AWS Whitepaper

AWS Outposts Überlegungen zu Design und Architektur für hohe Verfügbarkeit

AWS Outposts Überlegungen zu Design und Architektur für hohe Verfügbarkeit: AWS Whitepaper

Table of Contents

AWS Outposts Überlegungen zu Design und Architektur für hohe Verfügbarkeit

Datum der Veröffentlichung: 12. August 2021 () Dokumentverlauf

In diesem Whitepaper werden Überlegungen zur Architektur und empfohlene Vorgehensweisen erörtert, die IT-Manager und Systemarchitekten anwenden können, um hochverfügbare lokale Anwendungsumgebungen aufzubauen. AWS Outposts

Sind Sie Well-Architected?

Das AWS Well-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile der Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen in der Cloud treffen. Die sechs Säulen des Frameworks ermöglichen es Ihnen, bewährte Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme kennenzulernen. Mithilfe des AWS Well-Architected Tool, das kostenlos im verfügbar ist AWS Management Console, können Sie Ihre Workloads anhand dieser bewährten Methoden überprüfen, indem Sie für jede Säule eine Reihe von Fragen beantworten.

Weitere Expertentipps und bewährte Methoden für Ihre Cloud-Architektur — Referenzarchitekturbereitstellungen, Diagramme und Whitepapers — finden Sie im Architecture Center.AWS

Einführung

Dieses paper richtet sich an IT-Manager und Systemarchitekten, die Anwendungen mithilfe der AWS Cloud-Plattform bereitstellen, migrieren und betreiben und diese Anwendungen vor Ort mit AWS Outposts Rack, dem 42U-Rack-Formfaktor von AWS Outposts, ausführen möchten.

Es werden Architekturmuster, Anti-Patterns und empfohlene Verfahren für den Aufbau hochverfügbarer Systeme mit Rack vorgestellt. AWS Outposts Sie lernen, wie Sie Ihre AWS Outposts Rack-Kapazität verwalten und wie Sie Netzwerk- und Rechenzentrumsdienste nutzen, um hochverfügbare AWS Outposts Rack-Infrastrukturlösungen einzurichten.

AWS Outposts Rack ist ein vollständig verwalteter Service, der einen logischen Pool von Cloud-Rechen-, Speicher- und Netzwerkfunktionen bereitstellt. Mit Outposts-Racks können Kunden

unterstützte AWS Managed Services in ihren lokalen Umgebungen nutzen, darunter: Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon S3 on Outposts, AmazonElastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service(Amazon ECS), Amazon Relational Database Service(Amazon RDS) und andere Services auf Outposts.AWS Dienste auf Outposts werden auf demselben AWS Nitro-System bereitgestellt, das in der verwendet wird. AWS-Regionen

Durch die Nutzung von AWS Outposts Rack können Sie hochverfügbare lokale Anwendungen mit vertrauten AWS Cloud-Diensten und -Tools erstellen, verwalten und skalieren. AWS Outposts Rack eignet sich ideal für Workloads, die Zugriff auf lokale Systeme mit geringer Latenz, lokale Datenverarbeitung, Datenresidenz und Migration von Anwendungen mit lokalen Systemabhängigkeiten erfordern.

Erweiterung der AWS Infrastruktur und der Dienste auf lokale Standorte

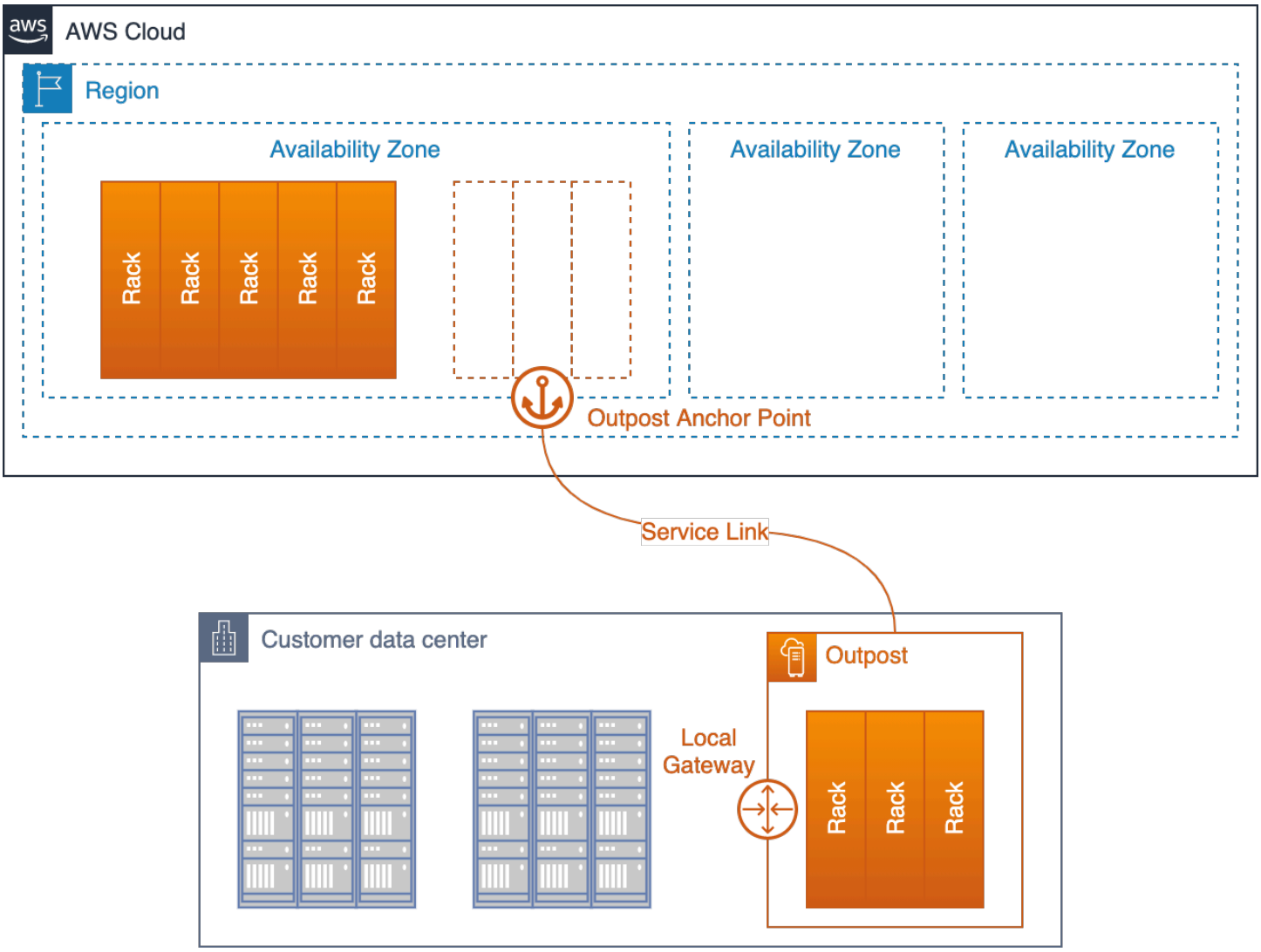
Der AWS Outposts Service stellt AWS Infrastruktur und Dienste für lokale Standorte in mehr als 50 Ländern und Gebieten bereit und gibt Kunden die Möglichkeit, dieselbe AWS Infrastruktur, AWS Dienste und Tools in praktisch jedem Rechenzentrum APIs, jeder Kollokationsfläche oder lokalen Einrichtung bereitzustellen, um ein wirklich konsistentes Hybriderlebnis zu erzielen. Um zu verstehen, wie man mit Outposts designt, sollten Sie die verschiedenen Ebenen verstehen, aus denen sich die AWS Cloud zusammensetzt.

An AWS-Regionist ein geografisches Gebiet der Welt. Jedes AWS-Region ist eine Sammlung von Rechenzentren, die logisch in Availability Zones (AZs) gruppiert sind. AWS-Regionen stellen mehrere (mindestens zwei) physisch getrennte und isolierte Availability Zones bereit, die mit geringer Latenz, hohem Durchsatz und redundanter Netzwerkkonnektivität verbunden sind. Jede AZ besteht aus einem oder mehreren physischen Rechenzentren.

Ein logischer Outpost (im Folgenden als Outpost bezeichnet) ist eine Bereitstellung von einem oder mehreren physisch verbundenen AWS Outposts Racks, die als eine Einheit verwaltet werden. Ein Outpost bietet einen Pool an AWS Rechen- und Speicherkapazität an einem Ihrer Standorte als private Erweiterung einer AZ in einem. AWS-Region

Das vielleicht beste Konzeptmodell dafür AWS Outposts ist, ein oder mehrere Racks von einem Rechenzentrum in einer AZ of an AWS-Region zu trennen und es in Ihrem eigenen Rechenzentrum oder Ihrer eigenen Colocation-Einrichtung zu installieren. Sie rollen die Racks vom AZ-Rechenzentrum zu Ihrem Rechenzentrum. Anschließend stecken Sie die Racks mit einem (sehr) langen Kabel an die Ankerpunkte im AZ-Rechenzentrum, sodass die Racks weiterhin als Teil des

AWS-Region Sie schließen sie auch an Ihr lokales Netzwerk an, um eine Konnektivität mit geringer Latenz zwischen Ihren lokalen Netzwerken und den Workloads zu gewährleisten, die auf diesen Racks ausgeführt werden. Auf diese Weise erhalten Sie die Betriebs- und API-Konsistenz von AWS Cloud, während Ihre Arbeitslast lokal bleibt.



Ein Außenposten, der in einem Kundenrechenzentrum eingerichtet und wieder mit dem Hauptstandort AZ und der übergeordneten Region verbunden ist

Der Outpost fungiert als Erweiterung des AZ, in dem er verankert ist. AWS betreibt, überwacht und verwaltet die AWS Outposts Infrastruktur als Teil der. AWS-Region Anstatt eines sehr langen physischen Kabels verbindet sich ein Outpost über eine Reihe verschlüsselter VPN-Tunnel, den Service Link, wieder mit seiner übergeordneten Region.

Der Service Link endet an einer Reihe von Ankerpunkten in einer Availability Zone (AZ) in der übergeordneten Region des Outposts.

Sie wählen, wo Ihre Inhalte gespeichert werden. Sie können Ihre Inhalte an den AWS-Region oder anderen Speicherorten replizieren und sichern. Ihre Inhalte werden ohne Ihre Zustimmung nicht außerhalb der von Ihnen ausgewählten Standorte verschoben oder kopiert, es sei denn, dies ist erforderlich, um dem Gesetz oder einer verbindlichen Anordnung einer Regierungsbehörde nachzukommen. Weitere Informationen finden Sie in den AWS Häufig gestellten Fragen zum Datenschutz.

Die Workloads, die Sie auf diesen Racks bereitstellen, werden lokal ausgeführt. Und obwohl die in diesen Racks verfügbare Rechen- und Speicherkapazität begrenzt ist und die Ausführung der Cloud-Dienste eines nicht möglich ist AWS-Region, profitieren die auf dem Rack bereitgestellten Ressourcen (Ihre Instanzen und deren lokaler Speicher) von den Vorteilen, dass sie lokal ausgeführt werden, während die Managementebene weiterhin im Rack betrieben wird. AWS-Region

Um Workloads auf einem Outpost bereitzustellen, fügen Sie Subnetze zu Ihren Virtual Private Cloud (VPC) -Umgebungen hinzu und geben einen Outpost als Standort für die Subnetze an. Anschließend wählen Sie das gewünschte Subnetz aus, wenn Sie unterstützte AWS Ressourcen über die Tools CLI AWS Management Console APIs, CDK oder Infrastructure as Code (IaC) bereitstellen. Instances in Outpost-Subnetzen kommunizieren über VPC-Netzwerke mit anderen Instances im Outpost oder in der Region.

Der Outpost Service Link überträgt sowohl Outpost-Verwaltungsverkehr als auch Kunden-VPC-Verkehr (VPC-Verkehr zwischen den Subnetzen im Outpost und den Subnetzen in der Region).

