versand.

Nach Abschluss des Imports löscht AWS Import/Export die Inhalte Ihres Speichergeräts, damit bei der Rücklieferung kein Datenverlust eintreten kann. AWS überschreibt alle beschreibbaren Blöcke auf dem Speichergerät mit Nullen. Sie müssen das Gerät nach dem Vorgang neu partitionieren und formatieren. Wenn AWS die Daten auf dem Gerät nicht löschen kann, wird es zur Zerstörung vorgesehen und unser Supportteam nimmt über die E-Mail-Adresse in der Manifestdatei, die Sie mit dem Gerät senden, Kontakt mit Ihnen auf.

Beim internationalen Versand eines Geräts sind Angaben für den Zoll und bestimmte Pflichtfelder in der Manifestdatei, die an AWS gesendet wird, erforderlich. AWS Import/Export verwendet diese Angaben, um eingehende Lieferungen zu überprüfen und für ausgehende Lieferungen die Zollunterlagen zu erstellen. Erforderlich sind u. a. die Angabe, ob die Daten auf dem Gerät verschlüsselt werden, und die Klassifizierung der Verschlüsselungssoftware. Beim Versand verschlüsselter Daten in die USA oder aus den USA muss die Verschlüsselungssoftware der Klassifikation 5D992 gemäß den Ausfuhrbestimmungen der USA (United States Export Administration Regulations) entsprechen.

AWS Data Pipeline

Der AWS Data Pipeline-Service unterstützt Sie beim Verarbeiten und Übertragen von Daten zwischen verschiedenen Datenquellen in bestimmten Intervallen mithilfe datengesteuerter Workflows und integrierter Abhängigkeitsüberprüfung. Wenn Sie eine Pipeline erstellen, definieren Sie Datenquellen, Bedingungen, Ziele, Verarbeitungsschritte und einen Betriebsplan. Sobald Sie eine Pipeline definiert und aktiviert haben, wird sie automatisch dem angegebenen Plan entsprechend betrieben.

Mit AWS Data Pipeline müssen Sie sich nicht mehr um das Überprüfen von Ressourcenverfügbarkeit, Verwalten von voneinander abhängigen Aufgaben, Wiederholen einzelner Aufgaben nach Fehlern oder Timeouts oder Erstellen eines Fehlerbenachrichtigungssystems kümmern. AWS Data Pipeline übernimmt das Starten der AWS-Services und Ressourcen, welche die Pipeline zur Verwaltung Ihrer Daten braucht (z. B. Amazon EC2 oder EMR), und überträgt die Ergebnisse in den Speicher (z. B. Amazon S3, RDS, DynamoDB oder EMR).

Bei Verwendung der Konsole erstellt AWS Data Pipeline die erforderlichen IAM-Rollen und Richtlinien, einschließlich einer Liste von vertrauenswürdigen Entitäten. Mit IAM-Rollen wird bestimmt, auf welche Daten die Pipeline zu greifen und welche Aktionen sie ausführen kann. Wenn die Pipeline eine Ressource, wie eine EC2-Instanz, erstellt, bestimmen die IAM-Rollen darüber hinaus, welche Ressourcen und Aktionen für die EC2-Instanz zulässig sind. Wenn Sie eine Pipeline erstellen, geben Sie eine IAM-Rolle an, die Ihre Pipeline steuert, und eine andere IAM-Rolle, die die Ressourcen der Pipeline (die sogenannte „Ressourcenrolle“) steuert. Die Rolle kann in beiden Fällen identisch sein. Als Best Practice im Rahmen der Sicherheit wird empfohlen, die Mindestberechtigungen zu prüfen, die erforderlich sind, damit die Pipeline funktioniert, und die IAM-Rollen entsprechend zu definieren.

Wie bei den meisten AWS-Services stellt der AWS Data Pipeline-Service die Option sicherer Endpunkte (HTTPS) für den Zugriff über SSL bereit.

Amazon Simple Database (SimpleDB)-Sicherheit

Amazon SimpleDB ist ein nicht relationaler Datenspeicher, der die Datenbankverwaltung entlastet und Ihnen ermöglicht, Datenelemente über Webservice-Anforderungen zu speichern und abzufragen. Amazon SimpleDB erstellt und verwaltet mehrere geografisch verteilte Repliken der Kundendaten automatisch. So wird hohe Verfügbarkeit und Datenhaltbarkeit erreicht.

Die Daten in Amazon SimpleDB werden in Domains gespeichert, die Datenbanktabellen ähneln. Im Gegensatz zu Datenbanktabellen können Sie jedoch keine Funktionen über mehrere Domains ausführen. Amazon SimpleDB-APIs bieten Steuerelemente auf Domain-Ebene, die nur authentifizierten Zugriff durch den Domain-Ersteller erlauben. Daher behalten Sie die vollständige Kontrolle darüber, welche Benutzer auf Ihre Daten zugreifen können.

Amazon SimpleDB bietet kein eigenständiges ressourcenbasiertes Berechtigungssystem. Der Service wird jedoch in AWS IAM integriert, sodass Sie anderen Benutzern in Ihrem AWS-Konto Zugriff auf Amazon SimpleDB-Domains innerhalb des AWS-Kontos erteilen können. Der Zugriff auf einzelne Domains wird durch eine unabhängige Zugriffskontrollliste kontrolliert, die authentifizierte Benutzer den Domains zuordnen, die ihnen gehören. Ein mit AWS IAM erstellter Benutzer erhält nur Zugriff auf Vorgänge und Domains, für die er mit einer Richtlinie Berechtigungen erhalten hat.

Darüber hinaus muss jede Anforderung des SimpleDB-Service eine gültige HMAC-SHA-Signatur enthalten. Andernfalls wird die Anforderung abgelehnt. Beim Zugriff auf Amazon SimpleDB mit einem der AWS SDKs übernimmt das SDK den Authentifizierungsprozess. Beim Zugreifen auf Amazon SimpleDB mit einer REST-Anforderung müssen Sie Ihre AWS-Zugriffsschlüssel-ID, eine gültige HMAC-SHA-Signatur (entweder HMAC-SHA1 oder HMAC-SHA256) und einen Zeitstempel angeben, damit die Anforderung authentifiziert werden kann. AWS verwendet Ihre Zugriffsschlüssel-ID, um Ihren geheimen Zugriffsschlüssel abzurufen und eine Signatur aus den Anforderungsdaten und dem geheimen Zugriffsschlüssel mit demselben Algorithmus zu generieren, den Sie verwendet haben, um die Signatur zu berechnen, die sie mit der Anforderung gesendet haben. Wenn die von AWS generierte Signatur mit der in der Anforderung gesendeten Signatur übereinstimmt, wird die Anforderung als authentisch eingestuft. Wird keine Übereinstimmung festgestellt, wird die Anforderung verworfen und von AWS eine Fehlermeldung ausgegeben.

Auf Amazon SimpleDB kann über SSL-verschlüsselte Endpunkte zugegriffen werden. Auf die verschlüsselten Endpunkte kann vom Internet oder von Amazon EC2 aus zugegriffen werden. In Amazon SimpleDB gespeicherte Daten werden nicht von AWS verschlüsselt. Der Kunde kann Daten jedoch verschlüsseln, bevor sie in Amazon SimpleDB hochgeladen werden. Diese verschlüsselten Attribute sind nur im Rahmen eines GET-Vorgangs abrufbar. Sie können nicht im Rahmen einer Abfragefilterbedingung verwendet werden. Das Verschlüsseln von Daten vor dem Versenden an Amazon SimpleDB trägt zum Schutz gegen Zugriff auf vertrauliche Kundendaten durch Dritte, einschließlich AWS, bei.

Wenn eine Domain aus Amazon SimpleDB gelöscht wird, wird die Entfernung der Zuordnung der Domain sofort gestartet und im Allgemeinen innerhalb von Sekunden im gesamten verteilten System verarbeitet. Sobald die Zuordnung entfernt ist, besteht kein Remotezugriff mehr auf die gelöschte Domain.

Wenn Element- und Attributdaten in einer Domain gelöscht werden, wird die Entfernung der Domain-Zuordnung sofort gestartet und im Allgemeinen innerhalb von Sekunden systemweit abgeschlossen. Sobald die Zuordnung entfernt ist, besteht kein Remotezugriff mehr auf die gelöschten Daten. Der entsprechende Speicherbereich wird dann nur für Schreibvorgänge verfügbar gemacht und die Daten werden von den neu gespeicherten Daten überschrieben.

In Amazon SimpleDB gespeicherte Daten werden an mehreren physischen Standorten im Rahmen des normalen Betriebs dieser Services und ohne Zusatzkosten gespeichert. Amazon SimpleDB gewährleistet die Haltbarkeit von Objekten, indem die Objekte beim ersten Schreibvorgang mehrfach über mehrere Availability Zones hinweg gespeichert und dann aktiv weiter repliziert werden, wenn das Gerät unverfügbar wird oder eine Beschädigung erkannt wird.

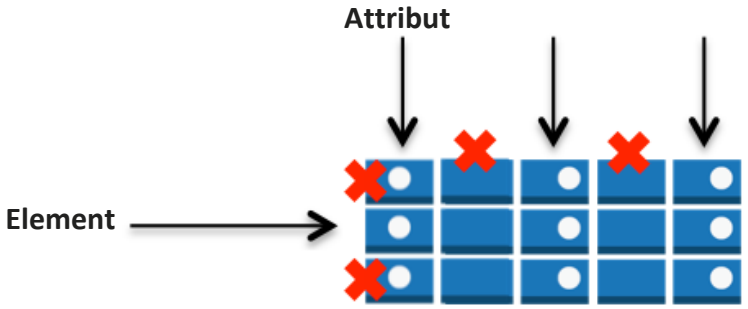
Amazon DynamoDB-Sicherheit

Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service von AWS. Er bietet schnelle und planbare Leistung mit nahtloser Skalierbarkeit. Mit Amazon DynamoDB können Sie den Verwaltungsaufwand für den Betrieb und die Skalierung verteilter Datenbanken in AWS verringern, sodass Sie sich nicht um Hardware-Bereitstellung, Einrichtung und Konfiguration, Replikation, Software-Patching oder Cluster-Skalierung kümmern müssen.

Sie können eine Datenbanktabelle erstellen, mit der eine beliebige Datenmenge gespeichert und abgerufen werden kann und der Anforderungsdatenverkehr verarbeitet werden kann. DynamoDB verteilt die Daten und den Datenverkehr für die Tabelle automatisch über eine entsprechende Anzahl von Servern, um die von Ihnen gewählte Anforderungskapazität und Datenmenge mit gleichbleibender konsistenter und schneller Leistung zu verarbeiten. Alle Datenelemente werden in Solid State Drives (SSD) gespeichert und automatisch über mehrere Availability Zones in einer Region repliziert, um eine integrierte Hochverfügbarkeit und Datenhaltbarkeit bereitzustellen.

Sie können automatische Sicherungen mit einer speziellen Vorlage in AWS Data Pipeline einrichten, die eigens zum Kopieren von DynamoDB-Tabellen erstellt wurde. Sie können vollständige oder inkrementelle Sicherungen in einer Tabelle in der gleichen Region oder einer anderen Region wählen. Sie können die Kopie für die Notfallwiederherstellung verwenden, falls die Originaltabelle durch einen Fehler im Code beschädigt wird, oder um die DynamoDB-Daten zwecks Unterstützung einer multi-regionalen Anwendung über mehrere Regionen zu verbinden.

In AWS IAM können Sie Berechtigungen einrichten, um zu kontrollieren, wer die DynamoDB-Ressourcen und die API verwenden kann. Neben der Zugriffskontrolle auf Ressourcenebene in IAM können Sie außerdem den Zugriff auf Datenbankebene kontrollieren. Sie können Berechtigungen auf Datenbankebene erstellen, die den Zugriff auf Elemente (Zeilen) und Attribute (Spalten) basierend auf den Anforderungen Ihrer Anwendung zulassen oder verweigern. Diese Berechtigungen auf Datenbankebene werden als *differenzierte Zugriffssteuerungselemente* bezeichnet. Sie werden mit einer IAM-Richtlinie erstellt, die angibt, unter welchen Umständen ein Benutzer oder eine Anwendung auf eine DynamoDB-Tabelle zugreifen kann. Die IAM-Richtlinie kann den Zugriff auf einzelne Elemente in einer Tabelle oder auf die Attribute dieser Elemente oder auf beides gleichzeitig beschränken.



Sie können wahlweise den Web-Identitätsverbund verwenden, um den Zugriff von Anwendungsbenutzern zu kontrollieren, die mithilfe der Anmeldedaten von Amazon, Facebook oder Google authentifiziert werden. Mit dem Web-Identitätsverbund ist es nicht mehr erforderlich, einzelne IAM-Benutzer zu erstellen. Stattdessen können sich Benutzer bei einem Identitätsanbieter anmelden und temporäre Sicherheitsanmeldeinformationen vom AWS Security Token Service (AWS STS) erhalten. AWS STS gibt temporäre AWS-Anmeldedaten an die Anwendung zurück und erlaubt ihr den Zugriff auf die konkrete DynamoDB-Tabelle.

Es sind jedoch nicht nur Datenbank- und Benutzerberechtigungen erforderlich. Jede Anforderung an den DynamoDB-Service muss eine gültige HMAC-SHA256-Signatur enthalten. Andernfalls wird die Anforderung abgelehnt. Die AWS SDKs signieren Ihre Anforderungen automatisch. Wenn Sie eigene HTTP POST-Anforderungen schreiben möchten, müssen Sie die Signatur im Header Ihrer Anforderung an Amazon DynamoDB angeben. Zum Berechnen der Signatur müssen Sie temporäre Sicherheitsanmeldedaten vom AWS Security Token Service anfordern. Verwenden Sie die temporären Sicherheitsanmeldedaten, um Ihre Anforderungen an Amazon DynamoDB zu signieren.

Auf Amazon DynamoDB kann über SSL-verschlüsselte Endpunkte zugegriffen werden. Auf die verschlüsselten Endpunkte kann vom Internet oder von Amazon EC2 aus zugegriffen werden.

Sicherheit bei Amazon Relational Database Service (Amazon RDS)

Mit Amazon RDS können Sie schnell eine relationale Datenbank (DB)-Instanz erstellen. Auch die zugewiesene Verarbeitungsressource und Speicherkapazität lässt sich entsprechend der Anforderung der Anwendung flexibel skalieren. Amazon RDS verwaltet die Datenbank-Instanz für Sie durch Ausführen von Sicherungen, Verarbeiten von Failover und Pflege der Datenbanksoftware. Derzeit ist Amazon RDS für MySQL, Oracle oder Microsoft SQL-Server- und PostgreSQL-Datenbank-Engines verfügbar.

Amazon RDS verfügt über mehrere Funktionen, welche die Zuverlässigkeit kritischer Produktionsdatenbanken erhöhen. Dazu zählen DB-Sicherheitsgruppen, Berechtigungen, SSL-Verbindungen, automatische Sicherungen, DB-Snapshots und Multi-AZ-Bereitstellungen. DB-Instanzen können außerdem in einer Amazon VPC bereitgestellt werden, um eine zusätzliche Netzwerkisolation zu erreichen.

Zugriffskontrolle

Wenn Sie erstmals eine DB-Instanz in Amazon RDS erstellen, legen Sie ein Masterbenutzerkonto an, das nur im Zusammenhang mit Amazon RDS zur Kontrolle des Zugriffs auf Ihre DB-Instanz(en) verwendet wird. Das Masterbenutzerkonto ist ein systemeigenes Datenbankbenutzerkonto, mit dem Sie sich bei Ihrer DB-Instanz mit allen Datenbankrechten anmelden können. Beim Erstellen der DB-Instanz können Sie den Masterbenutzernamen und das Passwort, die mit jeder DB-Instanz verknüpft werden sollen, angeben. Sobald Sie Ihre DB-Instanz erstellt haben, können Sie mit den Masterbenutzeranmeldedaten eine Verbindung mit der Datenbank herstellen. Anschließend können Sie zusätzliche Benutzerkonten erstellen, sodass Sie beschränken können, wer auf Ihre DB-Instanz zugreifen kann.

Sie können den Zugriff auf die Amazon RDS DB-Instanz über DB-Sicherheitsgruppen kontrollieren, die den Amazon EC2-Sicherheitsgruppen ähneln, jedoch mit diesen nicht zu verwechseln sind. DB-Sicherheitsgruppen fungieren wie eine Firewall. Sie steuern den Netzwerkzugriff auf die DB-Instanz. Die Datenbanksicherheitsgruppen verwenden standardmäßig den Zugriffsmodus „alles verweigern“ und Kunden müssen den Netzwerkzugang speziell autorisieren. Dazu stehen zwei Möglichkeiten zur Verfügung: Autorisierung eines Netzwerk-IP-Bereichs oder Autorisierung einer vorhandenen Amazon EC2-Sicherheitsgruppe. DB-Sicherheitsgruppen lassen nur den Zugriff auf den Datenbankserverport zu (alle anderen sind blockiert) und können aktualisiert werden, ohne die Amazon RDS DB-Instanz neu zu starten. So können Kunden ihren Datenbankzugriff nahtlos kontrollieren. Mit AWS IAM können Sie den Zugriff auf Ihre RDS DB-Instanzen weiter kontrollieren. Mit AWS IAM können Sie kontrollieren, welche RDS-Vorgänge jeder einzelne AWS IAM-Benutzer aufrufen darf.

Netzwerkisolation

Eine weitere Netzwerkzugriffskontrolle erhalten Sie, wenn Sie die DB-Instanzen in einer Amazon VPC ausführen. Mit der Amazon VPC können Sie Ihre DB-Instanzen isolieren, indem Sie den IP-Bereich angeben, den Sie verwenden möchten, und sie über ein branchenübliches verschlüsseltes IPsec VPN mit Ihrer vorhandenen IT-Infrastruktur verbinden. Durch das Ausführen von Amazon RDS in einer VPC ist eine DB-Instanz innerhalb eines privaten Subnetzes möglich. Sie können auch ein virtuelles privates Gateway einrichten, das Ihr Unternehmensnetzwerk auf Ihre VPC erweitert und den Zugriff auf die RDS DB-Instanz in dieser VPC zulässt. Weitere Informationen erhalten Sie im Amazon VPC User Guide.

In Multi-AZ-Bereitstellungen kann Amazon RDS durch Definieren eines Subnetzes für alle Availability Zones in einer Region eine neue Standby-DB in einer anderen Availability Zone erstellen, sofern sich ein entsprechender Bedarf ergibt. Sie können DB-Subnetzgruppen erstellen. Hierbei handelt es sich um Sammlungen von Subnetzen, die Sie für Ihre RDS DB-Instanzen in einer VPC ausweisen können. Jede DB-Subnetzgruppe sollte über mindestens ein Subnetz für jede Availability Zone in einer bestimmten Region verfügen. In diesem Fall wählen Sie beim Erstellen einer DB-Instanz in einer VPC eine DB-Subnetzgruppe aus. Amazon RDS verwendet diese DB-Subnetzgruppe und Ihre bevorzugte Availability Zone

dann, um ein Subnetz und eine IP-Adresse in diesem Subnetz auszuwählen. Amazon RDS erstellt ein Elastic Network Interface und verknüpft es mit Ihrer DB-Instanz mit der entsprechenden IP-Adresse.

Auf DB Instanzen, die in einer Amazon VPC bereitgestellt werden, kann über das Internet oder von Amazon EC2-Instanzen außerhalb der VPC über VPN oder Bastions-Hosts zugegriffen werden, die Sie in Ihrem öffentlichen Subnetz starten können. Um einen Bastions-Host zu verwenden, müssen Sie ein öffentliches Subnetz mit einer EC2-Instanz einrichten, die als SSH-Bastion fungiert. Dieses öffentliche Subnetz muss über ein Internet-Gateway und Routing-Regeln verfügen, die zulassen, dass der Datenverkehr über den SSH-Host weitergeleitet wird. Der Host leitet die Anforderungen dann an die private IP-Adresse Ihrer Amazon RDS DB-Instanz weiter.

DB-Sicherheitsgruppen können zur Sicherung von DB-Instanzen innerhalb einer Amazon VPC verwendet werden. Darüber hinaus kann der ein- und ausgehende Datenverkehr der einzelnen Subnetze über Netzwerkzugriffskontrolllisten zugelassen oder verweigert werden. Der gesamte über Ihre IPsec VPN-Verbindung in Ihre Amazon VPC ein- bzw. ausgehende Datenverkehr kann von Ihrer lokalen Sicherheitsinfrastruktur, einschließlich Netzwerk-Firewalls und Angriffserkennungssysteme, überprüft werden.