Wichtige Begriffe:

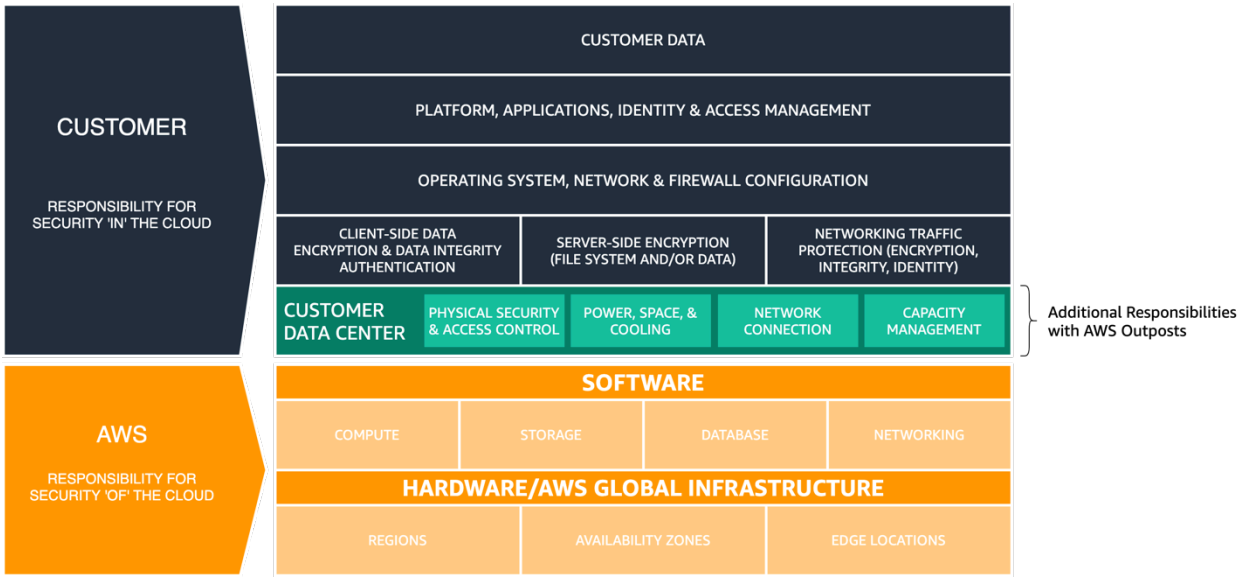
- AWS Outposts— ist ein vollständig verwalteter Service, der dieselbe AWS Infrastruktur, dieselben AWS Dienste und Tools für praktisch jedes Rechenzentrum APIs, jeden Colocation-Bereich oder jede lokale Einrichtung bietet und so für ein wirklich konsistentes Hybrid-Erlebnis sorgt.
- Outpost — ist eine Bereitstellung eines oder mehrerer physisch miteinander verbundener AWS Outposts Racks, die als eine einzige logische Einheit verwaltet werden, und ein Pool aus Rechen-, Speicher- und AWS Netzwerkressourcen werden am Standort eines Kunden bereitgestellt.
- Übergeordnete Region — die Region AWS-Region , die die Verwaltung, die Dienste auf der Kontrollebene und die regionalen AWS Dienste für eine Outpost-Installation bereitstellt.
- Anchor Availability Zone (Anker AZ) — Die Availability Zone in der übergeordneten Region, in der sich die Ankerpunkte für einen Außenposten befinden. Ein Außenposten fungiert als Erweiterung seines Anker-AZ. Der Anker AZ wird vom Kunden bei der Bestellung von Outposts ausgewählt. Nachdem ein Anker-AZ ausgewählt wurde, kann dieser für die Dauer der AWS Outposts Abonnementlaufzeit nicht mehr geändert werden.

- Ankerpunkte — Endpunkte in der Anker-AZ, die die Verbindungen von remote bereitgestellten Outposts empfangen.
- Service Link — eine Reihe verschlüsselter VPN-Tunnel, die einen Außenposten mit seiner zentralen Availability Zone in der übergeordneten Region verbinden.
- Local Gateway (LGW) — Ein virtueller Router mit logischer Verbindung, der die Kommunikation zwischen Ihrem Outpost und Ihrem lokalen Netzwerk ermöglicht.

Das Modell der geteilten Verantwortung verstehen AWS Outposts

Wenn Sie AWS Outposts Infrastruktur in Ihren Rechenzentren oder Colocation-Einrichtungen bereitstellen, übernehmen Sie im Modell der AWS gemeinsamen Verantwortung zusätzliche Aufgaben. AWS Bietet in der Region beispielsweise verschiedene Stromquellen, redundante Kernnetzwerke und robuste WAN-Konnektivität (Wide Area Network), um sicherzustellen, dass Dienste auch bei Ausfällen einer oder mehrerer Komponenten verfügbar sind.

Bei Outposts sind Sie dafür verantwortlich, die Outpost-Racks mit stabiler Stromversorgung und Netzwerkkonnektivität zu versorgen, um Ihre Verfügbarkeitsanforderungen für Workloads zu erfüllen, die auf Outposts ausgeführt werden.



AWS Das Modell der geteilten Verantwortung wurde aktualisiert für AWS Outposts

Mit AWS Outposts sind Sie für die physische Sicherheit und die Zugriffskontrollen der Rechenzentrumsumgebung verantwortlich. Sie müssen ausreichend Strom, Platz und Kühlung bereitstellen, damit der Outpost betriebsbereit bleibt und Netzwerkverbindungen bestehen, um den Outpost wieder mit der Region zu verbinden.

Da die Kapazität von Outpost begrenzt ist und durch die Größe und Anzahl der AWS Rack-Installationen an Ihrem Standort bestimmt wird, müssen Sie entscheiden, wie viel EC2 EBS- und S3-On-Outpost-Kapazität Sie benötigen, um Ihre ersten Workloads auszuführen, future Wachstum zu bewältigen und zusätzliche Kapazität bereitzustellen, um Serverausfälle und Wartungsereignisse zu minimieren.

AWS ist verantwortlich für die Verfügbarkeit der Outposts-Infrastruktur, einschließlich der Stromversorgungen, Server und Netzwerkgeräte in den AWS Outposts Racks. AWS verwaltet auch den Virtualisierungshypervisor, die Speichersysteme und die AWS Dienste, die auf Outposts ausgeführt werden.

Ein zentrales Stromregal in jedem Outposts-Rack wandelt Wechselstrom in Gleichstrom um und versorgt die Server im Rack über eine Sammelschienenarchitektur mit Strom. Bei der Busbar-Architektur kann die Hälfte der Stromversorgungen im Rack ausfallen und alle Server laufen ohne Unterbrechung weiter.

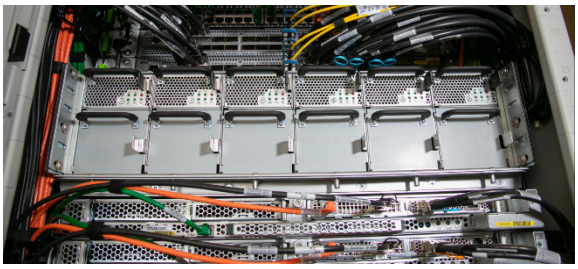


Abbildung 3: AWS Outposts AC-to-DC Stromversorgungen und Stromverteilung über Sammelschienen

Die Netzwerk-Switches und die Verkabelung innerhalb und zwischen den Outposts-Racks sind ebenfalls vollständig redundant. Ein Glasfaser-Patchpanel sorgt für Konnektivität zwischen einem Outpost-Rack und dem lokalen Netzwerk und dient als Abgrenzungspunkt zwischen der vom Kunden verwalteten Rechenzentrumsumgebung und der verwalteten Umgebung. AWS Outposts

AWS Ist genau wie in der Region für die auf Outposts angebotenen Cloud-Dienste verantwortlich und übernimmt zusätzliche Aufgaben, wenn Sie übergeordnete Managed Services wie Amazon RDS auf Outposts auswählen und bereitstellen. Sie sollten das Modell der AWS gemeinsamen Verantwortung und die Seiten mit den häufig gestellten Fragen (FAQ) für einzelne Dienste überprüfen, wenn Sie die Dienste für Outposts in Betracht ziehen und auswählen. Diese Ressourcen bieten zusätzliche Informationen zur Aufteilung der Zuständigkeiten zwischen Ihnen und AWS.

In Bezug auf Fehlermodi denken

Beim Entwerfen einer Anwendung oder eines Systems mit hoher Verfügbarkeit müssen Sie berücksichtigen, welche Komponenten ausfallen könnten, welche Auswirkungen Komponentenausfälle auf das System haben und welche RPO-/RTO-Ziele Sie für Ihre Anwendung verfolgen und welche Mechanismen Sie implementieren können, um die Auswirkungen von Komponentenausfällen zu mindern oder zu beseitigen. Wird Ihre Anwendung auf einem einzelnen Server, in einem einzigen Rack oder in einem einzigen Rechenzentrum ausgeführt? Was passiert, wenn ein Server, ein Rack oder ein Rechenzentrum vorübergehend oder dauerhaft ausfällt? Was passiert, wenn ein kritisches Subsystem wie das Netzwerk oder die Anwendung selbst ausfällt? Dies sind Fehlermodi.

Sie sollten die Fehlermodi in diesem Abschnitt bei der Planung Ihrer Outposts und Anwendungsbereitstellungen berücksichtigen. In den folgenden Abschnitten wird untersucht, wie Sie diese Fehlermodi minimieren können, um eine höhere Hochverfügbarkeit für Ihre Anwendungsumgebung zu erreichen.

Fehlermodus 1: Netzwerk

Eine Outpost-Bereitstellung ist für Verwaltung und Überwachung auf eine stabile Verbindung zur übergeordneten Region angewiesen. Netzwerkunterbrechungen können durch eine Vielzahl von Ausfällen wie Bedienungsfehler, Geräteausfälle und Ausfälle von Dienstanbietern verursacht werden. Ein Außenposten, der aus einem oder mehreren am Standort miteinander verbundenen Racks bestehen kann, gilt als unterbrochen, wenn er nicht über den Service Link mit der Region kommunizieren kann.

Redundante Netzwerkpfade können dazu beitragen, das Risiko von Unterbrechungen zu verringern. Sie sollten die Anwendungsabhängigkeiten und den Netzwerkverkehr zuordnen, um zu verstehen, welche Auswirkungen Unterbrechungen auf Workload-Operationen haben können. Planen Sie eine ausreichende Netzwerkredundanz ein, um Ihre Anforderungen an die Anwendungsverfügbarkeit zu erfüllen.

Während eines Verbindungsabbruchs laufen die auf einem Outpost laufenden Instanzen weiter und sind von lokalen Netzwerken aus über das Outpost Local Gateway (LGW) zugänglich. Lokale Workloads und Dienste können beeinträchtigt werden oder ausfallen, wenn sie auf Dienste in der Region angewiesen sind. Mutationsanfragen (wie das Starten oder Stoppen von Instances auf dem Outpost), der Betrieb der Kontrollebene und die Service-Telemetrie (z. B. CloudWatch Metriken)

schlagen fehl, solange der Outpost von der Region getrennt ist. CloudWatch Metriken werden für kurze Zeiträume einer Netzwerkunterbrechung lokal auf Ihrem Outpost gespoolt und zur Überprüfung an die Region gesendet, wenn die Service Link-Verbindung wieder hergestellt ist.

Fehlermodus 2: Instanzen

EC2 Amazon-Instances können beeinträchtigt werden oder ausfallen, wenn der Server, auf dem sie ausgeführt werden, ein Problem hat oder wenn bei der Instance ein Betriebssystem oder eine Anwendung ausfällt. Wie Anwendungen mit solchen Fehlern umgehen, hängt von der Anwendungsarchitektur ab. Monolithische Anwendungen verwenden in der Regel Anwendungs- oder Systemfunktionen für die Wiederherstellung, während modulare serviceorientierte Architekturen oder Microservice-Architekturen in der Regel ausgefallene Komponenten ersetzen, um die Serviceverfügbarkeit aufrechtzuerhalten.

Mithilfe automatisierter Mechanismen wie Amazon EC2 Auto Scaling Scaling-Gruppen können Sie ausgefallene Instances durch neue Instances ersetzen. Die auto Instanzwiederherstellung kann Instanzen neu starten, die aufgrund von Serverausfällen ausfallen, sofern auf den verbleibenden Servern genügend freie Kapazität verfügbar ist und der Service Link weiterhin verbunden ist.

Fehlermodus 3: Compute

Server können ausfallen oder beeinträchtigt werden und müssen möglicherweise aus einer Vielzahl von Gründen außer Betrieb genommen werden (vorübergehend oder dauerhaft), z. B. aufgrund von Komponentenausfällen und geplanten Wartungsarbeiten. Wie die Dienste im Outposts-Rack mit Serverausfällen und -beeinträchtigungen umgehen, ist unterschiedlich und kann davon abhängen, wie Kunden Hochverfügbarkeitsoptionen konfigurieren.

Sie sollten ausreichend Rechenkapazität bestellen, um ein `N+M` Verfügbarkeitsmodell zu unterstützen, bei dem `N` die erforderliche Kapazität und die `M` Reservekapazität für Serverausfälle bereitgestellt werden.