Verschlüsselung

Sie können Verbindungen zwischen Ihrer Anwendung und Ihrer DB-Instanz mit SSL verschlüsseln. Für MySQL und SQL Server erstellt RDS ein SSL-Zertifikat und installiert das Zertifikat auf der DB-Instanz, wenn die Instanz bereitgestellt wird. Für MySQL starten Sie den MySQL Client mit dem Parameter „--ssl_ca“, um auf den öffentlichen Schlüssel zu verweisen und die Verbindungen zu verschlüsseln. Für SQL Server laden Sie den öffentlichen Schlüssel herunter und importieren Sie das Zertifikat in das Windows-Betriebssystem. Oracle RDS verwendet die systemeigene Netzwerkverschlüsselung von Oracle mit einer DB-Instanz. Dazu fügen Sie einfach die systemeigene Netzwerkverschlüsselungsoption zu einer Optionsgruppe hinzu und verknüpfen diese Optionsgruppe mit der DB-Instanz. Sobald eine verschlüsselte Verbindung hergestellt ist, werden die Daten, die zwischen der DB-Instanz und Ihrer Anwendung übertragen werden, während der Übertragung verschlüsselt. Sie können auch festlegen, dass Ihre DB-Instanz nur verschlüsselte Verbindungen akzeptiert.

Amazon RDS unterstützt Transparent Data Encryption (TDE) für SQL Server (SQL Server Enterprise Edition) und Oracle (Bestandteil der Oracle Advanced Security Option der Oracle Enterprise Edition). Mit der TDE-Funktion werden Daten vor dem Speichern automatisch verschlüsselt und beim Abruf aus dem Speicher automatisch entschlüsselt. Wenn MySQL-Daten im Ruhezustand in der Datenbank verschlüsselt werden müssen, muss Ihre Anwendung die Verschlüsselung und Entschlüsselung von Daten vornehmen.

Beachten Sie, dass die Unterstützung von SSL innerhalb von Amazon RDS zur Verschlüsselung der Verbindung zwischen Ihrer Anwendung und Ihrer DB-Instanz dient. Er ist nicht zur Authentifizierung der DB-Instanz selbst geeignet.

SSL bietet zwar Sicherheitsvorteile, doch die SSL-Verschlüsselung ist ein berechnungsintensiver Vorgang und erhöht die Latenz Ihrer Datenbankverbindung. Weitere Informationen zur Funktionsweise von SSL mit MySQL erhalten Sie in der MySQL-Dokumentation. Informationen zur Funktionsweise von SSL mit SQL Server erhalten Sie im RDS User Guide.

Automatisierte Sicherungen und DB-Snapshots

Amazon RDS stellt zwei verschiedene Methoden zur Sicherung und Wiederherstellung Ihrer DB-Instanz(en) bereit: automatisierte Sicherungen und Datenbank-Snapshots (DB-Snapshots).

Die automatisierte Sicherungsfunktion von Amazon RDS ist standardmäßig aktiviert und ermöglicht eine Zeitpunktwiederherstellung Ihrer DB-Instanz. Amazon RDS sichert Ihre Datenbank und Transaktionsprotokolle und speichert beides für eine benutzerdefinierte Aufbewahrungsfrist. So können Sie Ihre DB-Instanz auf jede Sekunde

innerhalb Ihrer Aufbewahrungsfrist bis zu den letzten 5 Minuten wiederherstellen. Die Aufbewahrungsfrist für die automatische Sicherung kann auf maximal 35 Tage festgelegt werden.

Während des Sicherungsfensters kann die Speicherein- und -ausgabe unterbrochen werden, solange die Daten gesichert werden. Dieser Vorgang dauert in der Regel einige Minuten. Die E/A-Unterbrechung wird bei Multi-AZ-DB-Bereitstellungen vermieden, da die Sicherung aus dem Standby erfolgt.

DB-Snapshots sind vom Benutzer initiierte Sicherungen Ihrer DB-Instanz. Diese vollständigen Datenbanksicherungen werden von Amazon RDS gespeichert, bis Sie diese explizit löschen. Sie können DB-Snapshots einer beliebigen Größe kopieren und zwischen den öffentlichen Regionen von AWS verschieben oder denselben Snapshot gleichzeitig in mehrere Regionen kopieren. Sie können bei Bedarf dann eine neue DB-Instanz von einem DB-Snapshot erstellen.

DB-Instanz-Replikation

Die Cloud Computing-Ressourcen von Amazon sind in hochverfügbaren Rechenzentren in verschiedenen Regionen weltweit untergebracht. Jede Region enthält mehrere getrennte Standorte, die als Availability Zones bezeichnet werden. Jede Availability Zone ist so konzipiert, dass Sie vor Fehlern in anderen Availability Zones geschützt sind und eine kostengünstige Netzwerkkonnektivität mit geringer Latenz zu anderen Availability Zones in der gleichen Region bereitstellen.

Zur Herstellung von Hochverfügbarkeit Ihrer Oracle-, PostgreSQL- oder MySQL-Datenbanken können Sie Ihre RDS DB-Instanz in mehreren Availability Zones ausführen. Diese Option wird als Multi-AZ-Bereitstellung bezeichnet. Bei Auswahl dieser Option stellt Amazon automatisch eine synchrone Standby-Replikation Ihrer DB-Instanz in einer anderen Availability Zone bereit und verwaltet diese. Die primäre DB-Instanz wird über die Availability Zonen hinweg synchron auf die Standby-Replik repliziert. Bei Ausfall der DB-Instanz oder Availability Zone führt Amazon RDS automatisch ein Failover zum Standby aus, sodass die Datenbankvorgänge ohne Verwaltungseingriff schnell wieder aufgenommen werden können.

Für Kunden, die MySQL verwenden und über die Kapazitätsgrenzen einer einzelnen DB-Instanz für leseintensive Anwendungsaufgaben hinaus skalieren müssen, bietet Amazon RDS die Option „Read Replica“. Sobald Sie eine „Read Replica“ erstellen, werden die Datenbankaktualisierungen in der Quell-DB-Instanz mit der systemeigenen, asynchronen Replikation von MySQL auf die Read Replica repliziert. Sie können mehrere Read Replicas für eine bestimmte Quell-DB-Instanzen erstellen und den Lesedatenverkehr Ihrer Anwendung auf sie verteilen. Read Replicas können mit Multi-AZ-Bereitstellungen erstellt werden, um Leseskalierungsvorteile zusätzlich zur verbesserten Verfügbarkeit von Datenbankschreibvorgängen und Datenhaltbarkeit zu erhalten, die durch Multi-AZ-Bereitstellungen ermöglicht werden.

Automatisches Software-Patching

Amazon RDS stellt sicher, dass die relationale Datenbank-Software, die der Bereitstellung zugrunde liegt, mit den aktuellen Patches auf dem neuesten Stand bleibt. Bei Bedarf werden Patches in einem Wartungsfenster angewendet, das Sie festlegen können. Sie können sich das Amazon RDS-Wartungsfenster als Möglichkeit vorstellen, zu kontrollieren wann Änderungen der DB-Instanz (wie eine Skalierung der DB-Instanz-Klasse) und Software-Patching vorgenommen werden, wenn diese angefordert oder erforderlich sind. Wenn ein Wartungsereignis für eine bestimmte Woche geplant ist, wird es initiiert und an einem bestimmten Punkt während des 30-minütigen Wartungsfensters, das Sie angeben, abgeschlossen.

Die einzigen Wartungsereignisse, für die erforderlich ist, dass Amazon RDS die DB-Instanz offline schaltet, sind Skalierungsberechnungsvorgänge (die im Allgemeinen von Anfang bis Ende nur wenige Minuten dauern) oder notwendiges Software-Patching. Notwendiges Patching wird automatisch nur für Patches geplant, die sich auf die Sicherheit und Haltbarkeit beziehen. Dieses Patching erfolgt unregelmäßig (in der Regel nur einmal alle paar Monate)

und sollte meistens nur einen Bruchteil Ihres Wartungsfensters in Anspruch nehmen. Wenn Sie beim Erstellen Ihrer DB-Instanz kein bevorzugtes wöchentliches Wartungsfenster angeben, wird ein Standardwert von 30 Minuten zugewiesen. Wenn Sie den Ausführungszeitpunkt der automatischen Wartung ändern möchten, können Sie dazu Ihre DB-Instanz in der AWS Management Console ändern oder die API „ModifyDBInstance“ verwenden. Für jede DB-Instanz kann bei Bedarf ein anderes bevorzugtes Wartungsfenster festgelegt werden.

Wenn Sie Ihre DB-Instanz als Multi-AZ-Bereitstellungen ausführen, können Sie die Auswirkungen eines Wartungsereignisses weiter reduzieren, da Amazon RDS die Wartung über die folgenden Schritte ausführt: 1) Wartung am Standby ausführen, 2) Standby auf Primär hochstufen und 3) Wartung an der alten primären Instanz vornehmen, die dann zum neuen Standby wird

Wenn eine API zum Löschen der Amazon RDS DB-Instanzen („DeleteDBInstance“) ausgeführt wird, wird die DB-Instanz zum Löschen markiert. Sobald die Instanz nicht mehr den Status „wird gelöscht“ anzeigt, ist sie entfernt. An diesem Punkt ist kein Zugriff auf die Instanz mehr möglich. Sie kann nicht wiederhergestellt werden und wird von keinem der Tools oder APIs aufgelistet, es sei denn, es wurde eine letzte Snapshot-Kopie angefordert.

Ereignisbenachrichtigung

Sie können Benachrichtigungen für verschiedene wichtige Ereignisse erhalten, die in der RDS-Instanz auftreten können. Dazu zählen, ob die Instanz heruntergefahren, eine Sicherung gestartet, ein Failover aufgetreten, die Sicherheitsgruppe geändert wurde oder wenig Speicherplatz vorhanden ist. Der Amazon RDS-Service stuft Ereignisse in Kategorien ein, die Sie abonnieren können. So werden Sie benachrichtigt, wenn ein Ereignis in dieser Kategorie auftritt. Sie können eine Ereigniskategorie für eine DB-Instanz, einen DB-Snapshot, eine DB-Sicherheitsgruppe oder für eine DB-Parametergruppe abonnieren. RDS-Ereignisse werden über AWS SNS veröffentlicht und als E-Mail oder Textnachricht an Sie gesendet. Weitere Informationen über Ereigniskategorien für die RDS-Benachrichtigung erhalten Sie im RDS User Guide.

Sicherheit bei Amazon RedShift

Amazon Redshift ist ein SQL-Data Warehouse-Service in Petabytegröße. Er wird auf hochgradig optimierten und vollständig verwalteten AWS-Rechen- und Speicherressourcen ausgeführt. Der Service wurde daraufhin ausgelegt, schnell in beide Richtungen zu skalieren und die Abfragegeschwindigkeit auch bei extrem großen Datensätzen deutlich zu beschleunigen. Bei Redshift wird die Leistung durch Techniken, wie spaltenweise Speicherung, Datenkompression und Bereichskarten, erhöht. Damit wird die Menge der zur Durchführung von Abfragen erforderlichen Ein- und Ausgaben verringert. Das Data Warehouse basiert zudem auf einer MPP-Architektur (Massively Parallel Processing). Dadurch können SQL-Vorgänge parallel durchgeführt und verteilt werden, so dass alle verfügbaren Ressourcen genutzt werden.

Für ein Redshift-Data Warehouse müssen Sie einen Cluster mit mindestens einem Knoten bereitstellen und den Typ sowie die Anzahl der Knoten des Clusters festlegen. Der Knotentyp bestimmt den Speicherplatz, den Arbeitsspeicher und die CPU jedes Knotens. Jeder Cluster mit mehreren Knoten verfügt über einen Hauptknoten und mindestens zwei Verarbeitungsknoten. Ein Hauptknoten verwaltet Verbindungen, leitet Abfragen weiter, erstellt Ausführungspläne und verwaltet die Durchführung der Abfragen in den Verarbeitungsknoten. Die Verarbeitungsknoten speichern entsprechend der Anweisungen des Hauptknotens Daten, führen Berechnungen durch und Abfragen aus. Auf die Hauptknoten jedes Clusters kann mithilfe standardmäßiger PostgreSQL-Treiber über ODBC- und JDBC-Endpunkte zugegriffen werden. Die Verarbeitungsknoten werden auf einem getrennten, isolierten Netzwerk ausgeführt. Auf sie wird niemals direkt zugegriffen.

Sobald Sie einen Cluster bereitgestellt haben, können Sie Ihren Datensatz hochladen und mithilfe üblicher SQL-basierter Werkzeuge und Business-Intelligence-Anwendungen Abfragen zur Datenanalyse durchführen.

Clusterzugriff

Standardmäßig sind die von Ihnen erstellten Cluster für jeden geschlossen. Mit Amazon Redshift können Sie Firewall-Regeln (Sicherheitsgruppen) erstellen und so den Zugriff auf das Netzwerk des Data Warehouse-Clusters kontrollieren. Sie können Redshift auch innerhalb einer Amazon VPC ausführen. Der Data Warehouse-Cluster wird dann im eigenen virtuellen Netzwerk isoliert und mithilfe eines dem Industriestandard entsprechenden verschlüsselten IPsec-VPN mit der vorhandenen IT-Infrastruktur verbunden.

Das AWS-Konto, von dem der Cluster erstellt wird, hat vollen Zugriff auf diesen Cluster. Innerhalb des AWS-Kontos können Sie mit AWS IAM Benutzerkonten erstellen und Berechtigungen für diese Konten verwalten. Mit IAM können Sie Benutzern die Berechtigungen für verschiedene Clustervorgänge erteilen, die für ihre Arbeit erforderlich sind.

Wie bei allen Datenbanken, müssen Sie bei Redshift auf Datenbankebene Berechtigung erteilen und den Zugriff auf Ressourcenebene gewähren. Datenbankbenutzer sind named user-Konten, die eine Verbindung mit der Datenbank herstellen können und bei der Anmeldung bei Amazon Redshift authentifiziert werden. Bei Redshift vergeben Sie Datenbankbenutzern Berechtigungen pro Cluster und nicht pro Tabelle. Allerdings werden einem Benutzer nur die Tabellenzeilen angezeigt, die durch seine eigenen Aktivitäten erstellt worden sind. Zeilen anderer Benutzer sind für ihn nicht sichtbar.

Ein Benutzer, der ein Datenbankobjekt erstellt, ist dessen Besitzer. Standardmäßig kann nur ein Hauptbenutzer oder der Besitzer eines Objekts Abfragen für dieses Objekt durchführen, es bearbeiten oder Berechtigungen dafür vergeben. Die Verwendung eines Objektes erfordert die Erteilung entsprechender Berechtigungen an den Benutzer bzw. an die Gruppe, der der Benutzer zugehört. Und nur der Besitzer eines Objekts kann es bearbeiten oder löschen.

Datensicherungen

Amazon Redshift verteilt die Daten über alle Rechenknoten in einem Cluster. Bei Clustern mit mindestens zwei Verarbeitungsknoten werden die Daten jedes Knotens immer auf Datenträgern eines anderen Knotens gespiegelt. So wird das Risiko eines Datenverlusts verringert. Außerdem werden alle auf einen Knoten im Cluster geschriebenen Daten stetig mit Snapshots in Amazon S3 gesichert. Redshift speichert die Snapshots für eine vom Benutzer definierte Zeitspanne von 1 bis zu 35 Tagen. Sie können auch jederzeit eigene Snapshots aufnehmen. Diese nutzen alle vorhandenen System-Snapshots und werden gespeichert, bis Sie sie explizit löschen.

Amazon Redshift überwacht den Status der Cluster kontinuierlich. Daten auf fehlerhaften Geräten werden automatisch neu repliziert und Knoten, falls erforderlich, ersetzt. All das geschieht ohne einen Eingriff von Ihrer Seite. Allerdings werden Sie während der erneuten Replizierung möglicherweise leichte Leistungseinbußen bemerken.

Sie können den Cluster mithilfe der AWS Management Console oder der Amazon Redshift APIs mit jedem System- oder Benutzer-Snapshot wiederherstellen. Der Cluster ist verfügbar, sobald die Metadaten des Systems wiederhergestellt wurden. Sie können dann schon Abfragen durchführen, während im Hintergrund noch die Benutzerdaten aufgespielt werden.

Datenverschlüsselung

Sie können einen Cluster bei der Erstellung verschlüsseln und Ihre ruhenden Daten so zusätzlich schützen. Bei aktiver Clusterverschlüsselung speichert Amazon Redshift alle Daten in vom Benutzer erstellten Tabellen in verschlüsselter Form. Dazu werden hardwarebeschleunigte AES-256-Blockverschlüsselungsschlüssel verwendet. Das gilt für alle Daten, die auf den Datenträger geschrieben werden und jede Sicherung.

Amazon Redshift verwendet zur Verschlüsselung eine schlüsselbasierte Architektur mit vier Ebenen. Diese bestehen aus den Schlüsseln zur Datenverschlüsselung, einem Datenbankschlüssel, einem Clusterschlüssel und einem Hauptschlüssel:

- *Schlüssel zur Datenverschlüsselung* verschlüsseln Datenblöcke im Cluster. Jedem Datenblock wird ein zufällig generierter AES-256-Schlüssel zugewiesen. Diese Schlüssel werden mithilfe des Datenbankschlüssels für den Cluster verschlüsselt.
- Der *Datenbankschlüssel* verschlüsselt die Schlüssel zur Datenverschlüsselung im Cluster. Der Datenbankschlüssel ist ein zufällig generierter AES-256-Schlüssel. Er wird auf einem Datenträger in einem vom Amazon Redshift-Cluster getrennten Netzwerk gespeichert und mit dem Hauptschlüssel verschlüsselt. Amazon Redshift gibt den Datenbankschlüssel über einen sicheren Kanal weiter. Er wird zudem im Arbeitsspeicher des Clusters belassen.
- Der *Clusterschlüssel* verschlüsselt den Datenbankschlüssel für den Amazon Redshift-Cluster. Sie können den Clusterschlüssel mit AWS oder einem Hardware-Sicherheitsmodul (HSM) speichern. Hardware-Sicherheitsmodule bieten eine direkte Kontrolle der Schlüsselerstellung und -verwaltung. Sie ermöglichen so eine von der Anwendung und der Datenbank getrennte und eindeutige Schlüsselverwaltung.
- Der *Hauptschlüssel* verschlüsselt den Clusterschlüssel, wenn er in AWS gespeichert wird. Der Hauptschlüssel verschlüsselt den mit dem Clusterschlüssel verschlüsselten Datenbankschlüssel, wenn der Clusterschlüssel in einem Hardware-Sicherheitsmodul gespeichert wird.

Sie können die kryptografischen Schlüssel für die verschlüsselten Cluster mit Redshift jederzeit rotieren lassen. Dabei werden Schlüssel auch für alle automatischen und manuellen Snapshots des Clusters aktualisiert.

Beachten Sie, dass die Aktivierung der Verschlüsselung im Cluster Einfluss auf die Leistung haben wird, obwohl sie hardwarebeschleunigt ist. Die Verschlüsselung betrifft auch Sicherungen. Bei Wiederherstellung aus einem verschlüsselten Snapshot, wird auch der neue Cluster verschlüsselt.

Mit der serverseitigen Verschlüsselung von Amazon S3 können Sie die Dateien mit den Ladedaten für die Tabelle beim Hochladen auf Amazon S3 verschlüsseln. Beim Laden der Daten aus Amazon S3 entschlüsselt der Befehl "COPY" die Daten während die Tabelle geladen wird.

Datenbank-Auditprotokollierung

Amazon Redshift protokolliert alle SQL-Vorgänge einschließlich Verbindungsversuche, Abfragen und Änderungen an Ihrer Datenbank. Sie können auf diese Protokolle mithilfe von SQL-Abfragen der Systemtabellen zugreifen oder sie in einen sicheren Amazon S3-Bucket herunterladen. Dann können Sie den Cluster mit diesen Auditprotokollen für Sicherheits- und Fehlerbehebungszwecke überwachen.

Automatisches Software-Patching

Amazon Redshift erledigt die gesamte mit dem Einrichten, Betreiben und Skalieren des Data Warehouses verbundene Arbeit. Dazu zählen auch die Bereitstellung von Kapazitäten, die Überwachung des Clusters und das Durchführen von Patches und Updates der Amazon Redshift-Engine. Patches werden nur während bestimmter Wartungsfenster durchgeführt.

SSL-Verbindungen

Um Ihre Daten bei der Übertragung innerhalb der AWS-Cloud zu schützen, verwendet Amazon Redshift ein hardwarebeschleunigtes SSL für die Kommunikation mit Amazon S3 oder Amazon DynamoDB bei COPY-, UNLOAD-, Sicherungs- und Wiederherstellungsvorgängen. Sie können die Verbindung zwischen Ihrem Client und dem Cluster verschlüsseln, indem Sie SSL in der Parametergruppe des Clusters auswählen. Der Client kann auch den Redshift-Server authentifizieren. Dazu können Sie den öffentlichen Schlüssel (.pem-Datei) für das SSL-Zertifikat auf dem Client installieren und mit dem Schlüssel dann eine Verbindung mit den Clustern herstellen.