Hardwareersatz für ausgefallene Server wird im Rahmen des vollständig verwalteten AWS Outposts Rack-Service bereitgestellt. AWS überwacht aktiv den Zustand aller Server und Netzwerkgeräte in einer Outpost-Bereitstellung. Wenn physische Wartungsarbeiten erforderlich sind, vereinbaren AWS wir einen Termin für einen Besuch vor Ort, um ausgefallene Komponenten auszutauschen. Durch die Bereitstellung von Reservekapazitäten können Sie Ihre Workloads vor Hostausfällen schützen, während fehlerhafte Server außer Betrieb genommen und ersetzt werden.

Fehlermodus 4: Racks oder Rechenzentren

Rackausfälle können aufgrund eines Totalausfalls der Stromversorgung der Racks oder aufgrund von Umwelteinflüssen wie Kühlungsausfällen oder physischen Schäden am Rechenzentrum durch Überschwemmungen oder Erdbeben auftreten. Mängel in der Architektur der Stromverteilung in Rechenzentren oder Fehler bei der standardmäßigen Wartung der Stromversorgung von Rechenzentren können dazu führen, dass ein oder mehrere Racks oder sogar das gesamte Rechenzentrum nicht mit Strom versorgt werden.

Diese Szenarien können durch die Bereitstellung von Infrastruktur auf mehreren Stockwerken oder voneinander unabhängigen Standorten im Rechenzentrum auf demselben Campus oder in derselben Metropolregion abgemildert werden.

Wenn Sie diesen Ansatz mit AWS Outposts Rack verfolgen, müssen Sie sorgfältig abwägen, wie Anwendungen so konzipiert und verteilt werden, dass sie auf mehrere separate logische Outposts laufen, um die Anwendungsverfügbarkeit aufrechtzuerhalten.

Fehlermodus 5: AWS Availability Zone oder Region

Jeder Außenposten ist in einer bestimmten Availability Zone (AZ) innerhalb eines verankert. AWS-Region Ausfälle innerhalb der Basis-AZ oder der übergeordneten Region können zum Verlust des Outpost-Managements und der Veränderbarkeit führen und die Netzwerkkommunikation zwischen dem Outpost und der Region stören.

Ähnlich wie bei Netzwerkausfällen können Ausfälle in AZ oder Region dazu führen, dass der Außenposten von der Region getrennt wird. Die auf einem Outpost laufenden Instances laufen weiter und sind von lokalen Netzwerken aus über das Outpost Local Gateway (LGW) zugänglich. Sie können beeinträchtigt werden oder ausfallen, wenn sie, wie zuvor beschrieben, auf Dienste in der Region angewiesen sind.

Um die Auswirkungen von Ausfällen in AWS AZ und Region zu mildern, können Sie mehrere Outposts einsetzen, die jeweils in einer anderen AZ oder Region verankert sind. Anschließend können Sie Ihren Workload so gestalten, dass er in einem verteilten Bereitstellungsmodell mit mehreren Außenstellen ausgeführt wird. Dabei können Sie viele der ähnlichen Mechanismen und Architekturmuster verwenden, die Sie heute für die Planung und Bereitstellung verwenden. AWS

Die Kontrollebene der Dienste, auf denen sie ausgeführt werden, AWS Outposts befindet sich in der Region, in der sie verankert sind, wodurch eine Abhängigkeit sowohl von zonalen Diensten

wie Amazon EC2 und Amazon EBS als auch von regionalen Diensten wie Amazon RDS, Elastic Load Balancing und Amazon EKS entsteht. In Outposts können Anwendungen im Rahmen des Konzepts der statischen Stabilität eingesetzt werden, um die Widerstandsfähigkeit gegenüber Beeinträchtigungen durch Kontrollebenen zu verbessern.

Aufbau von HA-Anwendungen und Infrastrukturlösungen mit AWS Outposts Rack

Mit AWS Outposts Rack können Sie hochverfügbare lokale Anwendungen mit vertrauten AWS Cloud-Diensten und -Tools erstellen, verwalten und skalieren. Es ist wichtig zu verstehen, dass sich Cloud-HA-Architekturen und -Ansätze im Allgemeinen von herkömmlichen lokalen HA-Architekturen unterscheiden, die Sie heute möglicherweise in Ihrem Rechenzentrum ausführen.

Bei herkömmlichen lokalen HA-Anwendungsbereitstellungen werden Anwendungen in virtuellen Maschinen () bereitgestellt. VMs Komplexe IT-Systeme und Infrastrukturen werden bereitgestellt und gewartet, um den Betrieb und die Funktionsfähigkeit dieser virtuellen Maschinen aufrechtzuerhalten. Sie haben VMs oft spezifische Identitäten, und jede VM kann eine entscheidende Rolle in der gesamten Anwendungsarchitektur spielen.

Architektonische Rollen sind eng mit VM-Identitäten verknüpft. Systemarchitekten nutzen die Funktionen der IT-Infrastruktur, um hochverfügbare VM-Laufzeitumgebungen bereitzustellen, die jeder VM zuverlässigen Zugriff auf Rechenkapazität, Speichervolumen und Netzwerkdienste bieten. Wenn eine VM ausfällt, werden automatisierte oder manuelle Wiederherstellungsprozesse ausgeführt, um die ausgefallene VM wieder in einen fehlerfreien Zustand zu versetzen, häufig auf einer anderen Infrastruktur oder in einem komplett anderen Rechenzentrum.

Cloud-HA-Architekturen verfolgen einen anderen Ansatz. AWS Cloud-Dienste bieten zuverlässige Rechen-, Speicher- und Netzwerkfunktionen. Anwendungskomponenten werden in EC2 Instanzen, Containern, serverlosen Funktionen oder anderen verwalteten Diensten bereitgestellt.

Eine Instanz ist eine Instanziierung einer Anwendungskomponente — vielleicht eine von vielen, die diese Rolle übernehmen. Anwendungskomponenten sind lose miteinander und mit der Rolle, die sie in der gesamten Anwendungsarchitektur spielen, verknüpft. Die individuelle Identität einer Instanz ist im Allgemeinen nicht wichtig. Zusätzliche Instanzen können erstellt oder gelöscht werden, um je nach Bedarf nach oben oder unten zu skalieren. Fehlgeschlagene oder fehlerhafte Instances werden einfach durch neue fehlerfreie Instances ersetzt.

AWS Outposts Rack ist ein vollständig verwalteter Service, der AWS Rechen-, Speicher-, Netzwerk-, Datenbank- und andere Cloud-Dienste auf lokale Standorte ausdehnt und so für ein wirklich konsistentes Hybrid-Erlebnis sorgt. Sie sollten den Outposts-Rack-Service nicht als direkten Ersatz für IT-Infrastruktursysteme mit herkömmlichen lokalen HA-Mechanismen betrachten. Der Versuch,

AWS Services und Outposts zur Unterstützung einer traditionellen lokalen HA-Architektur zu verwenden, ist ein Anti-Pattern.

Workloads, die auf einem AWS Outposts Rack ausgeführt werden, verwenden Cloud-HA-Mechanismen wie Amazon EC2 Auto Scaling (zur horizontalen Skalierung, um Workload-Anforderungen gerecht zu werden), EC2 Integritätsprüfungen (um fehlerhafte Instances zu erkennen und zu entfernen) und Application Load Balancers (um eingehenden Workload-Verkehr auf skalierte oder ersetzte Instances umzuleiten). Bei der Migration von Anwendungen in die Cloud, sei es in ein AWS Outposts Rack AWS-Region oder ein Rack, sollten Sie Ihre HA-Anwendungsarchitektur aktualisieren, um die Vorteile von verwalteten Cloud-Services und Cloud-HA-Mechanismen nutzen zu können.

In den folgenden Abschnitten werden Architekturmuster, Anti-Patterns und empfohlene Verfahren für die Bereitstellung von AWS Outposts Rack in Ihren lokalen Umgebungen zur Ausführung von Workloads mit Hochverfügbarkeitsanforderungen vorgestellt. In diesen Abschnitten werden Muster und Verfahren vorgestellt, sie enthalten jedoch keine Einzelheiten zur Konfiguration und Implementierung. Sie sollten das AWS Outposts Rack FAQs und das Benutzerhandbuch sowie die Servicedokumentation für die Dienste, die auf dem Outposts-Rack ausgeführt werden, lesen FAQs und sich mit ihnen vertraut machen, wenn Sie Ihre Umgebung für das Outposts-Rack und Ihre Anwendungen für die Migration zu AWS Services vorbereiten.

Themen

Netzwerk

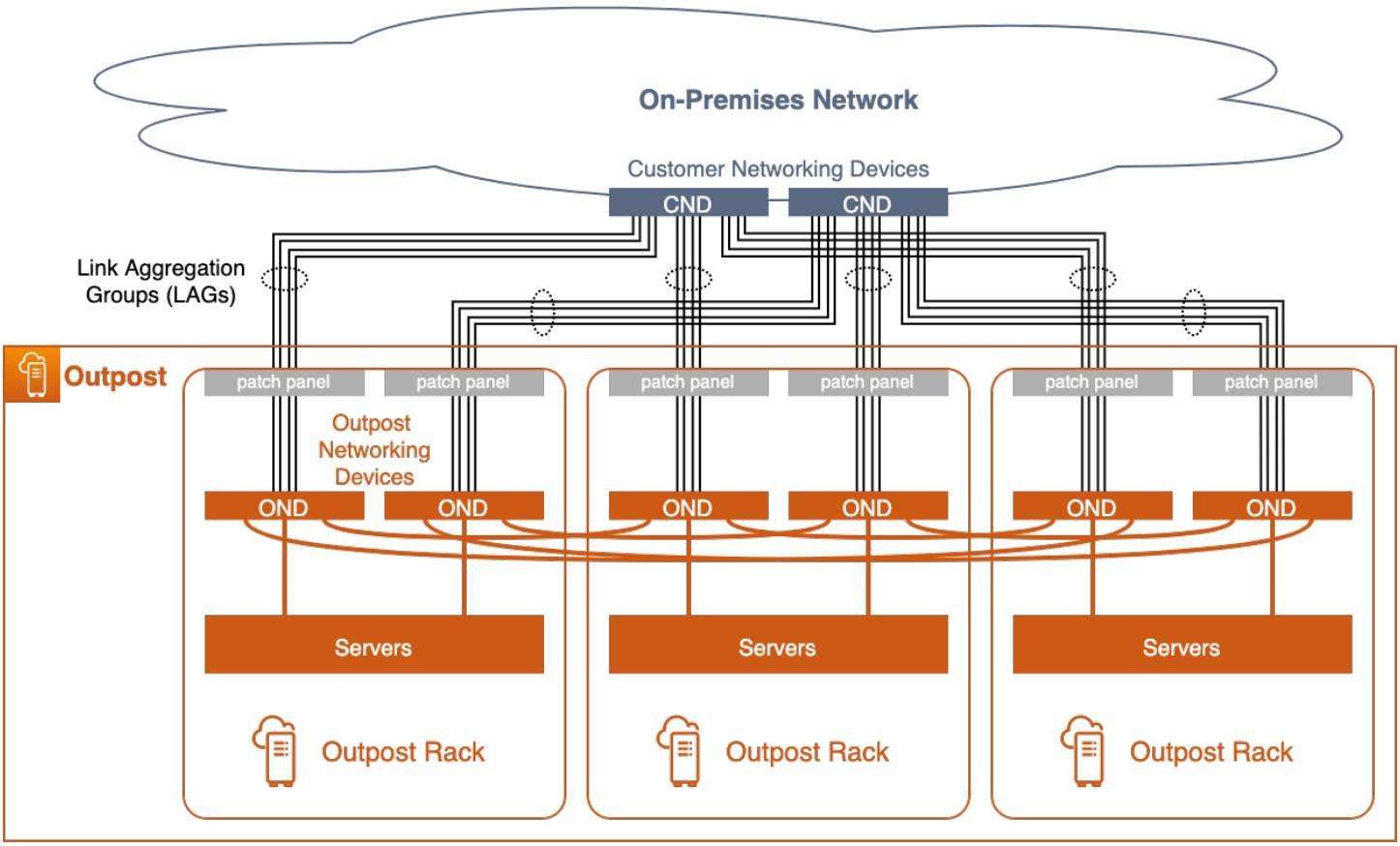
Eine Outpost-Bereitstellung hängt von einer stabilen Verbindung zu ihrem zentralen AZ ab, damit Verwaltung, Überwachung und Servicebetriebe ordnungsgemäß funktionieren. Sie sollten Ihr lokales Netzwerk so einrichten, dass redundante Netzwerkverbindungen für jedes Outpost-Rack und eine zuverlässige Konnektivität zu den Ankerpunkten in der Cloud bereitgestellt werden. AWS Berücksichtigen Sie auch die Netzwerkpfade zwischen den Anwendungs-Workloads, die auf

dem Outpost ausgeführt werden, und den anderen lokalen und Cloud-Systemen, mit denen sie kommunizieren. Wie werden Sie diesen Datenverkehr in Ihrem Netzwerk weiterleiten?