Sicherheit bei Amazon ElastiCache

Amazon ElastiCache ist ein Web-Service, der das Einrichten, Verwalten und Skalieren verteilter In-Memory-Cache-Umgebungen in der Cloud vereinfacht. Der Service verbessert die Leistung von Webanwendungen. Er ermöglicht Ihnen, Informationen aus einem schnellen, verwalteten In-Memory-Cachesystem abzurufen, anstatt vollständig auf langsamere datenträgerbasierte Datenbanken angewiesen zu sein. Mit ihm kann die Latenz und der Durchsatz vieler leseintensiver Anwendungsaufgaben (z. B. soziale Netzwerke, Gaming, Medienfreigabe und Frage- und Antwort-Portale) oder rechenintensiver Aufgaben (wie bei einem Empfehlungsdienst) deutlich verbessert werden. Das Zwischenspeichern verbessert die Leistung von Anwendungen, indem kritische Datenbestandteile für einen Zugriff mit niedriger Latenz im Arbeitsspeicher abgelegt werden. Zwischengespeicherte Informationen umfassen auch die Ergebnisse ein- und ausgabeintensiver Datenbankabfragen oder berechnungsintensiver Berechnungen.

Der Amazon ElastiCache-Service automatisiert zeitaufwendige Verwaltungsaufgaben bei In-Memory-Cache-Umgebungen, z. B. Patchverwaltung, Fehlererkennung und Wiederherstellung. Er arbeitet mit anderen Amazon Web-Services (z. B. Amazon EC2, Amazon CloudWatch und Amazon SNS) zusammen. So wird ein sicherer, leistungsstarker und verwalteter In-Memory-Cache bereitgestellt. Beispielsweise kann eine in Amazon EC2 ausgeführte Anwendung mit sehr niedriger Latenz sicher auf einen Amazon ElastiCache-Cluster in der gleichen Region zugreifen.

Mit dem Amazon ElastiCache-Service können Sie einen Cache-Cluster erstellen. Dieser ist eine Sammlung mindestens eines Cache-Knotens, von denen jeder eine Instanz des Memcached-Service ausführt. Ein Cache-Knoten ist ein Teil eines sicheren, dem Netzwerk angefügten, RAMs fester Größe. Jeder Cache-Knoten führt eine Instanz des Memcached-Service aus. Er verfügt über einen eigenen DNS-Namen und -Port. Mehrere Arten von Cache-Knoten werden unterstützt, jeder mit unterschiedlich viel zugewiesenem Arbeitsspeicher. Ein Cache-Cluster mit einer bestimmten Anzahl von Cache-Knoten und einer Cache-Parametergruppe kann eingerichtet werden. Die Cache-Parametergruppe steuert die Eigenschaften jedes Cache-Knotens. Alle Cache-Knoten innerhalb eines Cache-Clusters gehören demselben Typ an und verfügen über die gleichen Einstellungen für Parameter- und Sicherheitsgruppen.

Amazon ElastiCache ermöglicht die Zugriffskontrolle der Cache-Cluster mithilfe von Cache-Sicherheitsgruppen. Eine Cache-Sicherheitsgruppe fungiert wie eine Firewall. Sie steuert den Netzwerkzugriff auf den Cache-Cluster. Standardmäßig ist der Netzwerkzugriff auf den Cache-Cluster ausgeschaltet. Damit die Anwendungen auf den Cache-Cluster zugreifen können, müssen Sie den Zugriff von Hosts in bestimmten EC2-Sicherheitsgruppen explizit aktivieren. Sobald Zugangsregeln konfiguriert sind, gelten die gleichen Regeln für alle der Cache-Sicherheitsgruppe zugeordneten Cache-Cluster.

Sie können Netzwerkzugriff auf den Cache-Cluster ermöglichen. Erstellen Sie dazu eine Cache-Sicherheitsgruppe und autorisieren Sie die gewünschte EC2-Sicherheitsgruppe (die wiederum die berechtigten EC2-Instanzen festlegt) mit der „Authorize Cache Security Group Ingress API“ oder dem Befehl „CLI“. Zugriffskontrolle auf Grundlage des IP-Bereichs ist für Cache-Cluster aktuell nicht aktiviert. Alle Clients eines Cache-Clusters müssen sich innerhalb des EC2-Netzwerks befinden und über Cache-Sicherheitsgruppen autorisiert werden.

Sicherheit bei Amazon Simple Queue Service (Amazon SQS)

Amazon SQS ist ein höchst zuverlässiger, skalierbarer Message Queuing Service, der eine asynchrone nachrichtenbasierte Kommunikation zwischen verteilten Komponenten einer Anwendung ermöglicht. Die Komponenten können Computer oder Amazon EC2-Instanzen oder eine Kombination aus beidem sein. Mit Amazon SQS können Sie von einer Komponente jederzeit eine beliebige Anzahl von Nachrichten an eine Amazon SQS-Warteschlange senden. Die Nachrichten können sofort oder zu einem späteren Zeitpunkt (innerhalb von vier Tagen) von der gleichen oder einer anderen Komponente abgerufen werden. Die Nachrichten sind sehr haltbar. Jede Nachricht wird dauerhaft in hochverfügbaren, sehr zuverlässigen Warteschlangen gespeichert. Mehrere Prozesse können gleichzeitige Lese-Schreibvorgänge bei einer Amazon SQS-Warteschlange durchführen, ohne sich gegenseitig zu beeinflussen.

Zugriff auf Amazon SQS wird auf Grundlage eines AWS-Kontos oder eines mit AWS IAM erstellten Benutzers gewährt. Sobald das AWS-Konto authentifiziert wurde, verfügt es über vollen Zugriff auf alle Benutzervorgänge. Ein AWS IAM-Benutzer erhält allerdings nur Zugriff auf Vorgänge und Warteschlangen, auf die er mit einer Richtlinie Zugriff erhalten hat. Standardmäßig ist der Zugriff auf einzelne Warteschlangen auf das AWS-Konto begrenzt, von dem sie erstellt wurden. Allerdings können Sie mithilfe einer SQS-erstellten oder von Ihnen geschriebenen Richtlinie darüber hinaus Zugriff auf die Warteschlange ermöglichen.

Auf Amazon SQS kann über SSL-verschlüsselte Endpunkte zugegriffen werden. Auf die verschlüsselten Endpunkte kann vom Internet oder von Amazon EC2 aus zugegriffen werden. Innerhalb von Amazon SQS gespeicherte Daten werden von AWS nicht verschlüsselt. Allerdings kann der Benutzer Daten vor dem Hochladen auf Amazon SQS verschlüsseln, sofern die Anwendung, die die Warteschlange nutzt, über die Mittel zur Entschlüsselung der Nachricht bei Erhalt verfügt. Das Verschlüsseln von Nachrichten vor ihrem Versenden an Amazon SQS trägt zum Schutz gegen Zugriff auf vertrauliche Kundendaten durch nicht autorisierte Personen, einschließlich AWS, bei.

Sicherheit bei Amazon Simple Notification Service (Amazon SNS)

Amazon Simple Notification Service (Amazon SNS) ist ein Web-Service zum einfachen Einrichten, Betreiben und Versenden von Meldungen aus der Cloud. Er bietet Entwicklern eine hoch skalierbare, flexible und kosteneffiziente Möglichkeit zum Veröffentlichen von Meldungen aus einer Anwendung und der sofortigen Zustellung an Abonnenten oder andere Anwendungen.

Amazon SNS stellt eine einfache Web-Service-Schnittstelle bereit. Damit können Kunden Themen erstellen, über die Anwendungen (oder Personen) benachrichtigt werden sollen. Sie können Clients diese Themen abonnieren lassen, Nachrichten veröffentlichen und diese Nachrichten über ein frei wählbares Clientprotokoll (z. B. HTTP/HTTPS, E-Mail usw.) zustellen. Amazon SNS stellt Benachrichtigungen an Clients mit einem „Push“-Mechanismus zu. Dadurch ist ein regelmäßiges Prüfen auf bzw. „Anfragen“ nach neuen Informationen oder Updates nicht mehr erforderlich. Mit Amazon SNS können hochgradig zuverlässige, ereignisgesteuerte Workflows und Nachrichtenanwendungen erstellt werden. Komplexe Middleware und Anwendungsmanagement sind dazu nicht notwendig. Die potenziellen Verwendungsmöglichkeiten für Amazon SNS umfassen die Überwachung von Anwendungen, Workflow-Systemen, zeitkritischen Informationsupdates, mobilen Anwendungen und vielem mehr. Amazon SNS bietet einen Mechanismus zur Zugriffskontrolle damit Themen und Nachrichten gegen nicht autorisierten Zugriff geschützt sind. Themenbesitzer können Richtlinien für ein Thema festlegen. Dadurch kann der Personenkreis, der veröffentlichen oder ein Thema abonnieren kann, begrenzt. Darüber hinaus können Themenbesitzer die Übertragung verschlüsseln, indem Sie den Zustellmechanismus auf HTTPS festlegen.

Zugriff auf Amazon SNS wird auf Grundlage eines AWS-Kontos oder eines mit AWS IAM erstellten Benutzers gewährt. Sobald das AWS-Konto authentifiziert wurde, verfügt es über vollen Zugriff auf alle Benutzervorgänge. Ein AWS IAM-Benutzer hat allerdings nur Zugriff auf Vorgänge und Themen, auf die er über eine Richtlinie Zugriff erhalten hat. Standardmäßig ist der Zugriff auf einzelne Themen auf das AWS-Konto begrenzt, mit dem sie erstellt wurden. Allerdings können Sie mithilfe einer SNS-erstellten oder einer von Ihnen geschriebenen Richtlinie darüber hinaus Zugriff auf SNS ermöglichen.

Sicherheit bei Amazon Simple Workflow Service (Amazon SWF)

Der Amazon Simple Workflow Service (SWF) vereinfacht das Erstellen von Anwendungen, die Aufgaben über verteilte Komponenten koordinieren. Mit Amazon SWF können Sie die verschiedenen Prozessschritte in einer Anwendung als „Tasks“ strukturieren, die die Arbeit in verteilten Anwendungen vorantreiben. Amazon SWF koordiniert diese Tasks in einer zuverlässigen und skalierbaren Form. Amazon SWF managet Abhängigkeiten bei der Ausführung von Tasks , Ablaufkoordination und Gleichzeitigkeit auf Grundlage der Anwendungslogik des Entwicklers. Der Service speichert Tasks, vergibt sie an Anwendungskomponenten und verfolgt den Fortschritt sowie den aktuellen Status.

Amazon SWF stellt einfache API-Aufrufe bereit, die von Code in einer beliebigen Sprache auf der EC2-Instanz oder auf jedem beliebigen Computer mit Internetzugang ausgeführt werden können. Amazon SWF fungiert als Koordinationszentrum, mit dem der Anwendungs-Host interagiert. Sie erstellen die gewünschten Workflows mit ihren jeweiligen Tasks und einer beliebigen Bedingungslogik und speichern diese mit Amazon SWF.

Zugriff auf Amazon SWF wird auf Grundlage eines AWS-Kontos oder eines mit AWS IAM erstellten Benutzers gewährt. Jeder an der Durchführung eines Workflows Beteiligte (Entscheidungsträger, Arbeitskräfte, Workflow-Administratoren) muss ein IAM-Benutzer unter dem AWS-Konto sein, das die Amazon SWF-Ressourcen besitzt. Sie können Benutzern, die anderen AWS-Konten zugewiesen sind, keinen Zugriff auf Ihre Amazon SWF-Workflows gewähren. Ein AWS IAM-Benutzer hat allerdings nur Zugriff auf diejenigen Workflows und Ressourcen, auf die ihm über eine Richtlinie Zugriff gewährt wurde.

Sicherheit bei Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) ist ein hochgradig skalierbarer und kosteneffizienter Massen- und Transaktions-E-Mail-Sendeservice für Unternehmen und Entwickler. Amazon SES beseitigt die Komplexität und den Aufwand bei der Erstellung einer eigenen E-Mail-Lösung oder der Lizenzierung, der Installation und dem Betrieb des E-Mail-Service eines Drittanbieters. Der Amazon SES-Service integriert sich in andere AWS-Services. Er vereinfacht so das Versenden von E-Mails aus Anwendungen, die auf einem Service wie Amazon EC2 betrieben werden.

Leider gibt es Menschen, die unerwünschte Massen-E-Mails oder Spam verschicken und die Identität anderer Personen vortäuschen, um die eigene zu verbergen. Um diese Probleme zu reduzieren, müssen neue Benutzer den Besitz ihrer E-Mail-Adresse oder Domäne nachweisen. So wird vermieden, dass sie von anderen Personen verwendet werden. Darüber hinaus überprüft AWS regelmäßig den Status des Domänennachweises und widerruft den Nachweis, wenn er nicht länger gültig ist.

Amazon SES unternimmt proaktive Schritte, um den Versand fragwürdiger Inhalte zu verhindern. So erhalten Internetanbieter E-Mails von gleichbleibend hoher Qualität und betrachten den Service daher als vertrauenswürdigen E-Mail-Ursprung. Dadurch wird die Zustellbarkeit und Zuverlässigkeit für alle unserer Versender maximiert. Im Folgenden finden Sie einige der vorhandenen Schutzmaßnahmen:

- Internetanbieter interpretieren den plötzlichen Anstieg der E-Mail-Menge häufig als einen potenziellen Indikator für Spam-Aktivität. Sie reagieren möglicherweise mit der Blockierung solcher E-Mails. Um Ihnen zu helfen, dies

zu vermeiden, hebt Amazon SES die Anzahl der E-Mails, die Sie vom Service versenden können, automatisch bis auf die Zielmenge an.

- Amazon SES setzt Technologien zur Filterung von Inhalten ein. Nachrichten mit Spam oder Malware werden so schon vor der Versendung erkannt und blockiert.
- Amazon SES unterhält Feedback-Loops der großen Internetanbieter. Feedback-Loops geben an, welche E-Mails von einem Empfänger als Spam markiert wurden. Amazon SES gewährt Ihnen Zugriff auf diese Zustellmetrik (für Ihre E-Mail-Kampagnen), um Ihnen bei Ihrer Versandstrategie zu helfen.

Amazon SES verwendet das Simple Mail Transfer Protokoll (SMTP) zur Versendung von E-Mails. An sich stellt SMTP keine Authentifizierung bereit. Ein Spammer kann also E-Mails versenden, die augenscheinlich von jemand anderem stammen, während der tatsächliche Ursprung verborgen bleibt. Die meisten Internetanbieter haben Schritte unternommen, um die Seriosität von E-Mails zu bewerten. Internetanbieter erwägen dazu die Authentifizierung von E-Mails. Dabei muss ein Versender den Besitz des Kontos nachweisen, von dem aus er sendet. In einigen Fällen weigern sich Internetanbieter, eine nicht authentifizierte E-Mail weiterzuleiten. Amazon SES unterstützt drei von Internetanbietern verwendete Authentifizierungs-Mechanismen zur Erkennung seriöser E-Mails: SPF, Sender-ID und DKIM. Für optimale Zustellbarkeit empfiehlt AWS SES-Kunden, diesen Standards zu folgen.

- Sender Policy Framework (SPF) stellt eine Möglichkeit zur Nachverfolgung einer E-Mail bis zu ihrem Ursprungssystem bereit. Möchte ein E-Mail-Versender SPF-konform sein, veröffentlicht er mindestens einen DNS-Datensatz, der die Identität der Sende-Domäne sicherstellt. Diese DNS-Datensätze werden für gewöhnlich als eine TXT-Datei (Text) angegeben. Sie identifizieren eine Anzahl von Hosts, die zum Senden von E-Mails autorisiert sind. Sobald diese DNS-Datensätze erstellt und veröffentlicht wurden, können Internetanbieter einen Host authentifizieren. Dazu vergleichen Sie dessen IP-Adresse mit dem Satz von IP-Adressen im SPF-Datensatz. Weitere Informationen zu SPF finden Sie unter www.openspf.org und RFC 4408.
- Sender ID ist ein SPF-ähnliches Authentifizierungssystem. Wie SPF ist Sender ID auf die Zusammenarbeit zwischen Versendern und Internetanbietern angewiesen. Nur so kann überprüft werden, ob eine E-Mail bis zu ihrem Ursprungssystem zurückverfolgt werden kann. Möchte ein E-Mail-Versender Sender ID-konform sein, veröffentlicht er mindestens einen DNS-Datensatz, der die Identität der Sende-Domäne sicherstellt. Weitere Informationen zu Sender ID finden Sie unter http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx and RFC 4406.
- DomainKeys Identified Mail (DKIM) ist ein Standard, der Versendern erlaubt, ihre E-Mails mit digitalen Signaturen zu versehen. Internetanbieter können mit diesen Signaturen die Seriosität dieser Nachrichten überprüfen. Ein Internetanbieter, der die Nachricht erhält, kann die kryptografische Signatur entschlüsseln. Er nutzt dafür einen öffentlichen Schlüssel, der im DNS-Datensatz des Versenders veröffentlicht wird. So kann er die Echtheit der Nachricht sicherstellen. Durch Signieren Ihrer E-Mails mit DKIM verbessern Sie die Zustellbarkeit von E-Mails über DKIM-konforme Internetanbieter. Weitere Informationen zu DKIM finden Sie unter http://www.dkim.org.

Möchten Sie die Amazon SES SMTP-Schnittstelle verwenden, müssen Sie zunächst einen SMTP-Benutzernamen und ein Kennwort erstellen. Diese Angaben müssen sich von Ihrem AWS-Zugriffsschlüssel und dem geheimen Zugriffsschlüssel unterscheiden. Sobald Sie Ihre SMTP-Zugangsdaten erhalten haben, können Sie mit der Versendung von E-Mails über Amazon SES mithilfe jeder E-Mail-Clientanwendung beginnen. Voraussetzung dafür ist, dass die Anwendung über SMTP kommunizieren und mithilfe von Transport Layer Security (TLS) eine Verbindung mit einem SMTP-Endpunkt herstellen kann. Sie konfigurieren den E-Mail-Client mit dem Hostnamen der Amazon SES SMTP-Schnittstelle (email-smtp.us-east-1.amazonaws.com) und der Portnummer sowie Ihrem SMTP-Benutzernamen und dem Kennwort.

Der Amazon SES SMTP-Endpunkt (email-smtp.us-east-1.amazonaws.com) erfordert, dass alle Verbindungen mithilfe von TLS verschlüsselt werden. Amazon SES unterstützt zwei Mechanismen zur Herstellung einer verschlüsselten Verbindung: STARTTLS und RLS Wrapper. Wird STARTTLS bzw. TLS Wrapper von der Software nicht unterstützt, können Sie mit dem Open Source Programm „Stunnel“ eine verschlüsselte Verbindung einrichten (dies wird als „Secure Tunnel“ bezeichnet). Dann können Sie mithilfe dieses sicheren Tunnels eine Verbindung mit dem Amazon SES SMTP Endpunkt herzustellen.

Zugriff auf Amazon SES wird auf Grundlage eines AWS-Kontos oder eines mit AWS IAM erstellten Benutzers gewährt. Ein AWS IAM-Benutzer hat allerdings nur Zugriff auf die administrativen Funktionen, für die ihm über eine Richtlinie Zugriff gewährt wurde.

Sicherheit bei Amazon Elastic Transcoder Service

Der Amazon Elastic Transcoder-Service vereinfacht und automatisiert den für gewöhnlich komplizierten Vorgang der Mediendateikonvertierung von einem Format, einer Größe oder einer Qualität in ein anderes bzw. eine andere. Der Elastic Transcoder-Service konvertiert Videodateien in Standard Definition (SD) oder High Definition (HD) und auch Audiodateien. Er liest Eingaben aus einem Amazon S3-Bucket, kodiert sie um und schreibt das Ergebnis in einer neuen Datei in einen anderen S3-Bucket. Sie können den gleichen Bucket für die Ein- und Ausgabe verwenden und die Buckets können sich in jeder AWS-Region befinden. Der Elastic Transcoder akzeptiert Eingabedateien in zahlreichen Formaten aus dem Web- und Verbraucherbereich sowie professionelle Formate. Ausgabedateitypen umfassen unter anderem MP4-, TS- und WebM-Containertypen sowie das Speichern von H.264- oder VP8-Video und AAC- oder Vorbis-Audio.

Sie beginnen mit mindestes einer Eingabedatei und erstellen Umwandlungsaufträge für jede Datei in einer Art von Workflow, die als Umwandlungspipeline bezeichnet wird. Bei der Erstellung der Pipeline geben Sie die Eingabe- und Ausgabe-Buckets sowie eine IAM-Rolle an. Jeder Auftrag muss auf eine Medienkonvertierungsvorlage (eine sog. Umwandlungsvoreinstellung oder transcoding preset) verweisen. Damit wird mindestens eine Ausgabedatei erstellt. Eine Voreinstellung gibt Elastic Transcoder die Einstellungen an, die bei Verarbeitung einer bestimmten Eingabedatei verwendet werden sollen. Sie können bei Erstellung einer Voreinstellung viele Einstellungen wählen. Dazu zählen unter anderem die Samplerate, die Bitrate, die Auflösung (Ausgabehöhe - und breite), die Anzahl von Reference- und Keyframes, eine Videobitrate sowie einige Optionen zur Erstellung von Thumbnails usw.

Wir bemühen uns, Aufträge in der eingehenden Reihenfolge zu beginnen. Das ist allerdings keine Garantie. Die Fertigstellung der Aufgaben folgt in der Regel keiner Reihenfolge, da sie parallel bearbeitet werden und sich in der Komplexität unterscheiden. Sie können, falls erforderlich, jede Pipeline pausieren und fortsetzen.

Elastic Transcoder unterstützt die Verwendung von SNS-Meldungen. Damit werden der Beginn und das Ende jedes Auftrags sowie Fehler- oder Warnbedingungen gemeldet. Die Parameter für SNS-Meldungen werden jeder Pipeline zugewiesen. Elastic Transcoder auch die "List Jobs By Status"-Funktion verwenden, um nach allen Aufgaben zu suchen, die einem bestimmten Status aufweisen (z. B. „Fertig gestellt“) oder die Funktion „Read Job“, um detaillierte Informationen zu einer bestimmten Aufgabe abzurufen.

Wie alle anderen AWS-Services integriert sich Elastic Transcoder in AWS Identity and Access Management (IAM). Das ermöglicht die Zugriffskontrolle für den Service und andere AWS-Ressourcen, die Elastic Transcoder erfordert. Dies können Amazon S3-Buckets und Amazon SNS-Themen sein. Standardmäßig haben IAM-Benutzer keinen Zugriff auf Elastic Transcoder oder die davon verwendeten Ressourcen. Sollen IAM-Benutzer mit Elastic Transcoder arbeiten, müssen Sie ihnen den Zugriff darauf explizit gewähren.

Amazon Elastic Transcoder erfordert, dass jede Anfrage an die Steuer-API authentifiziert wird. So können nur authentifizierte Prozesse oder Benutzer ihre eigenen Amazon Transcoder-Pipelines und -Voreinstellungen erstellen, bearbeiten bzw. löschen. Anfragen werden mit einer HMAC-SHA256-Signatur versehen, die aus der Anfrage und einem aus dem geheimen Schlüssel des Benutzers abgeleiteten Schlüssels berechnet wird. Außerdem kann auf die API von Amazon Elastic Transcoder nur über SSL-verschlüsselte Endpunkte zugegriffen werden.

Haltbarkeit wird durch Amazon S3 gewährleistet. Hier werden Mediendateien redundant auf mehreren Geräten über mehrere Einrichtungen in einer Amazon S3-Region gespeichert. Als zusätzlichen Schutz gegen das versehentliche Löschen von Mediendateien durch einen Benutzer, können Sie die Versionierungs-Funktion in S3 verwenden, die es ermöglicht, jede Version von jedem Objekt, das in einem Amazon S3-Bucket gespeichert wurde, aufzubewahren, abzurufen und wiederherzustellen. Sie können Versionen zudem mithilfe der MFA Delete-Funktion von Amazon S3 Versionierung schützen. Sobald die Funktion für ein S3-Bucket aktiviert wurde, muss jede Anforderung zur Löschung einer Version einen sechsstelligen Code und die Seriennummer des Multi-Factor-Authentication-Geräts enthalten.

Sicherheit bei Amazon CloudWatch

Amazon CloudWatch ist ein Web-Service zur Überwachung von AWS-Cloud-Ressourcen, beginnend bei Amazon EC2. Er bietet Kunden einen Überblick über die Verwendung von Ressourcen, die operative Performance und das Gesamtnachfragemuster einschließlich Metriken wie CPU-Nutzung, Lese-/Schreibvorgänge bei Datenträgern und Netzwerk-Datenverkehr. Kunden können CloudWatch-Alarme so einstellen, dass CloudWatch sie informiert, wenn bestimmte Schwellenwerte überschritten werden, oder andere automatisierte Maßnahmen ergreift, z. B. das Hinzufügen bzw. Entfernen von EC2-Instanzen bei aktiviertem Auto Scaling.

Wie alle AWS-Services erfordert Amazon CloudWatch, dass jede Anfrage an die Steuer-API authentifiziert wird, damit nur authentifizierte Benutzer auf CloudWatch zugreifen und es verwenden können. Anforderungen werden mit einer HMAC-SHA1-Signatur versehen, die aus der Anforderung und dem privaten Schlüssel des Benutzers berechnet wird. Außerdem kann auf die Steuer-API von Amazon CloudWatch nur über SSL-verschlüsselte Endpunkte zugegriffen werden.

Sie können den Zugriff auf Amazon CloudWatch noch darüber hinaus kontrollieren. Erstellen Sie Benutzer mithilfe von AWS IAM unter Ihrem AWS-Konto und kontrollieren Sie die Berechtigungen, die Sie diesen Benutzern zum Aufruf bestimmter CloudWatch-Vorgänge gewähren.

Sicherheit bei Amazon CloudFront

Mit Amazon CloudFront können Kunden Inhalte auf einfache Weise, mit geringer Latenz und hohen Datenübertragungsgeschwindigkeiten an Endbenutzer verteilen. Es liefert dynamischen, statischen und gestreamten Inhalt mithilfe eines globalen Netzwerks von Edge-Standorten. Anforderungen für Kundenobjekte werden automatisch zum nächstgelegenen Edge-Standort umgeleitet. Dadurch werden Inhalte mit der bestmöglichen Leistung geliefert. Amazon CloudFront wurde für die Arbeit mit anderen AWS-Services, z. B. Amazon S3, Amazon EC2, Amazon Elastic Load Balancing, und Amazon Route 53 optimiert. Es arbeitet auch nahtlos mit jedem nicht AWS-Server zusammen, der die ursprünglichen, definitiven Versionen der Dateien enthält.

Amazon CloudFront erfordert, dass jede Anforderung an die Steuer-API authentifiziert wird, damit nur autorisierte Benutzer die eigenen Amazon CloudFront-Verteilungen erstellen, bearbeiten und löschen können. Anforderungen werden mit einer HMAC-SHA1-Signatur versehen, die aus der Anforderung und dem privaten Schlüssel des Benutzers berechnet wird. Außerdem kann auf die Steuer-API von Amazon CloudFront nur über SSL-verschlüsselte Endpunkte zugegriffen werden.

AWS garantiert nicht die Haltbarkeit der Daten an den Edge-Standorten von Amazon CloudFront. Der Service entfernt möglicherweise von Zeit zu Zeit Objekte, die zu selten angefordert werden, aus den Edge-Standorten. Haltbarkeit wird

durch Amazon S3 erreicht. Es fungiert als Ursprungsserver für Amazon CloudFront und speichert die ursprünglichen, definitiven Kopien der von Amazon CloudFront verteilten Objekte.

Wenn Sie den Personenkreis kontrollieren möchten, der Inhalte von Amazon CloudFront herunterladen kann, aktivieren Sie die Service-Funktion "privater Inhalt". Diese Funktion besteht aus zwei Komponenten: Die erste steuert die Art und Weise wie die Edge-Standorte von Amazon CloudFront auf Objekte in Amazon S3 zugreifen. Die zweite steuert wie Inhalte aus den Edge-Standorten von Amazon CloudFront an die Betrachter im Internet verteilt wird. Sie können auch anpassen, wie der Zugriff auf Ihre Inhalte auf Grundlage des geografischen Standorts der Betrachter blockiert wird. Aktivieren Sie dazu die geo-restriction-Funktion in CloudFront. Mit „geo-restriction“ können Sie bestimmen, ob IPs bestimmter Länder auf eine Whitelist oder Blacklist gesetzt werden.

Zugriffskontrolle für die ursprünglichen Kopien der Objekte in S3 erreichen Sie bei Amazon CloudFront, indem Sie mindestens eine „Ursprungszugriffsidentität“ ("Origin Access Identities") erstellen und den Verteilungen zuweisen. Sobald einer Amazon CloudFront-Verteilung eine Ursprungszugriffsidentität zugewiesen wird, nutzt die Verteilung diese Identität für den Objektabruf aus Amazon S3. Sie können dann die ACL-Funktion von Amazon S3 verwenden, die den Zugriff auf die Ursprungszugriffsidentität beschränkt, damit die ursprüngliche Kopie des Objektes nicht öffentlich lesbar ist.

Sie können den Personenkreis kontrollieren, der Objekte aus den Edge-Standorten von Amazon CloudFront herunterladen kann. Der Service nutzt dafür ein Überprüfungssystem mit signierter URL. Damit Sie dieses System verwenden können, müssen Sie zunächst ein Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel erstellen und den öffentlichen Schlüssel über die AWS-Website auf Ihr Konto hochladen. Zweitens müssen Sie Ihre Amazon CloudFront-Verteilung konfigurieren und angeben, welche Konten Sie zum Signieren von Anforderungen autorisieren möchten. Sie können dafür bis zu fünf AWS-Konten angeben. Drittens werden Sie Richtliniendokumente erstellen, in denen sie festlegen, unter welchen Bedingungen Amazon CloudFront die Inhalte verteilen soll, wenn Sie eine Anfrage erhalten. Diese Richtliniendokumente können den Namen des angeforderten Objekts angeben sowie das Datum und die Uhrzeit der Anforderung und die Quell-IP (oder den CIDR-Bereich) des Clients, der die Anforderung stellt. Sie berechnen die RSA-SHA1-Verschlüsselung des Richtliniendokuments und signieren es mithilfe des privaten Schlüssels. Als letztes fügen Sie das verschlüsselte Richtliniendokument und die Signatur als Abfrageparameter beim Verweisen der Objekte hinzu. Amazon CloudFront entschlüsselt die Signatur bei Erhalt einer Anforderung mit dem öffentlichen Schlüssel. Amazon CloudFront bedient nur Anforderungen mit einem gültigen Richtliniendokument und passender Signatur.

Beachten Sie, dass privater Inhalt eine optionale Funktion ist. Sie muss beim Einrichten der CloudFront-Verteilung aktiviert werden. Inhalte, die ohne Aktivierung dieser Funktion verteilt werden, sind öffentlich lesbar.

Mit Amazon CloudFront können Sie Inhalte optional über eine verschlüsselte Verbindung (HTTPS) übermitteln. Standardmäßig akzeptiert CloudFront Anforderungen über HTTP- und HTTPS-Protokolle. Allerdings lässt sich CloudFront auch so konfigurieren, dass HTTPS für alle Anforderungen obligatorisch ist. Auch können HTTP-Anforderungen mit CloudFront an HTTPS umgeleitet werden. Sie können sogar das Cacheverhalten von CloudFront in der gleichen Verteilung konfigurieren. So ermöglichen Sie HTTP und HTTPS. Dadurch können Sie HTTP für einige Objekte obligatorisch machen, für andere aber nicht.

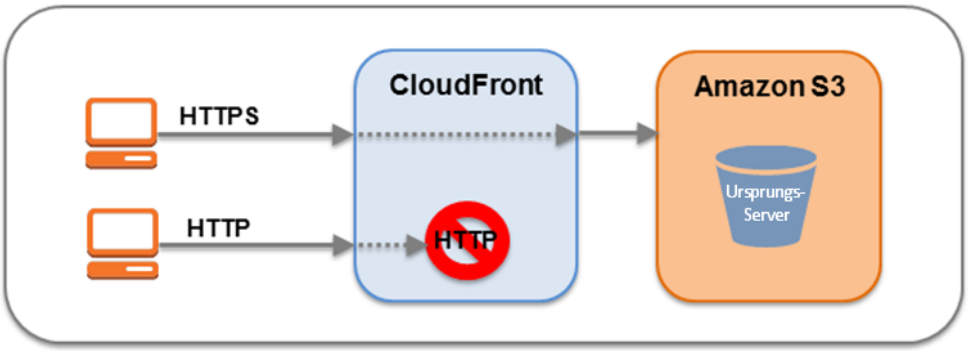


Abbildung 6: Verschlüsselte Amazon CloudFront-Übertragung

Sie können einen oder mehrere CloudFront-Ursprünge so konfigurieren, dass CloudFront Objekte mit demselben Protokoll vom Ursprungsserver abgerufen werden, das der Betrachter bei der Objektanforderung verwendet hat. Wenn Sie diese CloudFront-Einstellung nutzen und der Betrachter verwendet bei der Objektanforderung von CloudFront beispielsweise HTTPS, so verwendet CloudFront bei der Weiterleitung der Anforderung an den Ursprungsserver ebenfalls HTTPS.

Sofern Sie einen HTTP-Server als Ursprungsserver nutzen, müssen Sie bei Verwendung von HTTPS zwischen Benutzer und CloudFront und zwischen CloudFront und Ursprungsserver darauf achten, ein SSL-Zertifikat auf dem HTTP-Server zu installieren, das von der Zertifizierungsstelle eines Drittanbieters signiert sein muss, z. B. VeriSign oder DigiCert.

Egal, ob Sie HTTP oder HTTPS nutzen, Sie können alternative Domänennamen (zum Beispiel: example.com) anstelle des Domänennamens verwenden, der von CloudFront der Verteilung zugewiesen wird. Bei HTTPS reserviert Amazon an jedem Edge-Standort von CloudFront IP-Adressen für ihr SSL-Zertifikat. Damit kann CloudFront die eingehenden Anforderungen dem richtigen SSL-Zertifikat zuweisen. Bei HTTPS übermitteln moderne Webbrowser und HTTP-Clientbibliotheken den Hostnamen des Ziels am Anfang des SSL-Handshake-Vorgangs. Somit sind reservierte IP-Adressen nicht länger erforderlich.

Die Zugriffsprotokolle von Amazon CloudFront enthalten einen umfassenden Satz an Informationen über Inhaltsanforderungen, u.a. das angeforderten Objekt, Datum und Uhrzeit der Anforderung, der Edge-Standort, der die Anforderung bedient, die Client-IP-Adresse, den Referrer und den Benutzeragenten. Zugriffsprotokolle lassen sich bei der Konfiguration der Amazon CloudFront-Verteilung aktivieren. Geben Sie einfach den Namen des Amazon S3-Buckets an, in dem die Protokolle gespeichert werden sollen.

Sicherheit bei Amazon Elastic MapReduce (Amazon EMR)

Amazon Elastic MapReduce (Amazon EMR) ist ein verwalteter Web-Service. Damit können Sie Hadoop-Cluster ausführen, die große Datenmengen verarbeiten, indem sie die Arbeit und Daten auf etliche Server verteilen. Es wird eine erweiterte Version des Apache Hadoop-Frameworks genutzt, das auf der webweiten Infrastruktur von Amazon EC2 und Amazon S3 ausgeführt wird. Sie laden einfach die Daten und eine Datenverarbeitungsanwendung auf Amazon S3 hoch. Amazon EMR startet dann die angegebene Anzahl an Amazon EC2-Instanzen. Der Service beginnt mit der Ausführung des Auftragsablaufs, während die Eingabedaten aus Amazon S3 in die gestarteten Amazon EC2-Instanzen gezogen werden. Sobald der Auftragsablauf abgeschlossen ist, übermittelt Amazon EMR die Ausgabedaten an Amazon S3. Hier können Sie dann abgerufen oder als Eingabe in einen anderen Auftragsablauf verwendet werden.

Starten Sie einen Auftragsablauf in Ihrem Namen, richtet Amazon EMR zwei Amazon EC2-Sicherheitsgruppen ein: eine für die Master-Knoten und eine weitere für die Slaves. Die Master-Sicherheitsgruppe verfügt über einen offenen Port für die Kommunikation mit dem Service. Auch der SSH-Port ist geöffnet. Damit können Sie eine SSH-Verbindung mit dem beim Start angegebenen Schlüssel zu den Instanzen aufbauen. Die Slaves starten in einer getrennten Sicherheitsgruppe. Diese gestattet nur eine Interaktion mit der Master-Instanz. Standardmäßig werden beide Sicherheitsgruppen so eingerichtet, dass der Zugriff von externen Quellen, einschließlich Amazon EC2-Instanzen anderer Kunden, nicht gestattet wird. Da es sich um Sicherheitsgruppen innerhalb Ihres Kontos handelt, können Sie mit den Standard-EC2-Tools oder dem Dashboard neu konfiguriert werden. Zum Schutz der Eingabe- und Ausgabedatensätze der Kunden übermittelt Amazon EMR Daten mithilfe von SSL an bzw. von Amazon S3.

Amazon EMR bietet verschiedene Möglichkeiten, den Zugriff auf Ressourcen Ihres Clusters zu steuern. Sie können mit AWS IAM Benutzerkonten sowie Rollen erstellen und Berechtigungen konfigurieren. Diese steuern, auf welche AWS-Funktionen diese Benutzer und Rollen zugreifen können. Bei Start eines Clusters können Sie dem Cluster ein Amazon EC2-Schlüssel-Paar zuweisen, welches Sie dann verwenden können, wenn Sie sich über SSH mit dem Cluster verbinden. Sie können auch Berechtigungen einrichten, mit denen es anderen Benutzern als dem Standard-Hadoop-Benutzer möglich ist, Aufträge an den Cluster zu vergeben.

Standardmäßig ist ein Cluster beim Start durch einen IAM-Benutzer vor anderen IAM-Benutzern auf dem AWS-Konto verborgen. Diese Filterung wird bei allen Amazon EMR-Schnittstellen durchgeführt (der Konsole, CLI, API und SDKs) und verhindert, dass IAM-Benutzer auf Cluster, die von anderen IAM-Benutzern erstellt wurden, zugreifen und sie irrtümlich verändern. Das ist bei Clustern sinnvoll, die nur einem einzelnen IAM-Benutzer und dem Haupt-AWS-Konto angezeigt werden sollen. Sie können einen Cluster auch für IAM-Benutzer unter demselben AWS-Konto sichtbar und zugänglich machen.

Als zusätzlichen Schutz können Sie die EC2-Instanzen des EMR-Clusters in einer Amazon VPC starten. Das gleicht dem Start in einem privaten Subnetz. Damit können Sie den Zugriff auf das gesamte Subnetz kontrollieren. Sie können den Cluster auch in einer VPC starten und dem Cluster ermöglichen, mit einer VPN-Verbindung auf Ressourcen auf dem internen Netzwerk zuzugreifen. Eingabedaten können vor dem Hochladen auf Amazon S3 mithilfe jedes üblichen Datenverschlüsselungstools verschlüsselt werden. Werden die Daten vor dem Hochladen verschlüsselt, müssen Sie zu Anfang des Auftragablaufs einen Entschlüsselungsschritt hinzufügen, sobald Amazon Elastic MapReduce die Daten von Amazon S3 abruft.

Sicherheit bei Amazon Route 53

Amazon Route 53 ist ein autoritatives DNS-System. Ein autoritatives DNS-System bietet einen Update-Mechanismus, den Sie verwenden können, um Ihre öffentlichen DNS-Namen zu verwalten. Es beantwortet dann DNS-Abfragen, indem es Domänennamen in IP-Adressen übersetzt, damit Computer miteinander kommunizieren können. Mit Route 53 können Benutzeranforderungen mit einer Infrastruktur verbunden werden, die auf AWS ausgeführt wird (z. B. eine Amazon EC2-Instanz oder ein Amazon S3-Bucket), oder mit einer Infrastruktur außerhalb von AWS.

Amazon Route 53 erfüllt zwei DNS-Funktionen. Es ermöglicht Ihnen, die IP-Adressen (records) verwalten, die für Ihre Domänennamen gelistet sind und es beantwortet Anforderungen (queries) nach Übersetzung bestimmter Domänennamen in ihre entsprechenden IP-Adressen. Abfragen für Ihre Domänennamen werden mithilfe von Anycast automatisch zum nächsten DNS-Server umgeleitet, um geringstmögliche Latenz zu erreichen. Darüber hinaus können Sie mit Weighted Round-Robin (WRR), Latency Based Routing (LBR) und DNS Failover Weiterleitungsrichtlinien verwalten, die die DNS-Antworten des Systems dynamisch bestimmen.

Amazon Route 53 wurde basierend auf der hochverfügbaren und zuverlässigen Infrastruktur von AWS erstellt. Die verteilte Natur der AWS DNS-Server stellt ein einheitliches Weiterleiten der Endbenutzer an die Anwendung sicher. Route 53 unterstützt zudem die Verfügbarkeit der Website durch Health Checks und DNS-Failover-Funktionen. Sie können Route 53 auf einfache Weise so konfigurieren, dass der Zustand Ihrer Website regelmäßig geprüft wird (dies gilt auch für sichere, nur über SSL erreichbare Websites) und dass auf eine Sicherungs-Site umgeschaltet wird, wenn die primäre Site nicht reagiert.