Themen

Netzwerkanschluss

Jedes AWS Outposts Rack ist mit redundanten top-of-rack Switches konfiguriert, die als Outpost Networking Devices () ONDs bezeichnet werden. Die Rechen- und Speicherserver in jedem Rack sind mit beiden ONDs verbunden. Sie sollten jedes OND mit einem separaten Switch, einem sogenannten Customer Networking Device (CND), in Ihrem Rechenzentrum verbinden, um verschiedene physische und logische Pfade für jedes Outpost-Rack bereitzustellen. ONDs Stellen Sie mithilfe von Glasfaserkabeln und optischen Transceivern eine Verbindung zu Ihrem CNDs über eine oder mehrere physische Verbindungen her. Die physischen Verbindungen sind in LAG-Links (Logical Link Aggregation Group) konfiguriert.



Outpost mit mehreren Racks und redundanten Netzwerkanhängen

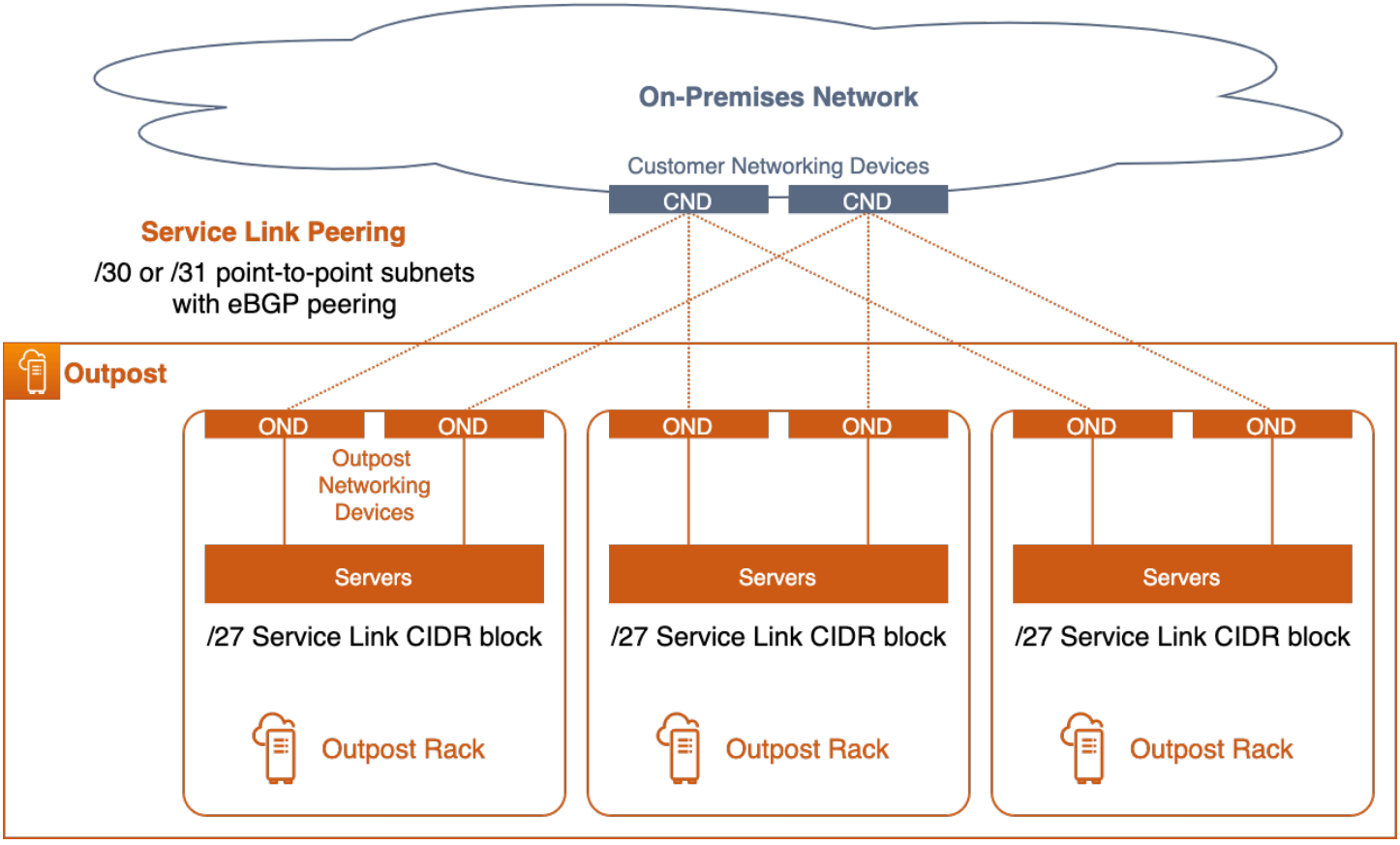
Die OND-zu-CND-Verbindungen werden immer in einer LAG konfiguriert — auch wenn es sich bei der physischen Verbindung um ein einzelnes Glasfaserkabel handelt. Wenn Sie die Links als LAG-Gruppen konfigurieren, können Sie die Verbindungsbandbreite erhöhen, indem Sie der logischen Gruppe zusätzliche physische Verbindungen hinzufügen. Die LAG-Verbindungen sind als IEEE 802.1q-Ethernet-Trunks konfiguriert, um getrennte Netzwerke zwischen dem Outpost und dem lokalen Netzwerk zu ermöglichen.

Jeder Outpost verfügt über mindestens zwei logisch getrennte Netzwerke, die mit dem Kundennetzwerk oder über das Kundennetzwerk kommunizieren müssen:

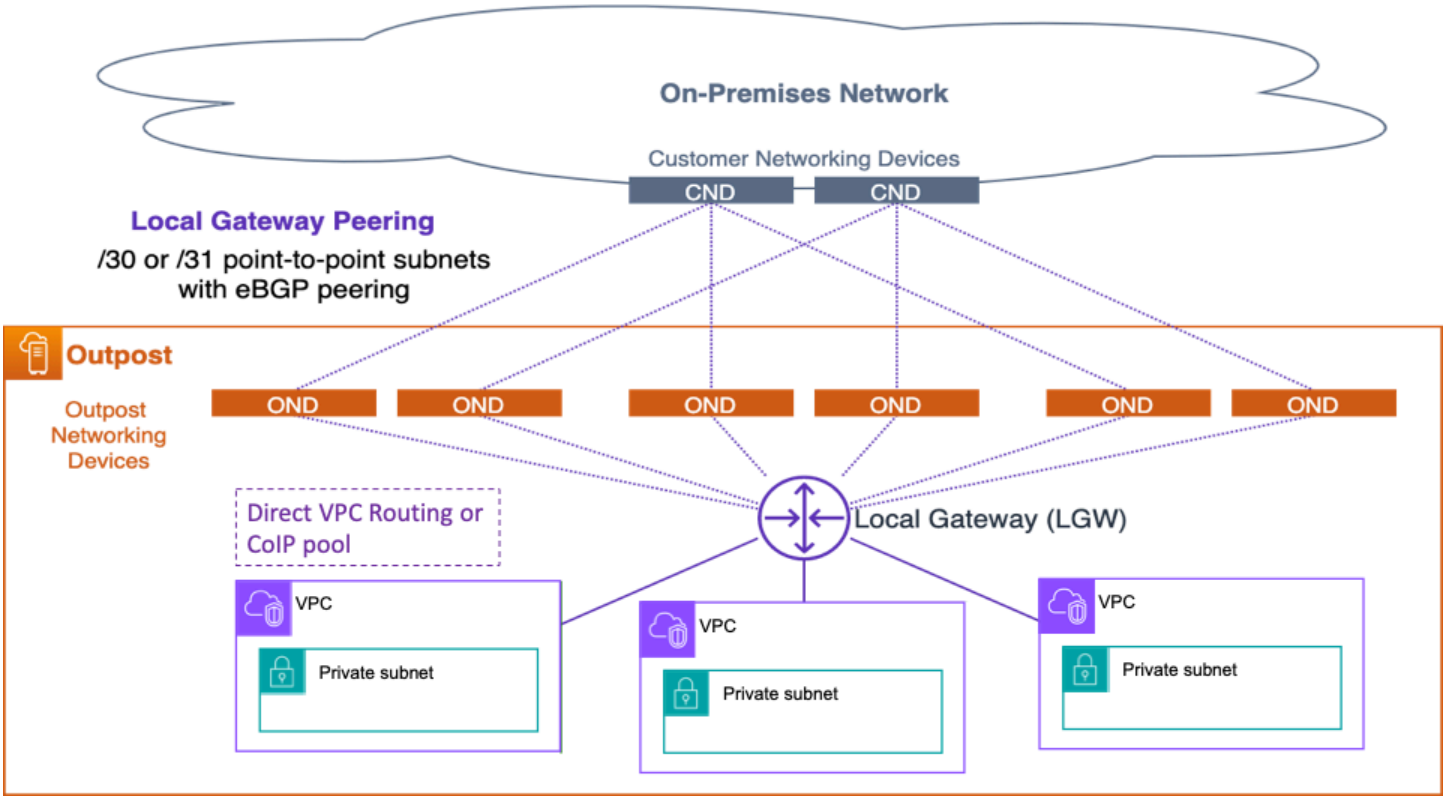
- Service Link-Netzwerk — weist den Outpost-Servern die Service-Link-IP-Adressen zu und erleichtert die Kommunikation mit dem lokalen Netzwerk, sodass sich die Server wieder mit den Outpost-Ankerpunkten in der Region verbinden können. Wenn Sie mehrere Rack-Implementierungen in einem einzigen logischen Outposts haben, müssen Sie jedem Rack einen Service Link /26 CIDR zuweisen.

- Lokales Gateway-Netzwerk — ermöglicht die Kommunikation zwischen den VPC-Subnetzen auf dem Outpost und dem lokalen Netzwerk über das Outpost Local Gateway (LGW).

Diese getrennten Netzwerke sind über eine Reihe von IP-Verbindungen über die LAG-Links mit dem lokalen Netzwerk verbunden. point-to-point Jeder OND-zu-CND-LAG-Link ist mit VLAN IDs, point-to-point (/30 oder /31) IP-Subnetzen und eBGP-Peering für jedes getrennte Netzwerk (Service Link und LGW) konfiguriert. Sie sollten die LAG-Links mit ihren point-to-point VLANs und Subnetzen als segmentierte Layer-2-Verbindungen mit Routing betrachten. Die gerouteten IP-Verbindungen bieten redundante logische Pfade, die die Kommunikation zwischen den getrennten Netzwerken im Outpost und dem lokalen Netzwerk erleichtern.



Service-Link-Peering



Lokales Gateway-Peering

Sie sollten die Layer-2-LAG-Links (und ihre VLANs) auf den direkt angeschlossenen CND-Switches beenden und die IP-Schnittstellen und das BGP-Peering auf den CND-Switches konfigurieren. Sie sollten die LAG VLANs zwischen Ihren Switches im Rechenzentrum nicht überbrücken. Weitere Informationen finden Sie unter Konnektivität auf Netzwerkebene im AWS Outposts Benutzerhandbuch.

In einem logischen Outpost mit mehreren Racks ONDs sind sie redundant miteinander verbunden, um eine hochverfügbare Netzwerkkonnektivität zwischen den Racks und den Workloads auf den Servern zu gewährleisten. AWS ist für die Netzwerkverfügbarkeit innerhalb des Outpost verantwortlich.