Wie bei allen AWS-Services muss bei Amazon Route 53 jede Anforderung an die Steuer-API authentifiziert werden, damit nur authentifizierte Benutzer auf Route 53 zugreifen und es verwalten können. API-Anforderungen werden mit einer HMAC-SHA1- oder HMAC-SHA256-Signatur versehen, die aus der Abfrage und dem geheimen AWS-Zugriffsschlüssel des Benutzers berechnet wird. Außerdem kann auf die Steuer-API von Amazon Route 53 nur über SSL-verschlüsselte Endpunkte zugegriffen werden. Es werden IPv4- und IPv6-Weiterleitung unterstützt.

Sie können den Zugriff auf die DNS-Verwaltungsfunktionen von Amazon Route 53 steuern, indem Sie mithilfe von AWS IAM unter Ihrem AWS-Konto Benutzer erstellen und die Berechtigungen dieser Benutzer zur Durchführung von Route 53-Vorgängen kontrollieren.

Sicherheit bei Amazon CloudSearch

Amazon CloudSearch ist ein vollständig verwalteter Service in der Cloud, der das Einrichten, Verwalten und Skalieren einer Suchlösung für Ihre Website vereinfacht. Amazon CloudSearch ermöglicht das Durchsuchen von großen Datensammlungen, z. B. Webseiten, Dokumentdateien, Forum-Posts oder Produktinformationen. Es gestattet Ihnen, Ihrer Website schnell eine Suchmöglichkeit hinzuzufügen, ohne Such-Experte werden oder sich über Hardwarebereitstellung, -einrichtung und -wartung Gedanken machen zu müssen. Da die Daten- und Datenverkehrsmenge schwankt, skaliert Amazon CloudSearch automatisch entsprechend Ihren Bedürfnissen.

Eine Amazon CloudSearch-Domäne kapselt die Datensammlung, die Sie durchsuchen möchten, die Such-Instanzen zur Verarbeitung der Suchabfragen und eine Konfiguration, die steuert, wie Ihre Daten indexiert und durchsucht werden. Sie erstellen für jede Datensammlung, die Sie durchsuchbar machen möchten, eine getrennte Suchdomäne. Für jede Domäne konfigurieren Sie Indexierungsoptionen. Diese beschreiben die im Index eingeschlossenen Felder und ihre Verwendungsweise, Textoptionen, die domänenspezifische Stoppwörter, Stämme und Synonyme definieren, Rangausdrücke, die Sie verwenden können, um die Anordnung von Suchergebnissen anzupassen, und Zugriffsrichtlinien, die den Zugriff auf Dokumente und die Suchendpunkte der Domäne regeln.

Der Zugriff auf die Endpunkte der Suchdomäne wird durch die IP-Adresse begrenzt. So können nur autorisierte Hosts Dokumente abschicken und Suchanfragen senden. IP-Adressautorisierung wird nur für die Zugriffskontrolle auf Dokumente und Suchendpunkte verwendet. Für jede Amazon CloudSearch-Konfigurationsanforderung muss die Standard-AWS-Authentifizierung durchgeführt werden.

Amazon CloudSearch bietet getrennte Endpunkte für den Zugriff auf den Konfigurations-, Such- und Dokumentenservice:

- Auf den Konfigurationsservice wird über einen allgemeinen Endpunkt zugegriffen: cloudsearch.us-east-1.amazonaws.com.
- Mit dem Dokumentenendpunkt werden Dokumente für die Indizierung an die Domäne gesendet. Es wird über einen domänenspezifischen Endpunkt darauf zugegriffen: http://doc-domainname-domainid.us-east-1.cloudsearch.amazonaws.com.
- Mit dem Suchendpunkt werden Suchanforderungen an die Domäne gesendet. Es wird über einen domänenspezifischen Endpunkt darauf zugegriffen: http://search-domainname-domainid.us-east-1.cloudsearch.amazonaws.com.

Wenn keine statische IP-Adresse vorhanden ist, müssen Sie jedes Mal den Computer neu autorisieren, sobald sich die IP-Adresse ändert. Wird die IP-Adresse dynamisch zugewiesen, teilen Sie die Adresse wahrscheinlich auch mit anderen Computern im Netzwerk. Das bedeutet, dass bei Autorisierung der IP-Adresse alle Computer, die diese Adresse teilen, auf den Dokumentendpunkt der Suchdomäne zugreifen können.

Wie bei allen AWS-Services müssen alle an die Steuer-API von Amazon CloudSearch gesendeten Anforderungen authentifiziert werden. So können nur authentifizierte Nutzer auf die CloudSearch-Domäne zugreifen und ihn verwalten. API-Anforderungen werden mit einer HMAC-SHA1 bzw. HMAC-SHA256-Signatur versehen, die aus der Anfrage und dem geheimen AWS-Zugriffsschlüssel des Benutzers berechnet wird. Außerdem kann auf die Steuer-API von Amazon CloudSearch nur über SSL-verschlüsselte Endpunkte zugegriffen werden. Sie können den Zugriff auf die Management-Funktionen von Amazon CloudSearch steuern, indem Sie mithilfe von AWS IAM unter Ihrem AWS-Konto Benutzer erstellen und die Berechtigung dieser Benutzer zur Durchführung von CloudSearch-Vorgängen kontrollieren.

Sicherheit bei AWS Elastic Beanstalk

AWS Elastic Beanstalk ist ein Verteilungs- und Verwaltungstool, das die Funktionen der Kapazitätsbereitstellung, des Load Balancing und des Auto Scaling für Ihre Anwendung automatisiert. Sie können den verteilbaren Code hochladen und AWS Elastic Beanstalk erledigt den Rest. Sobald eine Anwendung ausgeführt wird, erfüllt Elastic Beanstalk automatisch Verwaltungsaufgaben wie Überwachung, Versionsverteilung von Anwendungen, Protokolldatei-Snapshots und Health Checks. Werden Ressourcen (z. B. EC2-Instanzen) für ungesund befunden, werden sie ersetzt, damit die Anwendung in Gang gehalten wird.

AWS Elastic Beanstalk verwendet verschiedene AWS-Funktionen und -Services, z. B. Amazon EC2, Amazon RDS, Elastic Load Balancing, Auto Scaling, Amazon S3 und Amazon SNS. So wird eine Umgebung geschaffen, in der die Anwendung nahtlos ausgeführt wird. AWS Elastic Beanstalk startet automatisch eine oder mehrere EC2-Instanzen mithilfe einer sicher konfigurierten AMI und speichert die Anwendung in S3, aktiviert Load Balancing und Auto Scaling und überwacht den Status der Anwendungsumgebung.

Muss die Anwendung die API eines AWS-Services (z. B. DynamoDB oder CloudWatch) aufrufen, können Sie den AWS-Zugriffsschlüssel und den geheimen Schlüssel an die Anwendung übergeben. Dies geschieht mit Elastic Beanstalk-Umgebungsvariablen oder Sie erstellen mit einer IAM-Rolle temporäre Anmeldinformationen. Bei Erstellung einer IAM-Rolle wird ihr ein Instanz-Profil zugewiesen. Damit kann die Anwendung temporäre Sicherheits-Anmeldeinformationen abrufen und AWS API-Aufrufe durchführen. Wird die Anwendung auf AWS Elastic Beanstalk verteilt, startet Elastic Beanstalk die EC2-Instanz mithilfe des von Ihnen definierten Instanz-Profils. Die Anwendung verwendet die auf der EC2-Instanz verfügbaren Rollen-basierten Anmeldeinformationen. Sie ruft die Rollen-basierten Anmeldeinformationen aus dem Informationssicherheits-Managementsystem (ISMS) ab und führt mit diesen Anmeldeinformationen dann einen API-Aufruf des AWS-Services durch. Ein weiterer Sicherheitsvorteil bei der Verwendung von IAM-Rollen ist die mehrmals täglich erfolgende automatische Rotation der temporären Anmeldeinformationen.

Noch mehr Privatsphäre erhalten Sie, indem Sie Elastic Beanstalk-Anwendungen innerhalb einer Virtual Private Cloud (VPC) ausführen. Sie können ein privates, virtuelles Netzwerk in der AWS-Cloud definieren und bereitstellen und mithilfe einer VPN-Verbindung mit dem Unternehmensnetzwerk verbinden. Damit können Sie eine breitere Auswahl an Anwendungen auf Elastic Beanstalk ausführen. Beispielsweise können Sie Intranetanwendungen, z. B. eine Anwendung für Fehlertickets oder eine Reporting Site, auf Elastic Beanstalk ausführen.

Elastic Beanstalk automatisiert die Bereitstellung und Verteilung einer Anwendung. Dennoch können Sie mit der Elastic Beanstalk-Konsole Standardeinstellungen für die AWS-Ressourcen manuell überschreiben. So erlangen Sie soviel Kontrolle über die zugrunde liegende Infrastruktur, wie gewünscht. Außerdem können Sie eine Vielzahl von Überwachungs- und Sicherheitsfunktionen konfigurieren, die unter anderem Folgendes umfassen:

- Erzwingen von sicherer Datenübertragung von und zu der Anwendung durch Aktivieren von HTTPS auf dem Load Balancer
- Empfangen von E-Mail-Benachrichtigungen über Amazon Simple Notification Service (Amazon SNS), wenn sich der Anwendungsstatus ändert oder Anwendungsserver hinzugefügt bzw. entfernt werden
- Aktivieren sicherer Übertragung von E-Mail-Benachrichtigungen durch Angabe von HTTPS als Benachrichtigungsprotokoll
- Anpassen der Servereinstellungen der Anwendung und Übergabe von Umgebungsvariablen, einschließlich des geheimen AWS-Zugriffsschlüssels, der von einer Anwendung benötigt wird, um sich bei AWS-Ressourcen zu authentifizieren
- Aktivieren von sicherem Anmeldezugriff auf Amazon EC2-Instanzen zur sofortigen und direkten Fehlerbehebung
- Aktivieren von Protokolldateirotation, wodurch die Protokolldateien der EC2-Instanzen von Kunden stündlich in einen der Anwendung zugewiesenen Amazon S3-Bucket kopiert werden
- Zugreifen auf integrierte Amazon CloudWatch-Überwachungsmetriken, z. B. durchschnittliche CPU-Nutzung, Anforderungsanzahl und durchschnittliche Latenz

Alle AWS Elastic Beanstalk-Endpunkte verwenden für den Zugriff das HTTPS-Protokoll. Sie können den Zugriff auf Elastic Beanstalk-Services mithilfe von IAM-Richtlinien steuern. Zugriff auf AWS Elastic Beanstalk kann leicht gewährt werden. Sie können dazu anfangs eine der Richtlinienvorlagen in der AWS IAM-Konsole verwenden. AWS Elastic Beanstalk bietet zwei Vorlagen: eine für schreibgeschützten Zugriff und eine für Vollzugriff. Die Vorlage für schreibgeschützten Zugriff gewährt Lesezugriff auf AWS Elastic Beanstalk-Ressourcen. Die Vorlage für Vollzugriff gewährt vollen Zugriff auf alle AWS Elastic Beanstalk-Vorgänge sowie Berechtigungen zur Verwaltung abhängiger Ressourcen, z. B Elastic Load Balancing und Auto Scaling. Kunden können auch mit dem AWS Policy Generator benutzerdefinierte Richtlinien erstellen. So lassen sich

Berechtigungen für bestimmte AWS Elastic Beanstalk-Ressourcen, z. B. Anwendungen, Anwendungsversionen und Umgebungen, gewähren bzw. verweigern.

Sicherheit bei AWS CloudFormation

AWS CloudFormation ist ein Bereitstellungstool, das die Aufzeichnung der Basiskonfiguration der AWS-Ressourcenermöglicht, die Sie für den Betrieb Ihrer Anwendungen benötigen, damit Sie Ihre Anwendungen in einer geregelten und vorhersehbaren Weise bereitstellen und aktualisieren können. Sie definieren die AWS-Ressourcen, die zum Ausführen der Anwendung erforderlich sind, in einer einfachen Textdatei, genannt "Template". Sie kann wiederholt dazu genutzt werden, identische Kopien des gleichen Ressourcenstapels zu erstellen (oder als Grundlage eines neuen Stapels dienen). Sie können mit Parametern regionsspezifische Infrastrukturvariationen erfassen und steuern, z. B. Amazon EC2 AMIs, EBS-Snapshot-Namen, RDS-Datenbankgrößen usw. Mit Parametern können Werte festgelegt werden, die bei Erstellung des Stapels an das Template übergeben werden können. Mit Parametern können auch vertrauliche Informationen, z. B. Benutzernamen und Kennwörter, die nicht im Template selbst gespeichert werden sollten, effektiv angegeben werden.

AWS CloudFormation ermöglicht einfache Änderungen, z. B. das Aktualisieren von Eigenschaften vorhandener Ressourcen, oder komplexere Änderungen, z. B. das Hinzufügen und Entfernen von Ressourcen aus einem Stapel. Änderungen an einem Stapel werden durch das Bearbeiten des Templates und das Aktualisieren des Stapels vorgenommen. AWS CloudFormation versteht die Unterschiede zwischen aktuellen und neuen Templates und bearbeitet den Stapel entsprechend.

Mit dem CloudFormer-Tool können Sie eigene Templates erstellen. So beschreiben Sie AWS-Ressourcen und die jeweiligen Abhängigkeiten oder Laufzeitparameter. Oder Sie können die Beispiel-Templates von AWS CloudFormation verwenden. Genau wie AWS Elastic Beanstalk verteilt CloudFormation die Ressourcen auch automatisch. Sie müssen also die Reihenfolge in der die AWS-Ressourcen bereitgestellt werden ebensowenig selbst herausfinden wie die erforderlichen Feinheiten, damit die Abhängigkeiten funktionieren.

AWS CloudFormation zeichnet die Ressourcenerstellung und -löschung für jeden Stapel auf. Ihnen wird eine Liste aller Ressourcen angezeigt, die für einen Stapel bereitgestellt wurden, sowie der Verlauf der Bereitstellungsereignisse. Das Template ist eine Textdatei. Sie kann also wie jedes andere Anwendungsartefakt versionsgesteuert werden. Mit AWS CloudFormation können Sie eine Versionskontrolle über die Infrastrukturdefinition durchführen. Genau wie bei Anwendungsquellen.

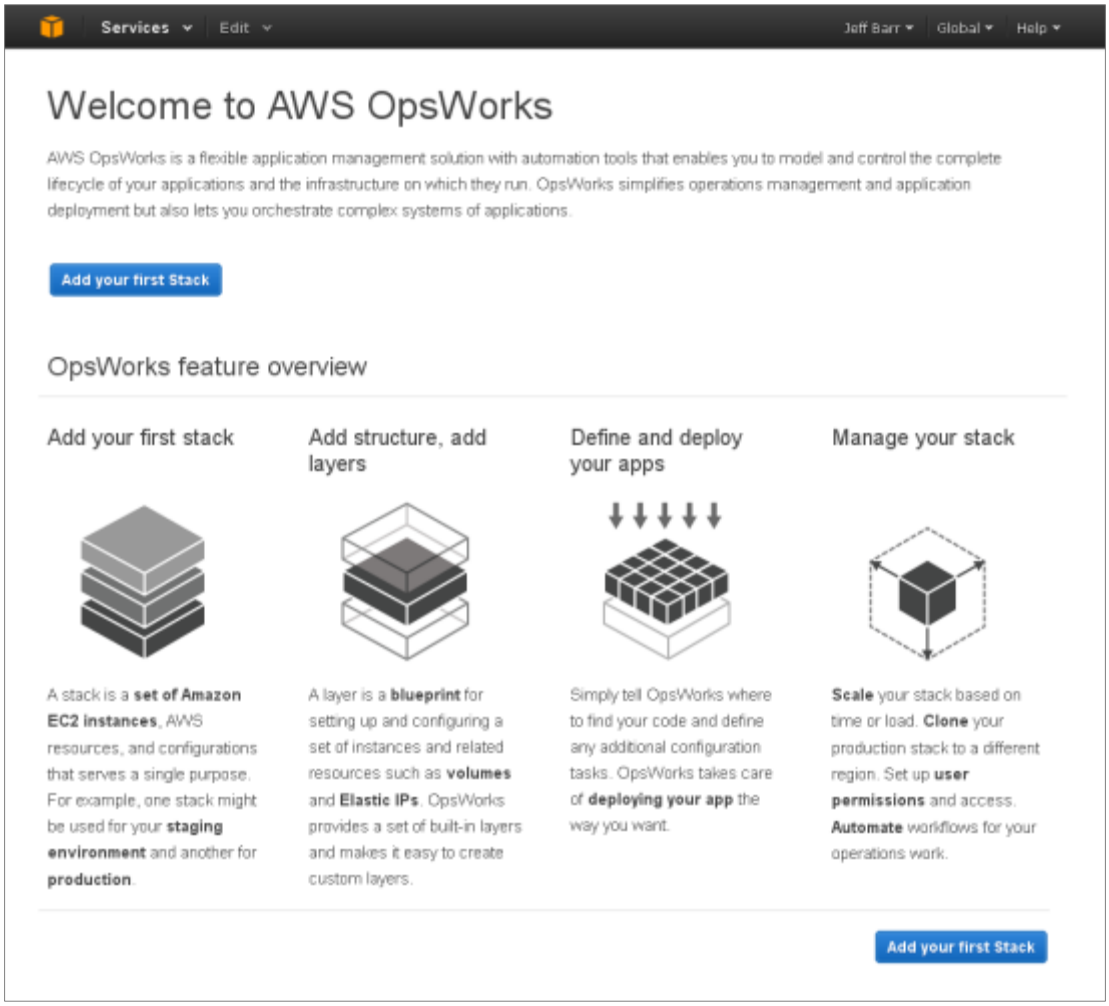
Alle AWS CloudFormation-Endpunkte verwenden das HTTPS-Protokoll für den Zugriff. Sie können den Zugriff auf Funktionen zur Erstellung und Verwaltung von AWS CloudFormation-Template steuern, indem Sie mithilfe von AWS IAM unter Ihrem AWS-Konto Benutzer erstellen und die Berechtigtung dieser Benutzer zur Durchführung von CloudFormation-Prozessen kontrollieren.

Sicherheit von AWS OpsWorks

AWS OpsWorks ist ein Anwendungsverwaltungs-Service, der die Steuerung des gesamten Lebenszyklus einer Anwendung vereinfacht. Er ermöglicht die Automatisierung und Verwaltung aller an der Bereitstellung der Anwendung beteiligten Prozesse. Dies schließt Ressourcenbereitstellung, Konfigurationsverwaltung, Anwendungsverteilung, Softwareupdates sowie Überwachung und Zugriffssteuerung ein.

Sie starten in OpsWorks mit der Erstellung eines *Stapels*. Dieser stellt eine Sammlung von EC2-Instanzen und Layer dar. Layer sind Vorlagen zum Konfigurieren, Starten und Verwalten von Instanzen. Sie definieren die Softwarekonfiguration für jeden Layer, einschließlich Installationsskripte und Initialisierungsaufgaben. Wird eine Instanz einer Schicht hinzugefügt, wendet OpsWorks die angegebene Konfiguration automatisch an.

Jeder Stapel hostet mindestens eine Anwendung. Er dient zudem als ein Container für jede andere AWS-Ressource, die Ihre Anwendung vielleicht benötigt (z. B. EBS-Menge und Elastic IP-Adressen) sowie für Benutzerberechtigungen, die der Anwendung zugeordnet sind. Sie weisen OpsWorks an, die Anwendung auf der EC2-Instanz zu installieren, indem es Software-Code aus einer oder aus mehreren Code-Repositories, z. B. Git oder Subversion, bezieht, über eine HTTP-Anforderung abruft oder aus einem Amazon S3-Bucket herunterlädt.



Nachdem Sie einen Stapel, seine Layer und seine Anwendungen definiert haben, können Sie EC2-Instanzen erstellen und bestimmten Layern zuweisen. Sie können die Instanzen manuell starten oder eine Skalierung auf Grundlage von Last oder Zeit definieren. In jedem Fall haben Sie volle Kontrolle über den Instanz-Typ, die Availability Zone, die Sicherheitsgruppe(n) und das Betriebssystem. Für noch bessere Kontrolle installierter Pakete und Versionen können Sie benutzerdefinierte AMIs verwenden. Wenn die Instanzen starten, werden diese entsprechend Ihren Angaben konfiguriert. Dies geschieht mithilfe der von Ihnen definierten Voreinstellungen für den Layer, der die Instanz enthält.

Sie können mit AWS IAM steuern, wie Benutzern gestattet wird, mit OpsWorks zu interagieren, z. B. beim Verwalten von Stapeln und Verwenden von SSH zur Verbindung mit EC2-Instanzen. Sie sind sogar so flexibel, dass Sie Benutzern Zugriff auf AWS OpsWorks gewähren, aber den direkten Zugriff auf abhängige Services wie Amazon EC2 sperren können. Sie können einem Benutzer zum Beispiel gestatten, Instanzen mit AWS OpsWorks zu stoppen, ihm aber nicht erlauben, Instanzen über die Amazon EC2-Konsole oder die API zu beenden.

Sie können mit IAM auch steuern, wie OpsWorks in Ihrem Namen handeln darf, um Stapelressourcen zu verwalten und wie Anwendungen, die auf von AWS OpsWorks gesteuerten Instanzen ausgeführt werden, auf AWS-Ressourcen zugreifen können (dies gilt nur, wenn Sie Anwendungen bereitstellen, die auf andere AWS-Services zugreifen und die ihre Anmeldeinformationen über Rollen in EC2-Instanzen erhalten).

Mit AWS OpsWorks können Sie die Verwendung eines *Verteilungsschlüssels* für den Abruf von Anwendungen aus einem Github-Repository erzwingen. Ein Verteilungsschlüssel ist ein SSH-Schlüssel ohne Kennwort. Er ermöglicht es AWS OpsWorks, Anwendungen oder Kochbücher aus einem privaten Github-Repository asynchron bereitzustellen, ohne dass weitere Eingaben von Ihnen erforderlich sind.

Darüber hinaus, kann auf die API von AWS OpsWorks nur über einen SSL-verschlüsselten Endpunkt (opsworks.us-east-1.amazonaws.com) zugegriffen werden. Sie müssen eine Verbindung mit diesem Endpunkt herstellen, um auf OpsWorks zugreifen zu können. Aber Sie können dann die API verwenden, um AWS OpsWorks anzuweisen, Stapel in jeder beliebigen AWS-Region zu erstellen.

Sicherheit bei Amazon Kinesis

Amazon Kinesis ist ein verwalteter Service, der für das Streaming großer Daten in Echtzeit entwickelt wurde. Er kann jede Datenmenge aus einer unbegrenzten Anzahl von Quellen annehmen und dabei bei Bedarf in beide Richtungen skalieren. Sie können Kinesis in Situationen verwenden, in denen Datenaufnahme und -verarbeitung in großen Mengen und in Echtzeit erforderlich ist, z. B. Serverprotokolle, soziale Medien oder Marktdaten-Feeds und Web Clickstream-Daten.

Anwendungen lesen und schreiben Datensätze bei Amazon Kinesis aus bzw. in *Streams*. Sie können eine beliebige Anzahl von Kinesis-Streams erstellen, um Daten zu erfassen, zu speichern und zu transportieren. Amazon Kinesis steuert die Infrastruktur, den Speicher, das Netzwerk und die Konfiguration, die zur Erfassung und Verarbeitung der Daten erforderlich ist, automatisch auf dem Durchsatzniveau, das Ihre Streaming-Anwendungen benötigen. Sie müssen sich über die Bereitstellung, Verteilung oder laufende Wartung von Hardware, Software oder anderen Services keine Gedanken machen, um die Erfassung und Speicherung großer Datenmengen in Echtzeit zu ermöglichen. Amazon Kinesis repliziert Daten zudem synchron über drei Einrichtungen innerhalb einer AWS-Region und bietet so hochgradige Verfügbarkeit und Datenhaltbarkeit.

In Amazon Kinesis erhalten Datensätze eine Sequenznummer, einen Partitionsschlüssel und einen Datenblob. Dabei handelt es sich um eine nicht übersetzte, unveränderliche Bytesequenz. Der Amazon Kinesis-Service inspiziert, interpretiert oder ändert Daten im Blob in keiner Weise. Auf Datensätze kann ab dem Zeitpunkt ihres Hinzufügens zu einem Amazon Kinesis-Stream nur 24 Stunden lang zugegriffen werden. Dann werden sie automatisch verworfen.

Ihre Anwendung verwendet einen Amazon Kinesis-Streams, der in der Regel auf einer Flotte aus Amazon EC2-Instanzen ausgeführt wird. Eine Kinesis-Anwendung verwendet die Amazon Kinesis Client Library, um aus dem Amazon Kinesis-Stream zu lesen. Die Kinesis Client Library kümmert sich für Sie um eine Vielzahl von Details, einschließlich Failover, Wiederherstellung und Load Balancing. Sie gestattet der Anwendung, sich auf die Verarbeitung der Daten zu konzentrieren, sowie sie verfügbar sind. Nach der Verarbeitung des Datensatzes, kann Ihr Konsumentencode diesen an einen weiteren Kinesis-Stream übergeben, ihn in einen Amazon S3-Bucket, ein Redshift-Data Warehouse oder eine DynamoDB-Tabelle schreiben, oder ihn einfach verwerfen. Eine Konnektorbibliothek steht zur Verfügung, damit Sie Kinesis leichter in andere AWS-Services (z. B. DynamoDB, Redshift und S3) und Produkte von Drittanbietern, wie Apache Storm, integrieren können.

Sie können den logischen Zugriff auf Kinesis-Ressourcen steuern, indem Sie mithilfe von AWS IAM Benutzer unter Ihrem AWS-Konto erstellen und die Berechtigung dieser Benutzer zur Durchführung von Kinesis-Vorgängen kontrollieren. Um das Ausführen Ihrer Produzenten- oder Konsumentenanwendungen auf einer Amazon EC2-Instanz zu erleichtern, können Sie die Instanz mit einer IAM-Rolle konfigurieren. Dadurch werden die AWS-Anmeldeinformationen, die die mit der IAM-Rolle verbundenen Berechtigungen widerspiegeln, den Anwendungen auf der Instanz verfügbar gemacht. Das bedeutet, dass Sie Ihre Langzeit-AWS-Anmeldeinformationen nicht verwenden müssen. Rollen bieten den zusätzlichen Vorteil, dass sie temporäre Anmeldeinformationen bereitstellen, die innerhalb kurzer Zeit ablaufen. Dadurch wird eine weitere Schutzmaßnahme hinzugefügt. Sehen Sie sich für weitere Informationen zu IAM-Rollen auch den Leitfaden IAM verwenden an.

Auf die Amazon Kinesis-API kann nur über einen SSL-verschlüsselten Endpunkt zugegriffen werden (kinesis.us-east-1.amazonaws.com), um eine sichere Übertragung von Daten zu AWS sicherzustellen. Sie müssen eine Verbindung mit dem Endpunkt herstellen, um auf Kinesis zugreifen zu können. Aber Sie können dann die API verwenden, um AWS Kinesis anzuweisen, einen Stream in jeder beliebigen AWS Region zu erstellen.

Amazon AppStream

Der Amazon AppStream-Service bietet ein Framework für das Ausführen von Streaming-Anwendungen, insbesondere für Anwendungen, die einfache Clients erfordern, die auf Mobilgeräten ausgeführt werden. So können Sie die Anwendung auf leistungsstarken, parallel verarbeitenden GPUs in der Cloud speichern und ausführen und die Eingaben und Ausgaben dann auf jegliches Client-Gerät streamen. Das kann eine zuvor vorhandene Anwendung sein, die Sie so bearbeitet haben, dass sie mit Amazon AppStream zusammenarbeitet oder eine neue Anwendung, die sie für die Zusammenarbeit mit dem Service entworfen haben.

Das Amazon AppStream SDK vereinfacht die Entwicklung von interaktiven Streaming- und Client-Anwendungen. Das SDK bietet APIs, über die Kundengeräte direkt mit der Anwendung verbunden werden, die Audio und Video erfassen und codieren, die Inhalte über das Internet nahezu in Echtzeit streamen und die Inhalte auf Client-Geräten decodieren sowie Benutzereingaben an die Anwendung zurückgegeben können. Da die Verarbeitung der Anwendung in der Cloud geschieht, kann die Anwendung skalieren und so extrem große Rechenlasten stemmen.

Amazon AppStream verteilt Streaming-Anwendungen auf Amazon EC2. Wenn Sie eine Streaming-Anwendung über die AWS Management Console verteilen, erstellt der Service das erforderliche Amazon Machine Image (AMI) zum Hosten der Anwendung und macht die Anwendung für Streaming-Clients verfügbar. Der Service skaliert die Anwendung bei Bedarf innerhalb der eingerichteten Kapazitätsgrenzen entsprechend den Anforderungen. Clients mit Amazon AppStream SDK stellen automatisch eine Verbindung mit der gestreamten Anwendung her.

Meistens werden Sie sicherstellen wollen, dass der Benutzer, der den Client ausführt, zur Nutzung der Anwendung autorisiert ist, bevor er eine Sitzungs-ID erhält. Wir empfehlen die Verwendung eines Berechtigungs-Service. Das ist ein Service, der Clients authentifiziert zudem deren Verbindung zur Anwendung autorisiert. In diesem Fall ruft der Berechtigungs-Service zudem die Amazon AppStream REST-API auf und erstellt eine neue Streaming-Sitzung für den Client. Nachdem der Berechtigungs-Service eine neue Sitzung erstellt hat, wird der Sitzungsbezeichner (session identifier) an den Client als Einmal-Berechtigungs-URL zurückgegeben. Der Client verwendet dieses Berechtigungs-URL zur Herstellung einer Verbindung mit der Anwendung. Der Berechtigungs-Service kann auf einer Amazon EC2-Instanz oder auf AWS Elastic Beanstalk gehostet werden.

Amazon AppStream verwendet ein AWS CloudFormation-Template, welche den Vorgang der Verteilung einer GPU EC2-Instanz mit den installierten AppStream Windows-Anwendungs- und Windows Client SDK-Bibliotheken automatisiert. Das Template ist für SSH-, RDC- oder VPN-Zugriff konfiguriert und ihm wurde eine Elastic IP-Adresse zugewiesen. Wenn Sie dieses Template zur Verteilung Ihres Standalone-Streaming-Servers verwendet, müssen Sie nur die Anwendung auf den Server hochladen und den Befehl zum Start ausführen. Danach können Sie die Anwendung mit dem Amazon AppStream Service Simulator-Tool im Standalone-Modus testen, bevor Sie sie produktiv einsetzen.

Amazon AppStream nutzt zudem das STX-Protokoll, um das Streaming der Anwendung von AWS zu lokalen Geräten zu verwalten. Das Amazon AppStream STX-Protokoll ist ein proprietäres Protokoll. Es wird zum Streamen von hochgradig qualitativen Videos über unterschiedliche Netzwerkverbindungen verwendet. Es überwacht die Netzwerkbedingungen und passt den Videostream automatisch an, damit Ihre Kunden von geringer Latenz und hoher Auflösung profitieren. Amazon AppStream verringert die Latenz, synchronisiert Audio und Video und erfasst Kundeneingaben, die an die Anwendung, die in AWS ausgeführt wird, zurückgegeben werden.

Sicherheit bei AWS CloudHSM

Der AWS CloudHSM-Service bietet Kunden einen dedizierten Zugriff auf ein Hardware-Sicherheitsmodul (HSM). Dieses wurde für eine sichere Speicherung kryptografischer Schlüssel entwickelt und ermöglicht es, Vorgänge innerhalb eines eingriffshemmenden und originalitätssicheren Geräts auszuführen. Sie können die für die Datenverschlüsselung verwendeten kryptografischen Schlüssel generieren, speichern und verwalten. Nur Sie können darauf zugreifen. Mit AWS CloudHSM-Geräten wird kryptografisches Schlüsselmaterial für eine Vielzahl von Verwendungen gespeichert und verarbeitet. Dazu zählen Datenbankverschlüsselung, Digital Rights Management (DRM), Public Key Infrastructure (PKI), Authentifizierung und Autorisierung sowie Dokumentsignierung und Transaktionsverarbeitung. Sie unterstützen einige der stärksten verfügbaren kryptografischen Algorithmen, einschließlich AES, RSA und ECC sowie viele andere.

Der AWS CloudHSM-Service kann zusammen mit Amazon EC2 und VPC verwendet werden. In diesem Fall erhält das Gerät eine eigene private IP-Adresse innerhalb des privaten Subnetzes. Sie können aus den EC2-Services über SSL/TLS eine Verbindung zu CloudHSM-Geräten herstellen. SSL/TLS nutzt die digitale Zwei-Wege-Zertifikatsauthentifizierung und SSL-Verschlüsselung mit 256 Bit zur Bereitstellung eines sicheren Kommunikationskanals.

Um die Netzwerklatenz zu verringern ist es empfehlenswert, CloudHSM in der gleichen Region wie die EC2-Instanz auszuwählen. Das kann die Performance Ihrer Anwendung erhöhen. Sie können einen Client auf der EC2-Instanz konfigurieren, der Ihren Anwendungen ermöglicht, die vom HSM bereitgestellten APIs zu verwenden. Dazu gehören PKCS#11, MS CAPI und Java JCA/JCE (Java Cryptography Architecture/Java Cryptography Extensions).

Bevor Sie ein HSM verwenden können, müssen Sie mindestens eine Partition auf dem Gerät erstellen. Eine kryptografische Partition ist eine logische und physische Sicherheitsgrenze, die den Zugriff auf die Schlüssel einschränkt, damit nur Sie die Schlüssel und die vom HSM durchgeführten Vorgänge steuern können. AWS verfügt über administrative Anmeldeinformationen für das HSM-Modul. Diese Anmeldeinformationen ermöglichen jedoch nur eine Verwaltung des HSM-Moduls, nicht jedoch der HSM-Partitionen auf dem Gerät. AWS verwendet diese Anmeldeinformationen zur Überwachung und Wartung des Status und der Verfügbarkeit Ihres HSM-Geräts. AWS kann die Schlüssel weder extrahieren noch das Gerät dazu bringen, einen kryptografischen Vorgang mit den Schlüsseln durchzuführen.

Das HSM-Gerät verfügt über physische und logische Eingriffserkennung und Antwortmechanismen. Diese löschen das kryptografische Schlüsselmaterial und generieren Ereignisprotokolle, falls ein Eingriff festgestellt wird. Das HSM-Gerät soll Eingriffe erkennen, falls die physische Sperrschicht des HSM-Geräts verletzt wird. Außerdem löscht das HSM-Gerät die HSM-Partitionen nach drei erfolglosen Versuchen, auf eine HSM-Partition mit Anmeldeinformationen des HSM-Administrators zuzugreifen.

Wenn das CloudHSM-Abonnement endet und Sie überprüft haben, dass der Inhalt des HSM nicht mehr benötigt wird, müssen Sie jede Partition und ihren Inhalt sowie die Protokolle löschen. AWS setzt das Gerät als Teil des Stilllegungsvorgangs zurück und löscht somit jegliches Schlüsselmaterial permanent.

Sicherheit bei AWS CloudTrail

AWS CloudTrail bietet ein Protokoll aller Anforderungen nach AWS-Ressourcen innerhalb Ihres Kontos. Für jedes aufgezeichnete Ereignis wird Folgendes angezeigt: auf welchen Service zugegriffen wurde, welche Aktion wozu durchgeführt wurde, alle Parameter der Aktion und wer die Anforderung gestellt hat. Sie können sehen, welcher Benutzer oder Service eine Aktion auf einem AWS-Service durchgeführt hat und ob es ein AWS-Stammkontobenutzer, ein IAM-Benutzer oder ein Rollen- bzw. Verbundbenutzer mit temporärer Sicherheits-Anmeldeinformationen war.

CloudTrail erfasst im Grunde Informationen zu jedem API-Aufruf einer AWS-Ressource. Der Aufruf kann von der AWS Management Console, CLI oder einem SDK stammen. Wird beim API-Aufruf ein Fehler zurückgegeben, stellt CloudTrail die Fehlerbeschreibung, einschließlich der Meldungen für Autorisierungsfehler, bereit.

Sobald Sie CloudTrail aktiviert haben, werden alle 5 Minuten Ereignisprotokolle an den ausgewählten S3-Bucket geliefert. Die Protokolldateien werden nach AWS-Konto-ID, Region, Servicename sowie Datum und Uhrzeit organisiert. Sie können CloudTrail so konfigurieren, dass Protokolldateien aus mehreren Regionen in einem einzelnen Amazon S3-Bucket aggregiert werden. Von dort aus können Sie sie dann auf Ihre bevorzugten Protokollverwaltungs- und -analyselösungen hochladen, um Sicherheitsanalysen durchzuführen und Benutzerverhaltensmuster zu erkennen.

Standardmäßig werden Protokolldateien unbegrenzt gespeichert. Die Protokolldateien werden mithilfe von S3 Server Side Encryption automatisch verschlüsselt und verbleiben im Bucket, bis Sie sie löschen oder archivieren. Mit Amazon S3-Lebenszyklus-Konfigurationsregeln können Sie alte Protokolldateien automatisch löschen oder in Amazon Glacier zur weiteren Lagerung kostengünstig archivieren.

Wie bei jedem anderen AWS-Service können Sie den Zugriff auf CloudTrail auf bestimmte Benutzer beschränken. Mit IAM können Sie steuern, welche AWS-Benutzer AWS CloudTrail-Spuren erstellen, konfigurieren oder löschen und welche Benutzer eine Protokollierung starten oder beenden können. Sie können den Zugriff auf die Protokolldateien mit IAM- oder S3-Bucketrichtlinien steuern. Sie können noch mehr Sicherheit erreichen, indem Sie auf dem S3-Bucket MFA Delete aktivieren.

Amazon WorkSpaces

Amazon WorkSpaces ist ein Managed Desktop-Service, der eine schnelle Bereitstellung von Cloud-basierten Desktops für Benutzer erlaubt. Sie wählen einfach ein Windows 7-Bundle, das den Anforderungen Ihrer Benutzer am besten entspricht und die Anzahl der WorkSpaces, die Sie starten möchten. Sobald WorkSpace bereit ist, erhalten Benutzer eine E-Mail mit Informationen dazu, wo sie den erforderlichen Client herunterladen und sich bei WorkSpace anmelden können. Sie können dann von einer Reihe von Endpunktgeräten aus auf den Cloud-basierten Desktop zugreifen, z. B. PCs, Laptops und Mobilgeräte. Allerdings werden die Daten Ihrer Organisation niemals an das Gerät des Endbenutzers gesendet oder dort gespeichert. Denn Amazon WorkSpace nutzt PC-over-IP (PCoIP). Dieses Verfahren bietet interaktives Video-Streaming ohne Übertragung der eigentlichen Daten. Das PCoIP-Protokoll komprimiert, verschlüsselt und codiert die Desktop-EDV des Benutzers. Sie überträgt „nur Pixel“ über jedes Standard-IP-Netzwerk an Endbenutzergeräte.

Für Zugriff auf den WorkSpace müssen Benutzer sich mit speziellen Anmeldeinformationen oder mit ihren regulären Active Directory-Anmeldeinformationen anmelden. Wenn Sie Amazon WorkSpace in das Active Directory des Unternehmens integrieren, gliedert sich WorkSpace in die Active Directory-Domäne ein und lässt sich genau wie jeder andere Desktop in der Organisation verwalten. Sie können WorkSpaces von Benutzern also mit Active Directory-Gruppenrichtlinien verwalten und Konfigurationsoptionen zur Steuerung des Desktops festlegen. Es ist nicht erforderlich, Active Directory oder eine andere Art lokales Verzeichnis zum Verwalten der Benutzer-WorkSpaces zu nutzen. In diesem Fall erstellen Sie innerhalb von Amazon WorkSpaces ein privates Cloudverzeichnis, das Sie zur Administration verwenden.

Jeder Workspace befindet sich auf einer eigenen EC2-Instanz innerhalb einer VPC. Sie können WorkSpaces in einer VPC erstellen, die Sie bereits besitzen. Oder Sie lassen WorkSpace mithilfe der WorkSpaces Quick Start-Option automatisch eine VPC für Sie erstellen. Bei Verwendung der Quick Start-Option erstellt WorkSpaces nicht nur die VPC, sondern führt auch einige weitere Bereitstellungs- und Konfigurationsaufgaben für Sie durch. Dazu zählen das Erstellen eines Internet Gateways für die VPC, das Einrichten eines Verzeichnisses innerhalb der VPC, das zum Speichern von Benutzer- und WorkSpace-Informationen verwendet wird, das Erstellen eines Verzeichnisadministratorkontos, das Erstellen der angegebenen Benutzerkonten und das Hinzufügen dieser Konten zum Verzeichnis sowie das Erstellen der WorkSpace-Instanzen. Die VPC kann mithilfe einer sicheren VPN-Verbindung auch mit einem lokalen Netzwerk verbunden werden, um den Zugriff auf ein vorhandenes lokales Active Directory und andere Intranetressourcen zu ermöglichen.