Empfohlene Vorgehensweisen für hochverfügbare Netzwerkanschlüsse ohne ACE

- Connect jedes Outpost Networking Device (OND) in einem Outpost-Rack mit einem separaten Customer Networking Device (CND) im Rechenzentrum.
- Trennen Sie die Layer-2-Links VLANs, Layer-3-IP-Subnetze und das BGP-Peering auf den direkt angeschlossenen Customer Networking Device (CND) -Switches. Stellen Sie keine Brücke

zwischen OND und CND zwischen dem lokalen Netzwerk oder zwischen dem lokalen Netzwerk her VLANs . CNDs

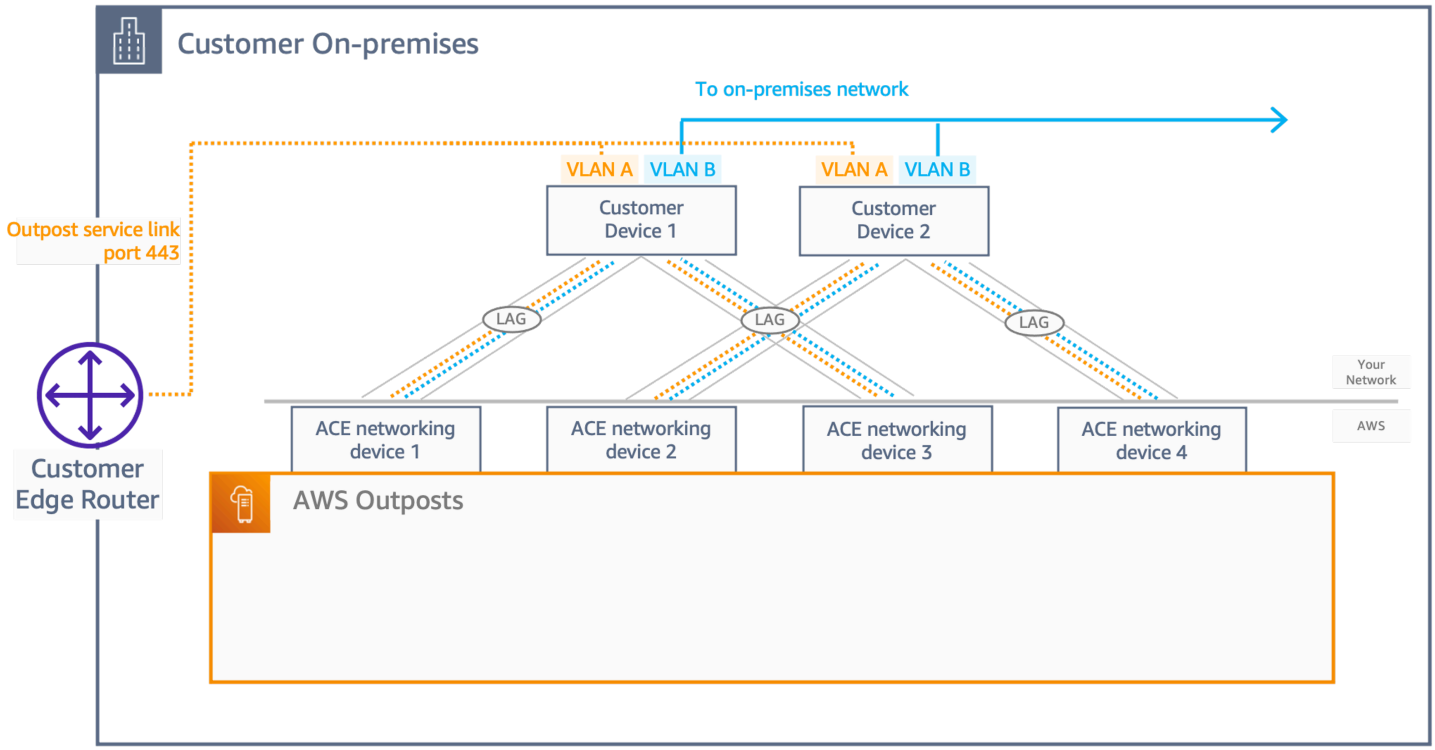
- Fügen Sie Links zu den Link Aggregation Groups (LAGs) hinzu, um die verfügbare Bandbreite zwischen dem Outpost und dem Rechenzentrum zu erhöhen. Verlassen Sie sich nicht auf die Gesamtbandbreite der verschiedenen Pfade durch beide. ONDs
- Nutzen Sie die verschiedenen Pfade durch die Redundanz ONDs , um eine stabile Konnektivität zwischen den Outpost-Netzwerken und dem lokalen Netzwerk zu gewährleisten.
- Um eine optimale Redundanz zu erreichen und eine unterbrechungsfreie OND-Wartung zu ermöglichen, empfehlen wir Kunden, BGP-Werbung und -Richtlinien wie folgt zu konfigurieren:
  - Die Netzwerkausrüstung des Kunden sollte BGP-Werbung von Outpost erhalten, ohne die BGP-Attribute zu ändern, und BGP aktivieren, falls eine Wartung erforderlich ist. multipath/load-balancing to achieve optimal inbound traffic flows (from customer towards Outpost). AS-Path prepending is used for Outpost BGP prefixes to shift traffic away from a particular OND/uplink Das Kundennetzwerk sollte Routen von Outpost mit AS-Path-Länge 1 gegenüber Routen mit AS-Path-Länge 4 bevorzugen, d. h. auf AS-Path-Prepending reagieren.
  - Das Kundennetzwerk sollte in Outpost für gleiche BGP-Präfixe mit denselben Attributen werben. ONDs Standardmäßig verteilt das Outpost-Netzwerk den ausgehenden Datenverkehr (zum Kunden hin) auf alle Uplinks. Routing-Richtlinien werden auf der Outpost-Seite verwendet, um den Datenverkehr von einem bestimmten OND wegzuleiten, falls Wartungsarbeiten erforderlich sind. Für diese Verkehrsverlagerung und für die unterbrechungsfreie Durchführung von Wartungsarbeiten ONDs sind auf allen Seiten gleiche BGP-Präfixe von Kundenseite erforderlich. Wenn das Netzwerk des Kunden gewartet werden muss, empfehlen wir die Verwendung von AS-Path Prepending, um den Datenverkehr vorübergehend von einem bestimmten Uplink oder Gerät abzuleiten.

Empfohlene Vorgehensweisen für hochverfügbare Netzwerkanschlüsse mit ACE

Für eine Multi-Rack-Bereitstellung mit vier oder mehr Computer-Racks müssen Sie das Aggregation, Core, Edge (ACE) -Rack verwenden, das als Netzwerkaggregationspunkt fungiert, um die Anzahl der Glasfaserverbindungen zu Ihren lokalen Netzwerkgeräten zu reduzieren. Das ACE-Rack stellt die Konnektivität zum Rack ONDs in jedem Outposts bereit und ist somit für AWS die Zuweisung und Konfiguration der VLAN-Schnittstelle zwischen den ONDs ACE-Netzwerkgeräten zuständig.

Isolierte Netzwerkschichten für Service Link- und Local Gateway-Netzwerke sind weiterhin erforderlich, unabhängig davon, ob ein ACE-Rack verwendet wird oder nicht, das auf VLAN-IP-Subnetze point-to-point (/30 oder /31) und eine eBGP-Peering-Konfiguration für jedes getrennte

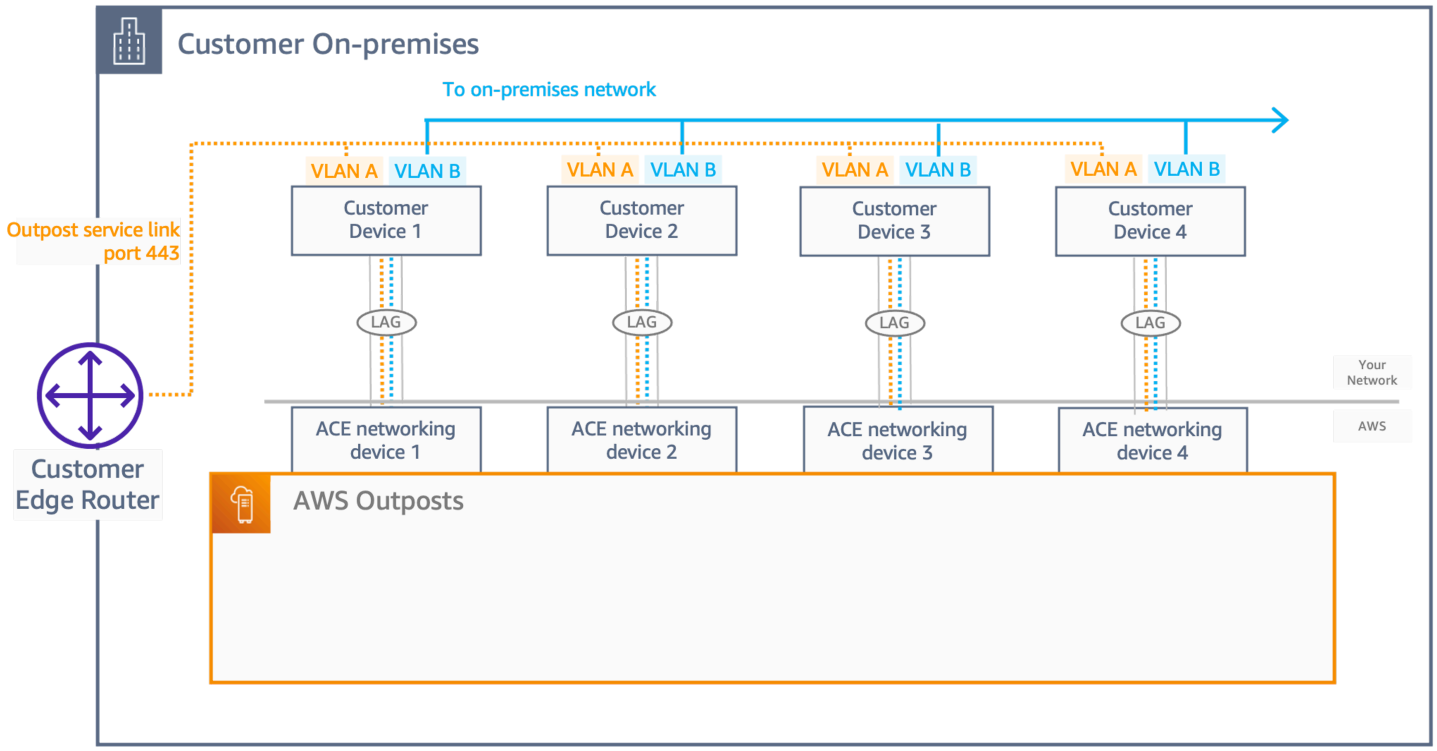
Netzwerk abzielt. Die vorgeschlagenen Architekturen sollten einer der beiden folgenden Architekturen folgen:



Netzwerkgeräte für zwei Kunden

- Bei dieser Architektur sollte der Kunde über zwei Netzwerkgeräte (CND) verfügen, um die ACE-Netzwerkgeräte miteinander zu verbinden und so Redundanz zu gewährleisten.
- Für jede physische Verbindung müssen Sie eine LAG aktivieren (um die verfügbare Bandbreite zwischen dem Outpost und dem Rechenzentrum zu erhöhen), auch wenn es sich um einen einzelnen physischen Port handelt. Dieser Port wird zwei Netzwerksegmente mit 2 point-to-point VLANs (/30 oder /31) und eBGP-Konfigurationen zwischen und übertragen. ACEs CNDs
- In einem stabilen Zustand erfolgt der Lastenausgleich nach dem to/from the customer network from the ACE layer, 25% traffic distribution across the ACE to customer. In order to allow this behavior, the eBGP peering's between ACEs and CNDs must have BGP multipath/load ECMP-Muster-Balancing (Equal-Cost Multipath), wobei der Lastenausgleich aktiviert ist und die Kundenpräfixe mit derselben BGP-Metrik auf den 4 eBGP-Peering-Verbindungen angekündigt werden.
- Um eine optimale Redundanz zu erreichen und eine unterbrechungsfreie OND-Wartung zu ermöglichen, empfehlen wir unseren Kunden, die folgenden Empfehlungen zu befolgen:
  - Das Netzwerkgerät des Kunden sollte für alle Geräte in Outpost gleiche BGP-Präfixe mit denselben Attributen bewerben. ONDs

- Das Netzwerkgerät des Kunden sollte BGP-Werbung von Outpost erhalten, ohne die BGP-Attribute zu ändern und um BGP-Multipath/Load-Balancing zu aktivieren.



Netzwerkgeräte für vier Kunden

Bei dieser Architektur verfügt der Kunde über vier Netzwerkgeräte (CND), um die ACE-Netzwerkgeräte miteinander zu verbinden, wodurch Redundanz und dieselbe Netzwerklogik, einschließlich eBGP und ECMP VLANs, wie sie für eine 2-CND-Architektur gelten, gewährleistet werden.

Anker-Konnektivität

Ein Outpost-Servicelink stellt eine Verbindung zu öffentlichen oder privaten Ankern (nicht zu beiden) in einer bestimmten Availability Zone (AZ) in der übergeordneten Region des Outposts her. Outpost-Server initiieren ausgehende Service Link-VPN-Verbindungen von ihren Service Link-IP-Adressen zu den Ankerpunkten in der Anker-AZ. Diese Verbindungen verwenden UDP- und TCP-Port 443. AWS ist verantwortlich für die Verfügbarkeit der Ankerpunkte in der Region.

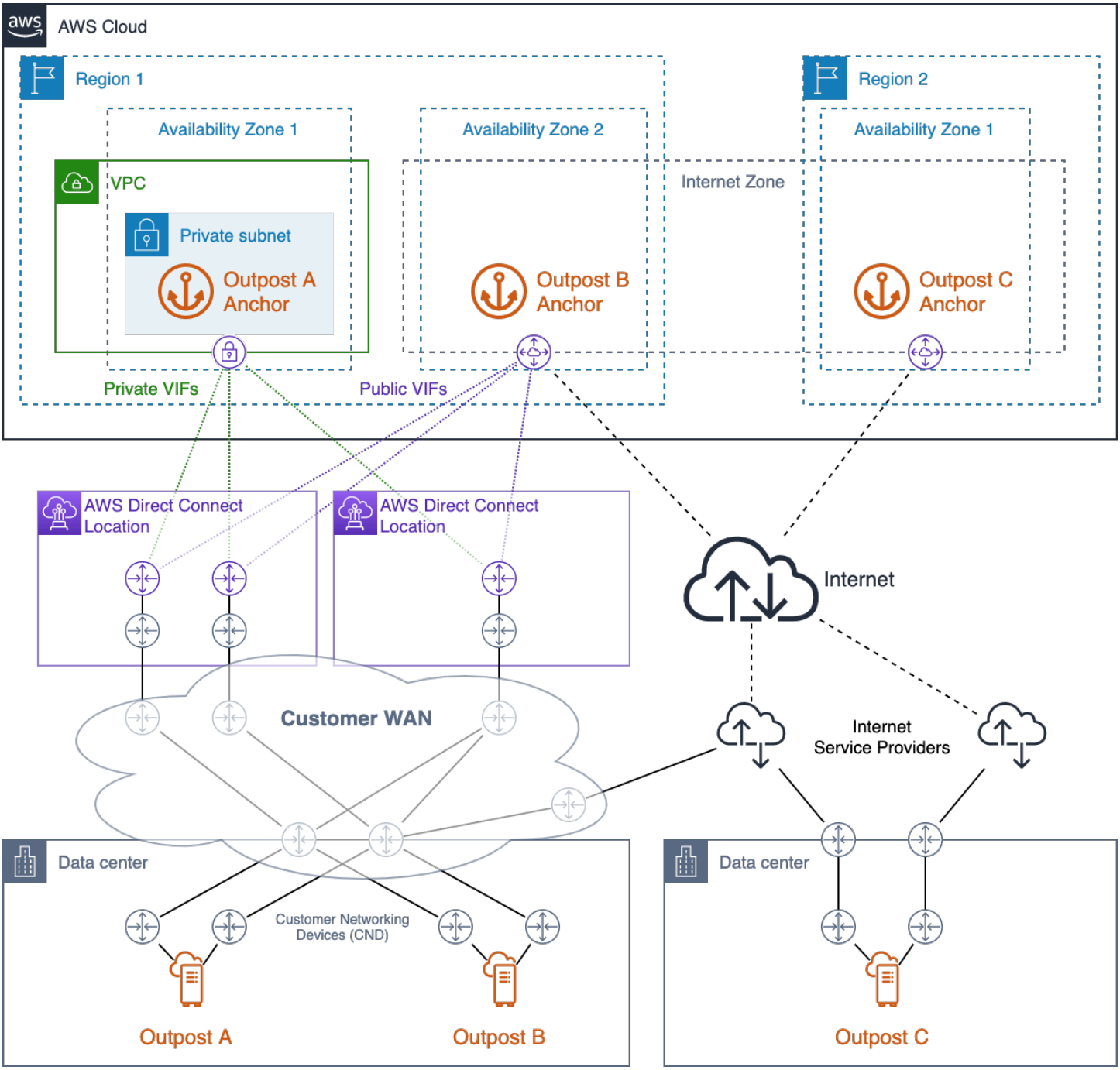
Sie müssen sicherstellen, dass die IP-Adressen der Outpost-Servicelinks über Ihr Netzwerk eine Verbindung zu den Ankerpunkten im Anker-AZ herstellen können. Die Service Link-IP-Adressen müssen nicht mit anderen Hosts in Ihrem lokalen Netzwerk kommunizieren.

Öffentliche Ankerpunkte befinden sich in den öffentlichen IP-Bereichen der Region (in den CIDR-Blöcken des EC2 Dienstes) und können über das Internet oder öffentliche virtuelle Schnittstellen AWS Direct Connect(DX) aufgerufen werden (). VIFs Die Verwendung öffentlicher Ankerpunkte ermöglicht eine flexiblere Pfadauswahl, da der Service Link-Verkehr über jeden verfügbaren Pfad geleitet werden kann, der die Ankerpunkte im öffentlichen Internet erfolgreich erreichen kann.

Private Ankerpunkte ermöglichen es Ihnen, Ihre IP-Adressbereiche für die Ankerkonnektivität zu verwenden. Private Ankerpunkte werden in einem privaten Subnetz innerhalb einer dedizierten VPC unter Verwendung von vom Kunden zugewiesenen IP-Adressen erstellt. Die VPC wird in dem Land erstellt AWS-Konto , dem die Outpost-Ressource gehört, und Sie sind dafür verantwortlich, dass die VPC verfügbar und ordnungsgemäß konfiguriert ist. Verwenden Sie eine Security Control Policy (SCP) in AWSOrigamiServiceGateway Organizations, um zu verhindern, dass Benutzer diese Virtual Private Cloud (VPC) löschen. Auf private Ankerpunkte muss über Direct Connect Private zugegriffen werden. VIFs

Sie sollten redundante Netzwerkpfade zwischen dem Outpost und den Ankerpunkten in der Region bereitstellen, wobei die Verbindungen auf separaten Geräten an mehr als einem Standort enden. Dynamisches Routing sollte so konfiguriert werden, dass der Verkehr automatisch auf alternative Pfade umgeleitet wird, wenn Verbindungen oder Netzwerkgeräte ausfallen. Sie sollten ausreichend Netzwerkkapazität bereitstellen, um sicherzustellen, dass der Ausfall eines WAN-Pfads die verbleibenden Pfade nicht überlastet.

Das folgende Diagramm zeigt drei Outposts mit redundanten Netzwerkpfaden zu ihrem Anker, die AZs über AWS Direct Connect öffentliche Internetverbindungen verfügen. Outpost A und Outpost B sind in verschiedenen Availability Zones in derselben Region verankert. Außenposten A ist mit privaten Ankerpunkten in AZ 1 der Region 1 verbunden. Außenposten B ist mit öffentlichen Ankerpunkten in AZ 2 der Region 1 verbunden. Außenposten C ist mit öffentlichen Ankern in AZ 1 der Region 2 verbunden.



Hochverfügbare Ankerkonnektivität mit AWS Direct Connect öffentlichem Internetzugang

Outpost A verfügt über drei redundante Netzwerkpfade, um seinen privaten Ankerpunkt zu erreichen. Zwei Pfade sind über redundante Direct Connect-Schaltungen an einem einzigen Direct Connect-Standort verfügbar. Der dritte Pfad ist über einen Direct Connect-Stromkreis an einem zweiten Direct Connect-Standort verfügbar. Dieses Design hält den Service Link-Verkehr von Outpost A in privaten

Netzwerken aufrecht und bietet Pfadredundanz, die den Ausfall eines der Direct Connect-Leitungen oder eines gesamten Direct Connect-Standorts ermöglicht.

Outpost B verfügt über vier redundante Netzwerkpfade, um seinen öffentlichen Ankerpunkt zu erreichen. Drei Pfade sind öffentlich verfügbar, die auf den von Outpost A genutzten Direct Connect-Leitungen und Standorten VIFs bereitgestellt werden. Der vierte Pfad ist über das Kunden-WAN und das öffentliche Internet verfügbar. Der Service Link-Verkehr von Outpost B kann über jeden verfügbaren Pfad geleitet werden, der die Ankerpunkte im öffentlichen Internet erfolgreich erreichen kann. Die Verwendung der Direct Connect-Pfade kann für eine konsistentere Latenz und eine höhere Bandbreitenverfügbarkeit sorgen, während der öffentliche Internetpfad für Disaster Recovery (DR) oder Bandbreitenerweiterungen verwendet werden kann.

Outpost C verfügt über zwei redundante Netzwerkpfade, um seinen öffentlichen Ankerpunkt zu erreichen. Outpost C wird in einem anderen Rechenzentrum als Outpost A und B bereitgestellt. Das Rechenzentrum von Outpost C verfügt nicht über eigene Leitungen, die mit dem Kunden-WAN verbunden sind. Stattdessen verfügt das Rechenzentrum über redundante Internetverbindungen, die von zwei verschiedenen Internetdienstanbietern () bereitgestellt werden. ISPs Der Service Link-Verkehr von Outpost C kann über eines der ISP-Netzwerke geleitet werden, um die Ankerpunkte im öffentlichen Internet zu erreichen. Dieses Design ermöglicht Flexibilität bei der Weiterleitung des Service Link-Verkehrs über jede verfügbare öffentliche Internetverbindung. Der end-to-end Pfad hängt jedoch von öffentlichen Netzwerken von Drittanbietern ab, in denen Bandbreitenverfügbarkeit und Netzwerklatenz schwanken.

Der Netzwerkpfad zwischen einem Outpost und seinen Service Link-Ankerpunkten muss der folgenden Bandbreitenspezifikation entsprechen:

- 500 Mbit/s — 1 Gbit/s verfügbare Bandbreite pro Outpost-Rack (z. B. 3 Racks: 1,5 — 3 Gbit/s verfügbare Bandbreite)

Empfohlene Verfahren für hochverfügbare Anker-Konnektivität

- Stellen Sie redundante Netzwerkpfade zwischen jedem Außenposten und seinen Ankerpunkten in der Region bereit.
- Verwenden Sie Direct Connect (DX) -Pfade, um Latenz und Bandbreitenverfügbarkeit zu kontrollieren.
- Stellen Sie sicher, dass der TCP- und UDP-Port 443 von den Outpost Service Link CIDR-Blöcken zu den EC2 IP-Adressbereichen in der übergeordneten Region geöffnet ist (ausgehend). Stellen Sie sicher, dass die Ports auf allen Netzwerkpfaden geöffnet sind.

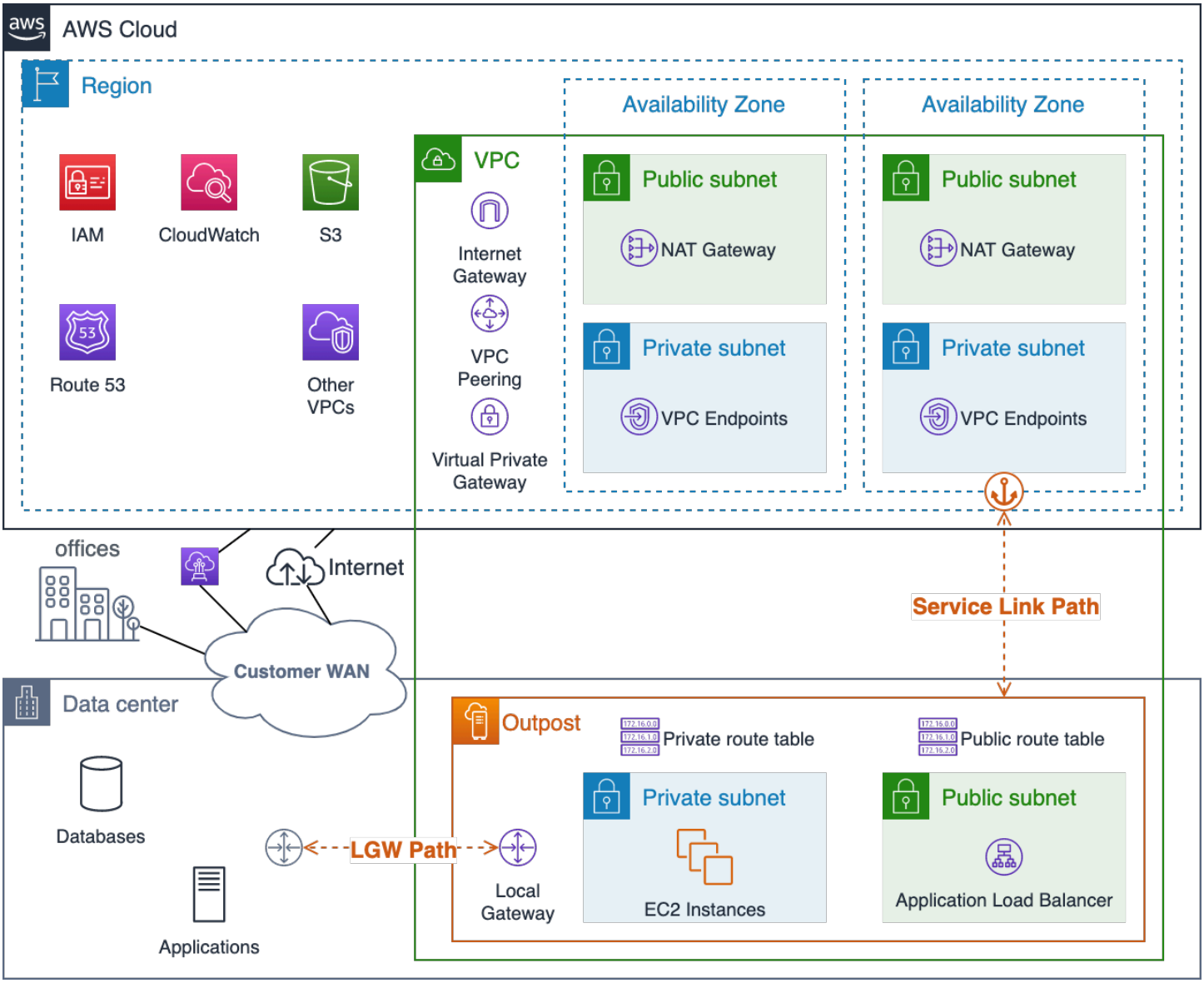
- Behalten Sie den Überblick über die EC2 Amazon-IP-Adressbereiche in Ihrer Firewall, wenn Sie eine Teilmenge der CIDR-Bereiche für die Region verwenden.
- Stellen Sie sicher, dass jeder Pfad die Anforderungen an Bandbreitenverfügbarkeit und Latenz erfüllt.
- Verwenden Sie dynamisches Routing, um die Verkehrsumleitung bei Netzwerkausfällen zu automatisieren.
- Testen Sie das Routing des Service Link-Datenverkehrs über jeden geplanten Netzwerkpfad, um sicherzustellen, dass der Pfad erwartungsgemäß funktioniert.