Dauerhafter Speicher für WorkSpaces wird von Amazon EBS bereitgestellt und zweimal täglich automatisch auf Amazon S3 gesichert. Ist WorkSpaces Sync auf einem WorkSpace aktiviert, wird der vom Benutzer gewählte Ordner kontinuierlich gesichert und auf Amazon S3 gespeichert. Sie können mit WorkSpaces Sync auf einem Mac oder PC auch Dokumente mit Ihrem WorkSpace synchronisieren. So haben Sie unabhängig vom verwendeten Desktopcomputer immer Zugriff auf Ihre Daten.

Da Workspaces ein verwalteter Service ist, kümmert AWS sich um bestimmte Sicherheits- und Wartungsaufgaben, wie tägliche Sicherungen und Patches. Updates von WorkSpace werden während eines wöchentlichen Wartungsfensters automatisch durchgeführt. Sie können die Konfiguration des Patch-Vorgangs für den WorkSpace eines Benutzers steuern. Standardmäßig ist Windows Update eingeschaltet. Sie können diese Einstellungen jedoch anpassen oder auf Wunsch einen alternativen Ansatz zur Patch-Verwaltung wählen. Für das zugrunde liegende OS ist Windows Update auf WorkSpaces standardmäßig aktiviert und für eine wöchentliche Installation von Updates konfiguriert. Sie können einen alternativen Patch-Ansatz wählen. Oder Sie konfigurieren Windows Updates so, dass Updates zu einem von Ihnen bestimmten Zeitpunkt durchgeführt werden.

Sie können mit IAM steuern, wer im Team administrative Funktionen wahrnehmen kann, z. B. das Erstellen oder Löschen von WorkSpaces oder das Einrichten von Benutzerverzeichnissen. Sie können auch einen WorkSpace für die Verzeichnisadministration einrichten, die von Ihnen bevorzugten Administrationstools für Active Directory installieren und Organisationseinheiten und Gruppenrichtlinien erstellen. Dadurch lassen sich Änderungen in der Active Directory leichter auf alle WorkSpace-Benutzer anwenden.

Anhang – Glossar und Begriffe

AMI: Ein Amazon Machine Image (AMI) ist ein in Amazon S3 gespeichertes, verschlüsseltes Computerabbild. Es enthält alle erforderlichen Informationen zum Start der Instanzen einer Kundensoftware.

Anmeldeinformationen: Elemente, über die ein Benutzer oder Prozess verfügen muss. Während des Authentifizierungsvorgangs wird den AWS-Services damit die Berechtigung für den Zugriff auf den Service bestätigt. AWS-Anmeldinformationen umfassen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel sowie X.509-Zertifikate und Multi-Faktor-Token.

API: In der Informatik definiert die Programmierschnittstelle (Application Programming Interface, API), wie eine Anwendung Services aus Bibliotheken bzw. Betriebssystemen anfordert.

Archiv: Bei Amazon Glacier ist ein Archiv eine Datei, die Sie speichern möchten. Gleichzeitig ist es eine Basiseinheit für die Speicherung. Es können beliebige Daten sein, z. B. ein Foto, ein Video oder ein Dokument. Jedes Archiv verfügt über eine eindeutige ID und optional eine Beschreibung.

Authentifizierung: Beim Authentifizierungsvorgang wird festgestellt, ob jemand oder etwas tatsächlich derjenige oder dasjenige ist, was er bzw. es zu sein vorgibt. Nicht nur Benutzer müssen authentifiziert werden. Auch jedes Programm, das eine Funktionalität aufrufen will, die von einer AWS-API freigegeben wird, muss authentifiziert werden. AWS erfordert die Authentifizierung jeder Anforderung anhand einer digitalen Signatur mit einer kryptografischen Hash-Funktion.

Auto Scaling: Ein AWS-Service, mit dem sich die Kapazität von Amazon EC2 entsprechend den definierten Bedingungen automatisch in beide Richtungen skalieren lässt.

Availability Zone: Amazon EC2-Standorte bestehen aus Regionen und Availability Zones. Availability Zones sind eigenständige Standorte, die so konzipiert sind, dass sie vor Ausfällen in anderen Availability Zonen geschützt sind, und eine kostengünstige Netzwerkkonnektivität mit geringer Latenz zu anderen Availability Zones in der gleichen Region bereitstellen.

AWS CloudFormation: Ein AWS-Bereitstellungstool, mit dem Kunden die Basiskonfiguration der AWS-Ressourcen aufzeichnen können, die zum Ausführen der Anwendungen erforderlich sind, damit sie ihre Anwendungen in einer geregelten und vorhersehbaren Weise bereitstellen und aktualisieren können.

Bastions-Host: Ein Computer, der dafür konfiguriert wurde, Angriffen standzuhalten. Er wird in der Regel auf der äußeren/öffentlichen Seite einer demilitarisierten Zone (DMZ) oder außerhalb der Firewall platziert. Sie können eine Amazon EC2-Instanz als SSH-Bastion aufsetzen indem Sie ein öffentliches Subnetzes als Teil einer Amazon VPC einrichten.

Bucket: Ein Container für Objekte, die in Amazon S3 gespeichert werden. Jedes Objekt ist in einem Bucket enthalten. Beispielsweise ist das Objekt namens photos/puppy.jpg, wenn es im Bucket johnsmith gespeichert wird, über die URL http://johnsmith.s3.amazonaws.com/photos/puppy.jpg adressierbar.

CIDR-Block: Ein Classless Inter-Domain Routing-Block von IP-Adressen.

Clientseitige Verschlüsselung: Das Verschlüsseln von Daten auf Seite des Clients vor dem Hochladen auf Amazon S3.

Dedicated Instance: Amazon EC2-Instanzen, die auf der Host-Hardware-Ebene physisch isoliert sind (d. h., sie werden auf Single-Tenant-Hardware ausgeführt).

Digitale Signatur: Eine digitale Signatur ist eine kryptografische Methode, mit der die Echtheit einer digitalen Nachricht oder eines Dokuments bestätigt wird. Bei einer gültigen digitalen Signatur kann ein Empfänger davon ausgehen, dass die Nachricht von einem autorisierten Versender erstellt und während der Übermittlung nicht verändert wurde. Digitale Signaturen werden von Kunden als Teil des Authentifizierungsvorgangs zum Signieren von Anforderungen bei den AWS-APIs verwendet.

Direct Connect Service: Ein Amazon-Service, der Ihnen die Bereitstellung einer direkten Verknüpfung zwischen dem internen Netzwerk und einer AWS-Region mithilfe einer dedizierten Verbindung mit hohem Durchsatz ermöglicht. Mit dieser dedizierten Verbindung können Sie dann direkte logische Verbindungen zur AWS-Cloud (z. B. zu Amazon EC2 und Amazon S3) und zu Amazon VPC herstellen. Sie umgehen dadurch Internetprovider im Netzwerkpfad.

DynamoDB-Service: Ein vollständig verwalteter NoSQL-Datenbank-Service von AWS. Er bietet schnelle und planbare Leistung mit nahtloser Skalierbarkeit.

EBS: Amazon Elastic Block Store (EBS) bietet Speichervolumen zur Verwendung mit Amazon EC2-Instanzen auf Blockebene. Amazon EBS-Volumen sind Speicher außerhalb der Instanzen. Sie bestehen unabhängig von der Instanz.

Elastic Beanstalk: Ein Entwicklungs- und Verwaltungstool von AWS. Es automatisiert die Funktionen der Kapazitätsbereitstellung, des Load Balancing und des Auto Scaling von Kundenanwendungen.

Elastic IP-Adresse: Eine statische, öffentliche IP-Adresse, die Sie jeder Instanz in einer Amazon VPC zuweisen können, wodurch die Instanz öffentlich wird. Mit Elastic IP-Adressen können Sie auch Instanz-Fehler maskieren, indem Sie Ihre öffentliche IP-Adresse schnell jeder beliebigen Instanz in einer VPC neu zuweisen können.

Elastic Load Balancing: Ein AWS-Service, mit dem der Datenverkehr auf einer Flotte von Amazon EC2-Instanzen verwaltet und auf Instanzen über alle Availability Zones innerhalb einer Region hinweg verteilt werden kann. Elastic Load Balancing kombiniert die Vorteile eines lokalen Load Balancers mit mehreren Sicherheitsvorteilen. Dazu zählen die Übernahme der Ver- und Entschlüsselung von EC2-Instanzen und ihre zentrale Verwaltung auf dem Load Balancer.

Elastic MapReduce (EMR) Service: Ein AWS-Web-Service, der ein gehostetes Hadoop-Framework verwendet. Dieses nutzt die webweite Infrastruktur von Amazon EC2 und Amazon S3. Mit Elastic MapReduce können Kunden leicht und kostengünstig extrem große Datenmengen („Big Data“) verarbeiten.

Elastic Network Interface: Innerhalb einer Amazon VPC stellt ein Elastic Network Interface eine optionale zweite Netzwerkschnittstelle dar, die an eine EC2-Instanz angefügt werden kann. Mit einem Elastic Network Interface können Sie ein Management-Netzwerk erstellen oder Netzwerk- und Sicherheitsanwendungen in der Amazon VPC verwenden. Es kann einfach von einer Instanz getrennt und einer anderen hinzugefügt werden.

ElastiCache: Ein AWS-Web-Service, der das Einrichten, Verwalten und Skalieren verteilter In-Memory-Cache-Umgebungen in der Cloud ermöglicht. Der Service verbessert die Leistung von Webanwendungen. Er ermöglicht Ihnen, Informationen aus einem schnellen, verwalteten In-Memory-Cache-System abzurufen, anstatt vollständig auf langsamere datenträgerbasierte Datenbanken angewiesen zu sein.

Endpunkt: Eine URL, die als Eintrittspunkt für einen AWS-Service fungiert: Um die Datenlatenz in Ihrer Anwendung zu verringern, ermöglichen die meisten AWS-Services die Auswahl eines regionalen Endpunkts zur Durchführung der Anforderung. Einige Web-Services ermöglichen die Verwendung allgemeiner Endpunkte, die keine Region angeben.

Diese generischen Endpunkte lösen zum us-east-1-Endpunkt des Service auf. Sie können eine Verbindung mit einem AWS-Endpunkt über HTTP oder sicheres HTTP (HTTPS) mittels SSL herstellen.

Firewall: Eine Hardware- oder Softwarekomponente, die eingehenden bzw. ausgehenden Netzwerkdatenverkehr steuert. Dies geschieht entsprechend einem bestimmten Regelsatz. Über Firewall-Regeln legenSie in Amazon EC2 die Protokolle, Ports und Quell-IP-Adressbereiche fest, die berechtigt sind, auf Instanzen zuzugreifen. Diese Regeln bestimmen, welcher eingehende Netzwerkdatenverkehr an die Instanz geliefert werden soll (z. B. Web-Datenverkehr auf Port 80 akzeptieren). Amazon VPC unterstützt eine vollständige Firewall-Lösung. So wird eine Filterung des eingehenden und ausgehenden Datenverkehrs auf Instanzen erreicht. Die Standardgruppe erlaubt eingehende Kommunikation von anderen Mitgliedern derselben Gruppe und ausgehende Kommunikation zu einem beliebigen Ziel. Der Datenverkehr kann anhand des IP-Protokolls, des Service-Ports und der Quell-/Ziel-IP-Adresse (CIDR-Block (Classless Inter-Domain Routing) oder einzelne IP-Adresse) beschränkt werden.

Fragment (shard): Bei Amazon Kinesis handelt es sich bei einem Fragment um eine eindeutig identifizierte Gruppe von Datensätzen in einem Amazon Kinesis-Stream. Ein Kinesis-Stream besteht aus mehreren Fragmenten. Jedes stellt eine feste Kapazitäteneinheit bereit.

Gast-OS: In einer virtuellen Computerumgebung können mehrere Betriebssysteme auf einer einzigen Hardware ausgeführt werden. Jede dieser Instanzen wird als Gast auf der Host-Hardware betrachtet und nutzt ein eigenes Betriebssystem.

Geheimer Zugriffsschlüssel: Ein Schlüssel der Ihnen von AWS zugewiesen wird, wenn Sie ein AWS-Konto eröffnen. Jeder AWS-Benutzer, der API-Aufrufe durchführen oder mit der Befehlszeilenschnittstelle arbeiten möchte, benötigt den geheimen Zugriffsschlüssel und die Zugriffsschlüssel-ID. Der Benutzer signiert jede Anforderung mit dem geheimen Zugriffsschlüssel und integriert die Zugriffsschlüssel-ID in die Anforderung. Damit die Sicherheit des AWS-Kontos gewährleistet ist, kann auf den geheimen Zugriffsschlüssel nur während der Schlüssel- bzw. der Benutzerstellung zugegriffen werden. Sie müssen den Schlüssel speichern, wenn sie erneut auf ihn zugreifen möchten (beispielsweise in einer sicher gespeicherten Textdatei).

Hardware-Sicherheitsmodul (HSM): Ein HSM ist ein Gerät, das sichere kryptografische Schlüsselspeicherung und Vorgänge innerhalb eines originalitätssicheren Hardware-Geräts ermöglicht. Hardware-Sicherheitsmodule sollen kryptografisches Schlüsselmaterial sicher speichern und dieses Schlüsselmaterial verwenden, ohne es außerhalb der kryptografischen Grenzen des Geräts offenzulegen. Der AWS CloudHSM-Service bietet Kunden einen dedizierten, Single-Tenant-Zugriff auf ein HSM-Gerät.

Hash: Mit einer kryptografischen Hash-Funktion wird eine digitale Signatur für das Signieren von Anforderungen an AWS APIs berechnet. Ein kryptografischer Hash ist eine Einweg-Funktion, die auf Grundlage der Eingabe einen einzigartigen Hash-Wert zurückgibt. Die Eingabe zur Hash-Funktion umfasst den Text der Anforderung und den geheimen Zugriffsschlüssel. Die Hash-Funktion gibt einen Hash-Wert zurück. Dieser wird der Anforderung als Signatur hinzugefügt.

HMAC-SHA1/HMAC-SHA256: In der Kryptografie ist ein Keyed-Hash Message Authentication Code (HMAC oder KHMAC) eine Form von Nachrichten-Authentifizierungscode (Message Authentication Code, MAC). Dieser wird mit einem bestimmten Algorithmus unter Verwendung einer kryptografische Hash-Funktion in Verbindung mit einem geheimen Schlüssel berechnet. Wie bei jedem MAC kann er dazu verwendet werden, gleichzeitig die Datenintegrität und die Echtheit der Nachricht zu überprüfen. Jede interaktive kryptografische Hash-Funktion, z. B. SHA-1 oder SHA-256, kann einen HMAC berechne. Der daraus resultierende MAC-Algorithmus wird als HMAC-SHA1 bzw. HMAC-SHA256 bezeichnet. Die kryptografische Stärke des HMAC hängt von der kryptografischen Stärke der zugrunde liegenden Hash-Funktion, der Größe und Qualität des Schlüssels sowie der Größe der Hash-Ausgabelänge in Bits ab.

Hypervisor: Ein Hypervisor, auch Virtual Machine Monitor (VMM) genannt, ist eine Software zur Virtualisierung von Computersoftware- bzw. Computerhardware-Plattformen, die das gleichzeitige Ausführen mehrerer Betriebssysteme auf einem Hostcomputer ermöglicht.

Identity and Access Management (IAM): AWS IAM ermöglicht die Erstellung mehrerer Benutzer und die Verwaltung ihrer Berechtigungen innerhalb des AWS-Kontos.

Import/Export-Service: Ein AWS-Service für die Übermittlung großer Datenmengen an AWS S3 oder die EBS-Speicherung. Dazu wird ein portables Gerät physisch an einen sicheren AWS-Standort Einrichtung versendet.

Instanz: Eine Instanz ist ein virtualisierter Server (auch als virtuelle Maschine (VM) bekannt) mit eigenen Hardware-Ressourcen und Gast-OS. Bei EC2 stellt eine Instanz die laufende Kopie eines Amazon Machine Images (AMI) dar.

IP-Adresse: Eine Internetprotokoll-Adresse (kurz: IP-Adresse) ist eine numerische Kennzeichnung, die Geräten zugewiesen wird, die Teil eines Computernetzwerks sind, bei dem dieses Internetprotokoll zur Kommunikation zwischen den Knoten verwendet wird.

IP-Spoofing: Die Erstellung von IP-Paketen mit einer gefälschten Quell-IP-Adresse wird Spoofing genannt. Spoofing hat zum Ziel, die Identität des Versenders zu verbergen oder ein anderes Computersystem vorzutäuschen.

Multi-Factor Authentication (MFA): Die Verwendung von mindestens zwei Authentifizierungsfaktoren. Authentifizierungsfaktoren sind etwas, was Sie wissen (z. B. ein Kennwort) oder etwas, was sie besitzen (z. B. ein Token, der eine zufällige Nummer generiert). Mit AWS IAM kann ein sechsstelliger Einmal-Code zusätzlich zum Benutzernamen und Kennwort der Anmeldeinformationen verwendet werden. Kunden erhalten diesen Einmal-Code von einem Authentifizierungsgerät, das sich physisch in ihrem Besitz befindet (entweder ein physisches Token-Gerät oder ein virtuelles Token vom Smartphone).

Netzwerk-ACLs: Zustandslose Datenverkehrsfilter, die auf den gesamten ein- und ausgehenden Datenverkehr eines Subnetzes in einer Amazon VPC angewendet werden. Netzwerk-ACLs können hierarchische Regeln enthalten. Damit kann Datenverkehr anhand des IP-Protokolls, des Service-Ports und der Quell-/Ziel-IP-Adresse zugelassen oder abgelehnt werden.

Objekt: Die grundlegenden Entitäten, die in Amazon S3 gespeichert werden. Objekte bestehen aus Objektdaten und Metadaten. Der Datenanteil ist für Amazon S3 nicht einsichtig. Metadaten sind ein Satz von Name-Wert-Paaren, die das Objekt beschreiben. Diese beinhalten einige Standardmetadaten, z. B. das Datum der letzten Änderung, sowie Standard-HTTP-Metadaten, wie den Inhaltstyp. Der Entwickler kann bei der Speicherung des Objekts auch benutzerdefinierte Metadaten angeben.

Paravirtualisierung: In der Informatik ist Paravirtualisierung eine Virtualisierungstechnik, die virtuellen Maschinen eine Softwareschnittstelle darstellt, die der zugrunde liegenden Hardware ähnelt, aber nicht mit ihr identisch ist.

Peering: Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs, die es Ihnen ermöglicht, den Datenverkehr zwischen den VPCs mithilfe von privaten IP-Adressen zu steuern. Instanzen in jeder der VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk.

Port-Scanning: Bei einem Port-Scan handelt es sich um eine Reihe von Nachrichten, die jemand in der Absicht, in einen Computer einzudringen, sendet, um in Erfahrung zu bringen, welche Computernetzwerk-Services, die jeweils einer allgemein bekannten Portnummer zugewiesen sind, der Computer bereitstellt.

Region: Ein benannter Satz von AWS-Ressourcen im gleichen geografischen Gebiet. Jede Region enthält mindestens zwei Availability Zones.

Relational Database Service (RDS): Ein AWS-Service, mit dem Sie eine relationale Datenbank-Instanz (kurz: DB-Instanz) erstellen können. Auch die zugewiesene Rechenleistung und die Speicherkapazität lässt sich entsprechend der Anwendungsanforderung flexibel skalieren. Amazon RDS ist für MySQL, Oracle oder Microsoft SQL-Server-Datenbank-Engines verfügbar.

Replizierung: Das kontinuierliche Kopieren von Daten von einer Datenbank, mit dem Ziel eine zweite Version der Datenbank aufrechtzuerhalten, in der Regel zum Zweck der Notfallwiederherstellung. Kunden können für die Amazon RDS-Datenbankreplizierung mehrere Availability Zones verwenden. Unter MySQL können sie auch Read Replicas verwenden.

Rolle: Eine Entität in AWS IAM, die einen Satz von Berechtigungen beinhaltet, die von einer anderen Entität angenommen werden können. Mithilfe von Rollen können Anwendungen, die auf Amazon EC2-Instanzen ausgeführt werden, sicher auf AWS-Ressourcen zugreifen. Sie gewähren einer Rolle einen bestimmten Berechtigungssatz, verwenden die Rolle zum Start einer Amazon EC2-Instanz und überlassen EC2 die automatische Verwaltung der AWS-Anmeldeinformationen für die auf Amazon EC2 ausgeführten Anwendungen.

Route 53: Ein autoritatives DNS-System, das einen Update-Mechanismus bereitstellt, mit dem Entwickler öffentliche DNS-Namen verwalten, DNS-Abfragen beantworten und Domänennamen in IP-Adressen übersetzen können. Damit wird eine Kommunikation zwischen Computern ermöglicht.

Schlüssel: In der Kryptografie ist ein Schlüssel ein Parameter, der die Ausgabe eines kryptografischen Algorithmus (ein sogenannter Hashing-Algorithmus) bestimmt. Ein Schlüsselpaar ist ein Satz von Sicherheits-Anmeldeinformationen, der zum elektronischen Identitätsnachweis verwendet wird und aus einem öffentlichen und einem privaten Schlüssel besteht.