Routing von Anwendungen und Arbeitslasten

Für Anwendungs-Workloads gibt es zwei Wege aus dem Outpost heraus:

- Der Service-Link-Pfad: Bedenken Sie, dass der Anwendungsdatenverkehr mit dem Traffic auf der Kontrollebene von Outposts konkurrieren wird. Außerdem ist die MTU auf 1300 Byte begrenzt.
- Der lokale Gateway-Pfad (LGW): Bedenken Sie, dass das lokale Netzwerk des Kunden den Zugriff sowohl auf lokale als auch auf interne Anwendungen ermöglicht. AWS-Region

Sie konfigurieren die Routing-Tabellen des Outpost-Subnetzes, um zu steuern, welcher Pfad zum Erreichen der Zielnetzwerke verwendet werden soll. Routen, die auf das LGW verweisen, leiten den Verkehr vom lokalen Gateway zum lokalen Netzwerk weiter. Routen, die auf die Dienste und Ressourcen in der Region verweisen, wie Internet Gateway, NAT Gateway, Virtual Private Gateway und TGW, verwenden Service Link, um diese Ziele zu erreichen. Wenn Sie eine VPC-Peering-Verbindung mit mehreren VPCs auf demselben Outpost haben, VPCs verbleibt der Verkehr zwischen den Outpost und verwendet nicht den Service-Link zurück zur Region. Informationen zum VPC-Peering finden Sie unter Connect VPCs using VPC Peering im Amazon VPC-Benutzerhandbuch.



Visualisierung des Outpost-Servicelinks und der LGW-Netzwerkpfade

Bei der Planung des Anwendungsroutings sollten Sie darauf achten, sowohl den normalen Betrieb als auch die eingeschränkte Routing- und Serviceverfügbarkeit bei Netzwerkausfällen zu berücksichtigen. Der Service Link-Pfad ist nicht verfügbar, wenn ein Outpost von der Region getrennt wird.

Sie sollten verschiedene Pfade bereitstellen und dynamisches Routing zwischen dem Outpost LGW und Ihren kritischen lokalen Anwendungen, Systemen und Benutzern konfigurieren. Redundante Netzwerkpfade ermöglichen es dem Netzwerk, den Datenverkehr um Ausfälle herum weiterzuleiten und sicherzustellen, dass lokale Ressourcen bei teilweisen Netzwerkausfällen mit den Workloads kommunizieren können, die auf dem Outpost ausgeführt werden.

Outpost-VPC-Routenkonfigurationen sind statisch. Sie konfigurieren Subnetz-Routing-Tabellen über die AWS Management Console CLI und andere Infrastructure as Code (IaC) -Tools. Sie können die Subnetz-Routing-Tabellen jedoch während eines Verbindungsabbruchs nicht ändern. APIs Sie müssen die Konnektivität zwischen dem Outpost und der Region wiederherstellen, um die Routing-Tabellen zu aktualisieren. Verwenden Sie für den normalen Betrieb dieselben Routen, die Sie bei Verbindungsabbrüchen verwenden möchten.

Ressourcen auf dem Outpost können das Internet über den Service Link und ein Internet Gateway (IGW) in der Region oder über den Local Gateway (LGW) -Pfad erreichen. Durch die Weiterleitung des Internetverkehrs über den LGW-Pfad und das lokale Netzwerk können Sie vorhandene lokale Interneteingangs- und -ausgangspunkte verwenden. Dies kann im Vergleich zur Verwendung des Service Link-Pfads zu einem IGW in der Region zu einer geringeren Latenz und höheren MTUs und niedrigeren AWS Datenausgangsgebühren führen.

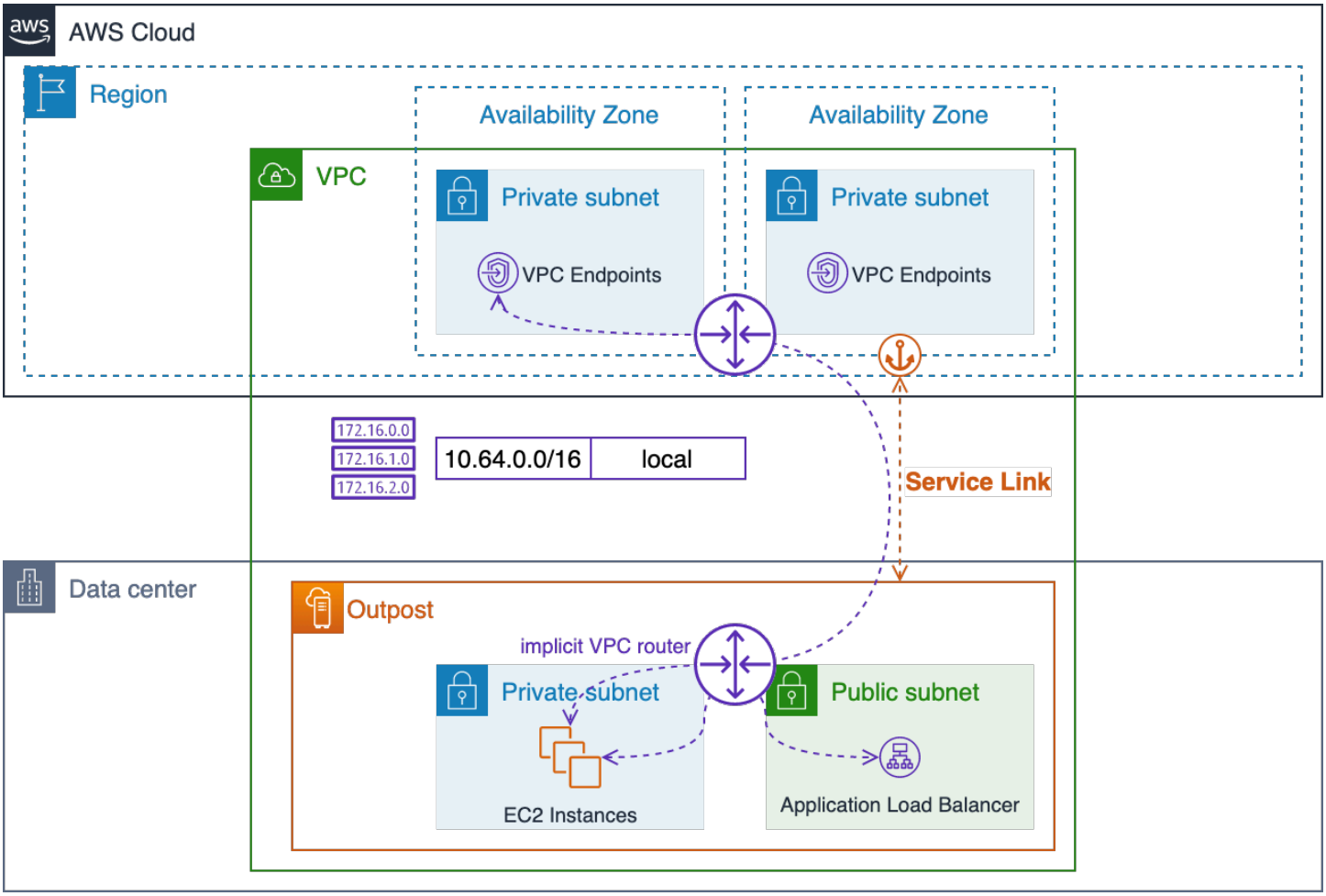
Wenn Ihre Anwendung lokal ausgeführt werden muss und über das öffentliche Internet zugänglich sein muss, sollten Sie den Anwendungsdatenverkehr über Ihre lokalen Internetverbindungen an das LGW weiterleiten, um die Ressourcen auf dem Outpost zu erreichen.

Sie können zwar Subnetze in einem Outpost wie öffentliche Subnetze in der Region konfigurieren, dies kann jedoch für die meisten Anwendungsfälle unerwünscht sein. Eingehender Internetverkehr wird über den Service Link zu den Ressourcen, die auf dem Outpost laufen, aufgenommen AWS-Region und über diesen weitergeleitet.

Der Antwortverkehr wird wiederum über die Service-Verbindung und wieder über die Internetverbindungen von weitergeleitet. AWS-Region Dieses Verkehrsmuster kann die Latenz erhöhen und es fallen Gebühren für ausgehende Daten an, wenn der Verkehr die Region auf dem Weg zum Außenposten verlässt und wenn der Rückverkehr durch die Region zurückkehrt und ins Internet gelangt. Wenn Ihre Anwendung in der Region ausgeführt werden kann, ist die Region der beste Ort, um sie auszuführen.

Der Verkehr zwischen VPC-Ressourcen (in derselben VPC) folgt immer der lokalen VPC-CIDR-Route und wird von den impliziten VPC-Routern zwischen Subnetzen weitergeleitet.

Beispielsweise wird der Verkehr zwischen einer EC2 Instance, die auf dem Outpost läuft, und einem VPC-Endpunkt in der Region immer über den Service Link geleitet.



Lokales VPC-Routing über die impliziten Router

Empfohlene Verfahren für das Routing von Anwendungen/Workloads

- Verwenden Sie nach Möglichkeit den Local Gateway (LGW) -Pfad anstelle des Service Link-Pfads.
- Leiten Sie den Internetverkehr über den LGW-Pfad weiter.
- Konfigurieren Sie die Outpost-Subnetz-Routingtabellen mit einer Reihe von Standardrouten. Diese werden sowohl für den normalen Betrieb als auch bei Verbindungsabbrüchen verwendet.
- Stellen Sie redundante Netzwerkpfade zwischen dem Outpost LGW und wichtigen lokalen Anwendungsressourcen bereit. Verwenden Sie dynamisches Routing, um die Verkehrsumleitung bei Netzwerkausfällen vor Ort zu automatisieren.

Datenverarbeitung

Während die EC2 Kapazität bei Amazon scheinbar unendlich AWS-Regionen ist, ist die Kapazität auf Outposts begrenzt. Sie sind für die Planung und Verwaltung der Rechenkapazität Ihrer Outposts-Bereitstellungen verantwortlich.