Schlüsselrotation: Ein Prozess zur periodischen Änderung der kryptografischen Schlüssel, die für die Verschlüsselung der Daten oder für digitale Signaturanforderungen verwendet werden. Genauso wie das Ändern eines Kennworts, verringert das Rotieren von Schlüsseln das Risiko eines nicht autorisierten Zugriffs, falls Angreifer den Schlüssel erhalten oder dessen Wert bestimmen können. AWS unterstützt mehrere gleichzeitige Zugriffsschlüssel und Zertifikate. Damit können Kunden Schlüssel und Zertifikate regelmäßig ohne Ausfallzeiten bei der Anwendung in und außer Betrieb nehmen.

Secure Sockets Layer (SSL): Ein kryptografisches Protokoll, das Internetsicherheit auf der Anwendungsschicht herstellt. Die Protokollspezifikationen TLS 1.0 und SSL 3.0 verwenden kryptografische Mechanismen, um Sicherheits-Services zu implementieren, mit denen eine sichere TCP/IP-Verbindung hergestellt und aufrechterhalten wird. Die sichere Verbindung verhindert das Mithören, die Einflussnahme oder die Nachrichtenfälschung. Sie können eine Verbindung mit einem AWS-Endpunkt über HTTP oder sicheres HTTP (HTTPS) mittels SSL herstellen.

Security Token Service (STS): Die APIs des AWS STS geben temporäre Sicherheits-Anmeldeinformationen zurück. Diese bestehen aus einem Sicherheits-Token, einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Sie können mit STS Sicherheits-Anmeldeinformationen an Benutzer ausgeben, die temporären Zugriff auf die Ressourcen benötigen. Diese Benutzer können vorhandene IAM-Benutzer oder Nicht-AWS-Benutzer (verbundene bzw. förderierte Identitäten), Systeme oder Anwendungen sein, die Zugriff auf die Ressourcen erfordern.

Serverseitige Verschlüsselung (SSE): Eine Option bei der S3-Speicherung für die automatische Verschlüsselung ruhender Daten. Mit Amazon S3 SSE können Daten beim Hochladen verschlüsselt werden. Dazu muss beim Schreiben des Objekts einfach ein zusätzlicher Anforderungs-Header hinzugefügt werden. Entschlüsselung geschieht automatisch bei Abruf der Daten.

Service: Software oder Rechenfähigkeit, die über ein Netzwerk bereitgestellt wird (z. B. Amazon EC2, Amazon S3).

Sicherheitsgruppe: Eine Sicherheitsgruppe verleiht Ihnen Kontrolle über die Protokolle, Ports und Quell-IP-Adressbereiche, die berechtigt sind, auf Ihre Amazon EC2-Instanz zuzugreifen. Mit anderen Worten, sie definiert die Firewall-Regeln für die Instanz. Diese Regeln bestimmen, welcher eingehende Netzwerkdatenverkehr an die Instanz geliefert werden soll (z. B. Web-Datenverkehr auf Port 80 akzeptieren).

Signatur: Bedeutet eine digitale Signatur, die eine mathematische Methode zur Bestätigung der Echtheit einer digitalen Nachricht ist. AWS verwendet Signaturen, die mit einem kryptografischen Algorithmus und Ihrem privaten Schlüssel berechnet werden. Damit lassen sich die Anforderungen, die an den Web-Service gesendet werden, authentifizieren.

Simple Data Base (Simple DB): Ein nicht relationaler Datenspeicher. Mit ihm können AWS-Kunden Datenelemente über Web-Serviceanforderungen abfragen und anfordern. Amazon SimpleDB erstellt und verwaltet mehrere geografisch verteilte Repliken der Kundendaten automatisch. So wird hohe Verfügbarkeit und Datenhaltbarkeit erreicht.

Simple Email Service (SES): Ein AWS-Service, der einen skalierbaren Service zum Versand von Massen- und Transaktions-E-Mails für Unternehmen und Entwickler bereitstellt. Die Zustellbarkeit und Zuverlässigkeit für Versender wird bei Amazon SES maximiert. Dazu werden proaktive Schritte unternommen, mit denen der Versand fragwürdiger Inhalte verhindert werden sollen. Internetanbieter können den Service daher als vertrauenswürdigen E-Mail-Ursprung erachten.

Simple Mail Transfer Protocol (SMTP): Ein Internetstandard für die Übermittlung von E-Mails über IP-Netzwerke. SMTP wird von Amazon Simple Email Service verwendet. Kunden, die Amazon SES verwenden, können eine SMTP-Schnittstelle zum Versand von E-Mails nutzen. Sie müssen aber über TLS eine Verbindung zu einem SMTP-Endpunkt herstellen.

Simple Notification Service (SNS): Ein AWS-Service, der das Einrichten, Betreiben und Versenden von Meldungen aus der Cloud vereinfacht. Amazon SNS bietet Entwicklern die Möglichkeit zum Veröffentlichen von Meldungen aus einer Anwendung und zum sofortigen Zustellen an Abonnenten oder andere Anwendungen.

Simple Queue Service (SQS): Ein besonders zuverlässiger, skalierbarer Service von AWS, der eine asynchrone nachrichtenbasierte Kommunikation zwischen verteilten Komponenten einer Anwendung ermöglicht. Die Komponenten können Computer oder Amazon EC2-Instanzen oder eine Kombination aus beidem sein.

Simple Storage Service (S3): Ein AWS-Service für die sichere Speicherung von Objektdateien. Der Zugriff auf Objekte kann auf Datei- oder Bucket-Ebene gesteuert werden. Außerdem kann er auf Grundlage anderer Bedingungen wie IP-Quelle der Anforderung, Uhrzeit der Anforderung usw. begrenzt werden. Daten lassen sich mit AES-256-Verschlüsselung auch automatisch verschlüsseln.

Simple Workflow Service (SWF): Ein AWS-Service, der Kunden das Erstellen von Anwendungen ermöglicht, die Aufgaben über verteilte Komponente koordinieren. Mit Amazon SWF können Entwickler die verschiedenen Prozessschritte bei einer Anwendung als „Tasks“ strukturieren. Diese treiben die Arbeit in verteilten Anwendungen voran. Amazon SWF koordiniert diese Tasks und managet Abhängigkeiten bei der Ausführung von Tasks, Ablaufkoordination und Gleichzeitigkeit auf Grundlage der Anwendungslogik des Entwicklers.

Single Sign-on: Die Möglichkeit, mit nur einer Anmeldung Zugriff auf mehrere Anwendungen und Systeme zu erhalten. Ein sicherer Single-Sign-on kann für Verbundbenutzer (AWS- und nicht AWS-Benutzern) ermöglicht werden, indem temporäre Sicherheits-Anmeldeinformationen über eine URL an die AWS Management Console übermittelt werden.

Snapshot: Eine vom Kunden initiierte Sicherung eines EBS-Volume, die in Amazon S3 gespeichert wird, oder eine vom Kunden initiierte Sicherung auf einer RDS-Datenbank, die in Amazon RDS gespeichert wird. Ein Snapshot kann verwendet werden als Ausgangspunkt für ein neues EBS-Volume oder eine neue Amazon RDS-Datenbank zur verwendet werden. Snapshots können auch der Sicherstellung langfristiger Datenhaltbarkeit und Wiederherstellbarkeit dienen.

Storage Gateway: Ein AWS-Service, der eine lokale Softwareanwendung des Kunden mithilfe einer VM sicher mit Amazon S3-Speicher verbindet. Der Kunde richtet auf einem Host in seinem Rechenzentrum eine VM ein, auf der VMware ESXi-Hypervisor ausgeführt wird. Daten werden asynchron von der lokalen Speicherhardware des Kunden über SSL an AWS übermittelt und dann mit AES-256 verschlüsselt in Amazon S3 gespeichert.

Struktur-Hash: Ein Baumhash wird generiert, indem ein Hash für jedes megabytegroße Datensegment berechnet wird. Dann werden die Hashes in Form eines Baums kombiniert, um stetig wachsende aneinanderhängende Datensegmente darzustellen. Glacier gleicht den Hash mit den Daten ab und stellt so sicher, dass sie auf dem Weg nicht verändert wurden.

Temporäre Sicherheits-Anmeldeinformationen: AWS-Anmeldeinformationen für den Zugriff auf AWS-Services. Mit temporären Sicherheits-Anmeldeinformationen kann ein Identitätsverbund zwischen AWS-Services und nicht AWS-Benutzern in Ihrem eigenen Identitäts- und Autorisierungssystem hergestellt werden. Temporäre Sicherheits-Anmeldeinformationen bestehen aus einem Sicherheits-Token, einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel.

Transcoder: Ein System für die Transkodierung (Konvertierung) einer Mediendatei (Audio oder Video) aus einem Format, einer Größe oder einer Qualität in eine andere. Amazon Elastic Transcoder vereinfacht die Transkodierung von Videodateien auf eine skalierbare und kostengünstige Weise.

Transport Layer Security (TLS): Dieses kryptografisches Protokoll stellt Sicherheit über das Internet auf der Anwendungsschicht bereit. Kunden, die Simple Email Service von Amazon benutzt haben, müssen über TLS eine Verbindung mit einem SMTP-Endpunkt herstellen.

Vault: In Amazon Glacier ist ein Vault ein Container zum Speichern von Archiven. Zum Erstellen eines Vaults geben Sie einen Namen an und wählen eine AWS-Region aus, in der er erstellt werden soll. Jede Vault-Ressource verfügt über eine eindeutige Adresse.

Verbundbenutzer (federated users): Benutzer, Systeme oder Anwendungen, die zwar aktuell über keine Zugriffsberechtigung für die AWS-Services verfügen, denen aber ein temporärer Zugriff gewährt werden soll. Dieser Zugriff wird über die APIs von AWS Security Token Service (STS) gewährt.

Versioning: Jedes Objekt in Amazon S3 verfügt über einen Schlüssel und eine Versions-ID. Objekte mit dem gleichen Schlüssel aber unterschiedlichen Versions-IDs können im gleichen Bucket gespeichert werden. Versioning wird auf Bucket-Ebene mithilfe von PUT Bucket-Versioning aktiviert.

Virtual MFA: Die Möglichkeit eines Benutzers, den sechsstelligen Einmal-MFA-Code vom Smartphone anstelle eines Token/Fob zu erhalten. Bei MFA wird ein zusätzlicher Faktor (der sechsstellige Code) zusammen mit dem Benutzernamen und dem Kennwort für die Authentifizierung verwendet.

Virtual Private Cloud (VPC): Ein AWS-Service, mit dem Kunden einen isolierten Bereich der AWS-Cloud bereitstellen können. Dies umfasst die Auswahl eines eigenen IP-Adressbereichs, das Definieren eines Subnetzes und das Konfigurieren von Routing-Tabellen und Netzwerk-Gateways.

Virtual Private Network (VPN): Die Möglichkeit, ein privates, sicheres Netzwerk zwischen zwei Standorten über ein öffentliches Netzwerk zu erstellen, z. B. das Internet. AWS-Kunden können eine IPsec VPN-Verbindung zwischen der Amazon VPC und ihrem Rechenzentrum hinzufügen. Dadurch wird das Rechenzentrum effektiv auf die Cloud erweitert. Außerdem wird für öffentliche Subnetz-Instanzen in der Amazon VPC direkter Zugriff auf das Internet gewährt. In dieser Konfiguration installieren die Kunden ein VPN-Gerät im Rechenzentrum Ihres Unternehmens.

Virtuelle Instanz: Sobald eine AMI gestartet wurde, wird das daraus resultierende ausgeführte System als Instanz bezeichnet. Alle Instanzen, die auf der gleichen AMI basieren, sind anfangs identisch. Jede Information darauf geht verloren, wenn die Instanz beendet wird oder ausfällt.

X.509: In der Kryptografie ist X.509 ein Standard für eine Public Key Infrastructure (PKI) für Single-Sign-on und eine Privilege Management Infrastructure (PMI). X.509 legt Standardformate für öffentliche Schlüsselzertifikate, Zertifikataufhebungslisten, Attributzertifikate und einen Überprüfungsalgorithmus für den Zertifikatspfad fest. Einige AWS-Services verwenden bei einigen Schnittstellen X.509-Zertifikate anstelle eines geheimen Zugriffsschlüssels. Beispielsweise verwendet Amazon EC2 für den Zugriff auf die Abfrageschnittstelle einen geheimen Zugriffsschlüssel aber ein Anmeldezertifikat für den Zugriff auf die SOAP- und die Befehlszeilentool-Schnittstelle.

Zertifikat: Eine Anmeldeinformation, die von einigen AWS-Services zum Authentifizieren von AWS-Konten und -Benutzern verwendet wird. Auch als X-509-Zertifikat bekannt. Das Zertifikat ist gepaart mit einem privaten Schlüssel.

Zugriffskontrollliste (ACL): Eine Liste von Berechtigungen oder Regeln für den Zugriff auf ein Objekt oder eine Netzwerkressource. In Amazon EC2 fungieren Sicherheitsgruppen auf Instanz-Ebene als Zugriffskontrolllisten. Sie steuern, welche Benutzer Zugriffsberechtigung für bestimmte Instanzen haben. Sie können in Amazon S3 mit Zugriffskontrolllisten für Benutzergruppen Lese- oder Schreibzugriff auf Buckets oder Objekten vergeben. In Amazon VPC fungieren Zugriffskontrolllisten wie Netzwerk-Firewalls. Sie steuern den Zugriff auf Subnetzebene.

Zugriffsschlüssel-ID: Eine Zeichenfolge, die AWS verteilt, um jeden AWS-Benutzer eindeutig zu identifizieren. Es ist ein alphanumerisches Token, das mit Ihrem geheimen Zugriffsschlüssel verknüpft ist.

Zustandbehaftete Firewall: In der Informatik überwacht eine zustandbehaftete Firewall (jede Firewall, die zustandbehaftete Paketüberprüfungen (SPI) oder zustandbehaftete Überprüfungen durchführt) den Zustand von Netzwerkverbindungen (z. B. TCP-Streams, UDP-Kommunikation), die durch sie hindurch laufen.

Änderungen seit der letzen Version (Nov 2013):

- Aktualisierte Regionen
- Einige Regionen wurden mit neuen Funktionen aktualisiert: CloudFront, DirectConnect, DynamoDB, EBS, ELB, EMR, Glacier, IAM, OpsWorks, RDS, RedShift, Route 53, Storage Gateway und VPC
- Sicherheit bei AppStream hinzugefügt
- Sicherheit bei CloudTrail hinzugefügt
- Sicherheit bei Amazon Kinesis hinzugefügt
- Sicherheit bei WorkSpaces hinzugefügt

Änderungen seit der letzen Version (Mai/Juni 2013):

- IAM mit Rollen und API-Zugriff aktualisiert
- MFA mit API-Zugriff für Kunden-definierte privilegierte Aktionen aktualisiert
- RDS aktualisiert, Ereignisbenachrichtigungen, Multi-AZ und SSL to SQL-Server 2012 hinzugefügt
- VPC aktualisiert, Mehrfach-IP-Adressen, statische Routing-VPN und standardmäßige VPC-By-Default
- Mehrere weitere Services mit neuen Funktionen aktualisiert: CloudFront, CloudWatch, EBS, ElastiCache, Elastic Beanstalk, Route 53, S3, Storage Gateway
- Sicherheit bei Glacier hinzugefügt
- Sicherheit bei RedShift hinzugefügt
- Sicherheit bei Data Pipeline hinzugefügt
- Sicherheit bei Transcoder hinzugefügt
- Sicherheit bei Trusted Advisor hinzugefügt
- Sicherheit bei OpsWorks hinzugefügt
- Sicherheit bei CloudHSM hinzugefügt

Änderungen seit der letzen Version (Mai 2011):

- Neugestaltung zur besseren Identifizierung der Infrastruktur gegenüber servicespezifischer Sicherheit
- Überschrift „Zusammenfassung der Kontrollumgebung“ auf „AWS-Compliance-Programm“ geändert
- Überschrift „Information und Kommunikation“ auf „Verwaltung und Kommunikation“ geändert
- Überschrift „Mitarbeiterlaufbahn“ auf „Logischer Zugriff“ geändert
- Überschrift „Konfigurationsverwaltung“ auf „Änderungsverwaltung" geändert
- Abschnitt „Umgebungssicherheitsrichtlinien“ mit Abschnitt „Physische Sicherheit“ zusammengelegt
- Informationen im Abschnitt „Sicherungen“ in den Abschnitten „S3“, "SimpleDB“ und „EBS“ eingefügt
- Aktualisierung von Zertifikaten, um die SAS70-Namensänderung zu SSAE 16 umzusetzen, und FedRAMP hinzugefügt
- Aktualisierung des Abschnitts „Netzwerksicherheit“, um Sichere Netzwerkarchitektur und Netzwerküberwachung und -schutz hinzuzufügen
- Aktualisierung von IAM, um Rollen-/Schlüsselbereitstellung, virtuelle MFA, temporäre Sicherheits-Anmeldeinformationen und einzelne Anmeldung einzufügen
- Aktualisierung von Regionen, um neue Regionen und eine GovCloud-Beschreibung einzufügen
- EBS, S3, SimpleDB, RDS und EMR aktualisiert, um Service- und Sicherheitsbeschreibungen zu verdeutlichen
- Aktualisierung von VPC, um Konfigurationsoptionen, VPN und Schnittstellen für elastische Netzwerke hinzuzufügen
- Aktualisierung des Abschnitts „Amazon Direct Connect-Sicherheit“
- Aktualisierung des Abschnitts „Sicherheit bei Amazon Elastic Load Balancing“
- Hinzufügen von AWS Storage Gateway-Sicherheit

- Hinzufügen von AWS Import/Export-Sicherheit
- Hinzufügen von Sicherheit bei Auto Scaling
- Hinzufügen von Amazon DynamoDB-Sicherheit
- Hinzufügen von Sicherheit bei Amazon ElastiCache
- Hinzufügen von Sicherheit bei Amazon Simple Workflow Service (Amazon SWS)
- Hinzufügen von Sicherheit bei Amazon Simple Email Service (Amazon SES)
- Hinzufügen von Sicherheit bei Amazon Route 53
- Hinzufügen von Sicherheit bei Amazon CloudSearch
- Hinzufügen von Sicherheit bei AWS Elastic Beanstalk
- Hinzufügen von Sicherheit bei AWS CloudFormation
- Glossar aktualisiert

Änderungen seit der letzen Version (Aug 2010):

- Hinzufügen von AWS Identity and Access Management (AWS IAM)
- Hinzufügen von Sicherheit bei Amazon Simple Notification Service (Amazon SNS)
- Hinzufügen von Sicherheit bei Amazon CloudWatch
- Hinzufügen von Sicherheit bei Auto Scaling
- Aktualisierung von Amazon Virtual Private Cloud (Amazon VPC)
- Aktualisierung der Kontrollumgebung
- Entfernen von Risikomanagement, ausführliche Darstellung in einem eigenen Whitepaper

Änderungen seit der letzen Version (Nov 2009):

- Hauptrevidierung

Änderungen seit der letzen Version (Juni 2009):

- Änderung des Abschnitts „Zertifikate und Akkreditierungen“, um SAS70 einzubeziehen
- Hinzufügen von Amazon Virtual Private Cloud (Amazon VPC)
- Hinzufügen des Abschnitts „Sicherheits-Anmeldeinformationen“, um AWS Multi-Faktor-Authentifizierung und Schlüsselrotation hervorzuheben
- Hinzufügen von Amazon Relational Database Service (Amazon RDS)-Sicherheit

Änderungen seit der letzen Version (Sep 2008):

- Hinzufügen von Grundsätzen für ein sicheres Design
- Aktualisierung von Informationen zu physischer Sicherheit und Hinzufügen von Hintergründüberprüfungen
- Abschnitt „Sicherungen“ hinsichtlich Amazon EBS aktualisiert
- Aktualisierung des Abschnitts „Sicherheit bei Amazon EC2“, um Folgendes hinzuzufügen:
- Zertifikatbasiertes SSHv2
- Informationen und Diagramm zu Sicherheitsgruppen mit mehreren Ebenen
- Beschreibung von Hypervisor und Diagramm zu Instanz-Isolierung
- Fehlertrennung
- Hinzufügen von Konfigurationsverwaltung
- Abschnitt „Amazon S3“ mit Informationen und Verdeutlichungen aktualisiert
- Aktualisierung der Außerbetriebnahme von Speichergeräten
- Hinzufügen von Sicherheit bei Amazon SQS
- Hinzufügen von Sicherheit bei Amazon CloudFront
- Hinzufügen von Sicherheit bei Amazon Elastic MapReduce

Anmerkungen