Themen

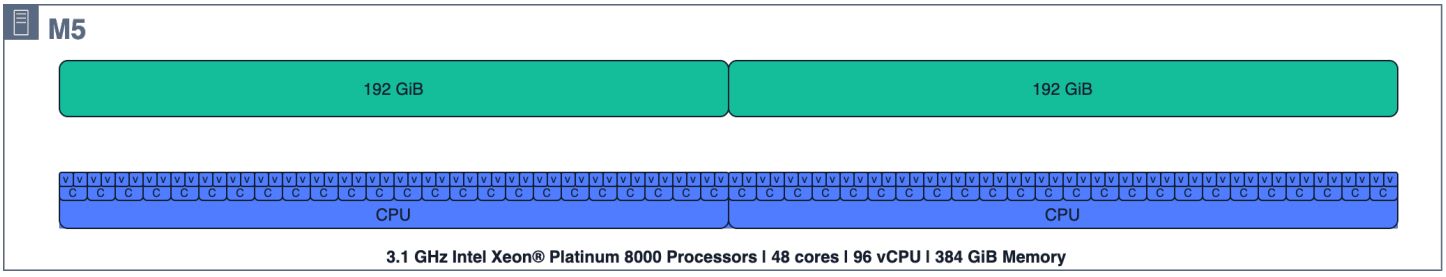
- Kapazitätsplanung
- Kapazitätsverwaltung
- Platzierung von Instanzen

Kapazitätsplanung

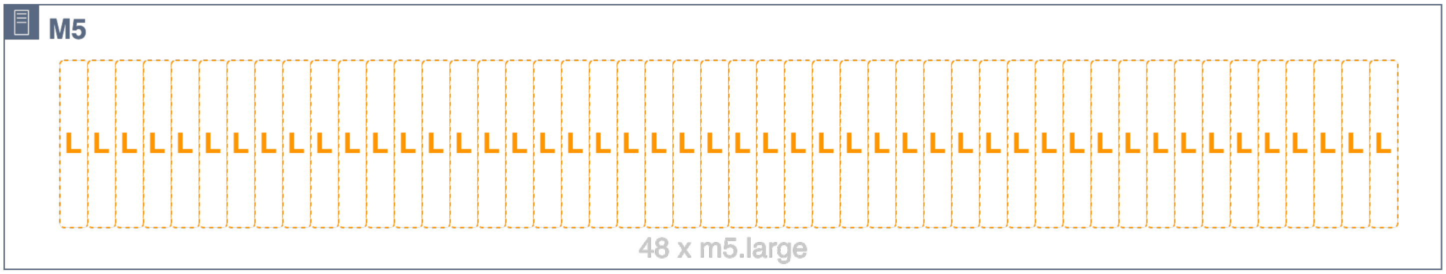
Während die EC2 Kapazität bei Amazon scheinbar unendlich AWS-Regionen ist, ist die Kapazität auf Outposts begrenzt — begrenzt durch das Gesamtvolumen der bestellten Rechenkapazität. Sie sind für die Planung und Verwaltung der Rechenkapazität Ihrer Outposts-Bereitstellungen verantwortlich. Sie sollten ausreichend Rechenkapazität bestellen, um ein N+M-Verfügbarkeitsmodell zu unterstützen, wobei N die erforderliche Anzahl von Servern und M die Anzahl der Reserveserver ist, die für Serverausfälle bereitgestellt werden. N+1 und N+2 sind die gängigsten Verfügbarkeitsstufen.

Jeder Host (`C5`, `M5R5`, usw.) unterstützt eine einzelne Instanzfamilie. EC2 Bevor Sie Instances auf EC2 Rechenservern starten können, müssen Sie Slot-Layouts bereitstellen, die die EC2 Instanzgrößen angeben, die jeder Server bereitstellen soll. AWS konfiguriert jeden Server mit dem angeforderten Slotting-Layout.

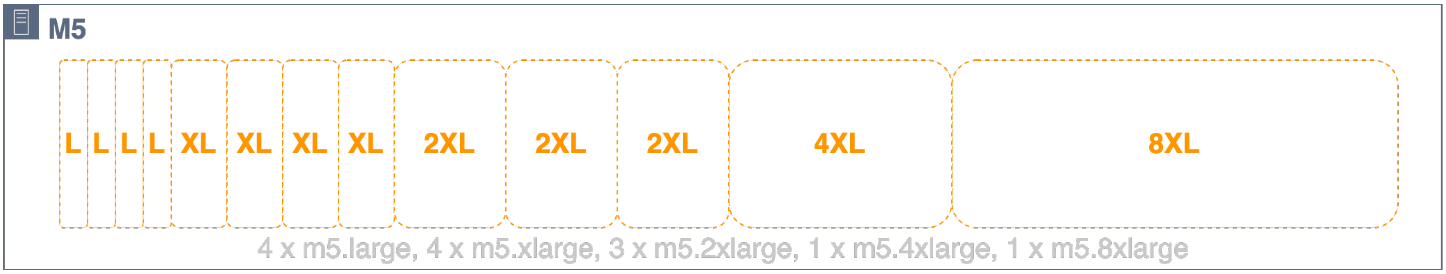
Hosts können homogen eingesetzt werden, wobei alle Steckplätze dieselbe Instanzgröße haben (z. B. 48 `m5.large` Steckplätze), oder heterogene Steckplätze mit einer Mischung von Instance-Typen (z. B. 4, 4`m5.large`, 3 `m5.xlarge` `m5.2xlarge`m5.4xlarge, 1 und 1`m5.8xlarge`). Visualisierungen dieser Steckplatzkonfigurationen finden Sie in den nächsten drei Abbildungen.



*`m5.24xlarge`*Host-Rechenressourcen



`m5.24xlarge`Der Host ist homogen in 48 Steckplätze aufgeteilt `m5.large`



`m5.24xlarge`Der Host ist heterogen in 4`m5.large`, 4, 3 `m5.xlargem5.2xlarge`, 1 und 1 Steckplätze aufgeteilt `m5.4xlarge` `m5.8xlarge`

Die volle Hostkapazität muss nicht in Steckplätze gesteckt werden. Einem Host, der über nicht zugewiesene Kapazität verfügt, können Steckplätze hinzugefügt werden. Sie können ein Steckplatz-Layout ändern, indem Sie die Kapazitätsverwaltung verwenden APIs oder UIs eine neue Kapazitätsaufgabe erstellen. AWS Outposts Weitere Informationen finden Sie unter Kapazitätsmanagement für AWS Outposts im AWS Outposts Benutzerhandbuch für Racks. Möglicherweise müssen Sie bestimmte Instances herunterfahren oder neu starten, um eine neue Kapazitätsaufgabe abzuschließen, wenn das neue Steckplatz-Layout nicht angewendet werden kann, solange bestimmte Steckplätze von laufenden Instances belegt sind. Mit der `CreateCapacityTask` API können Sie die Anzahl der einzelnen Instance-Größen angeben, die auf der angegebenen Outpost-ID vorhanden sein sollen. Falls eine Aufgabe aufgrund laufender Instances nicht abgeschlossen werden kann, werden Instanzen zurückgegeben, die gestoppt werden müssen, um die Anfrage zu erfüllen. An dieser Stelle können Sie optional angeben, dass Sie „N" zusätzliche Optionen für den Fall sehen möchten, dass Sie eine der zurückgegebenen Instances nicht beenden möchten, und Sie können auch eine EC2 Instanz-ID, ein Instanz-Tag, EC2 ein Konto oder einen Dienst angeben, die nicht als Instanz zum Herunterfahren vorgeschlagen werden sollten, um die Kapazitätsaufgabenanforderung zu erfüllen. Nachdem Sie die Option ausgewählt haben, für die Sie sich entscheiden möchten, empfehlen wir, den Dry Run-Parameter zu verwenden, um die vorgeschlagenen Änderungen zu validieren und die möglichen Auswirkungen vor der Implementierung zu verstehen.

Alle Hosts tragen ihre bereitgestellten Slots zu den EC2 Kapazitätspools im Outpost bei, und alle Slots eines bestimmten Instance-Typs und einer bestimmten Größe werden als ein einziger EC2 Kapazitätspool verwaltet. Zum Beispiel würde der vorherige, heterogen gegliederte Host mit`m5.large`,, `m5.xlarge` `m5.2xlarge`m5.4xlarge, und `m5.8xlarge` Steckplätzen diese Steckplätze zu fünf EC2 Kapazitätspools beitragen — einem Pool für jeden Instance-Typ und jede Instance-Größe. Diese Pools können auf mehrere Hosts verteilt sein, und die Platzierung von Instanzen sollte berücksichtigt werden, um eine hohe Verfügbarkeit der Workloads zu erreichen.

Bei der Planung von Kapazitätsreserven für die Verfügbarkeit von N+M-Hosts ist es wichtig, Server-Slots und EC2 Kapazitätspools zu berücksichtigen. AWS erkennt, wenn ein Host ausfällt oder heruntergefahren ist, und plant einen Besuch vor Ort, um den ausgefallenen Host zu ersetzen. Sie sollten Ihre EC2 Kapazitätspools so gestalten, dass sie den Ausfall von mindestens einem Server jeder Instance-Familie (N+1) in einem Outpost tolerieren. Mit diesem Mindestmaß an Hostverfügbarkeit können Sie ausgefallene oder heruntergestufte Instances auf den freien Steckplätzen der verbleibenden Hosts derselben Familie neu starten, wenn ein Host ausfällt oder außer Betrieb genommen werden muss.

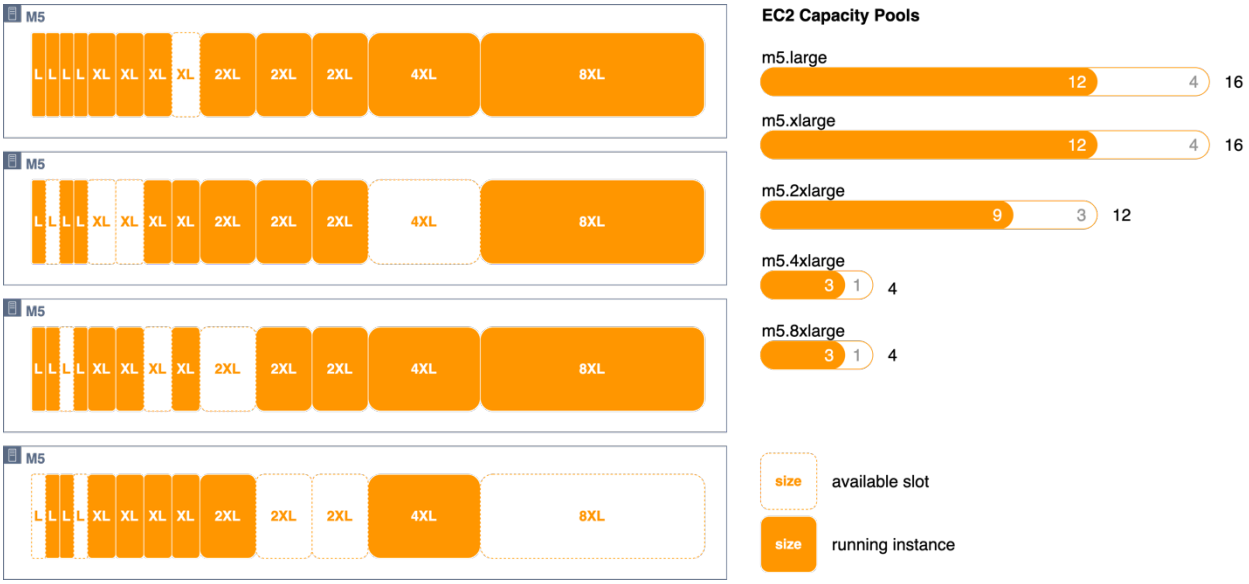
Die Planung der N+M-Verfügbarkeit ist einfach, wenn Sie über Hosts mit homogenen Steckplätzen oder Gruppen von Hosts mit unterschiedlichen Steckplätzen und identischen Steckplatzlayouts verfügen. Sie berechnen einfach die Anzahl der Hosts (N), die Sie für die Ausführung all Ihrer Workloads benötigen, und fügen dann (M) zusätzliche Hosts hinzu, um Ihre Anforderungen an die Serververfügbarkeit bei Ausfall- und Wartungsereignissen zu erfüllen.

Die folgenden Steckplatzkonfigurationen können aufgrund der NUMA-Grenzen nicht verwendet werden:

- 3 `m5.8xlarge`
- 1 `m5.16xlarge` und 1 `m5.8xlarge`

Wenden Sie sich an Ihr AWS-Konto Team, um Ihre geplante AWS Outposts Rack-Steckplatzkonfiguration zu überprüfen.

In der folgenden Abbildung sind vier `m5.24xlarge` Hosts heterogen mit einem identischen Steckplatzlayout ausgestattet. Die vier Hosts bilden fünf Kapazitätspools. EC2 Jeder Pool wird mit maximaler Auslastung (75%) ausgeführt, um die Verfügbarkeit von N+1 für die auf diesen vier Hosts ausgeführten Instances aufrechtzuerhalten. Wenn ein Host ausfällt, ist ausreichend Platz vorhanden, um die ausgefallenen Instances auf den verbleibenden Hosts neu zu starten.



Visualisierung von EC2 Host-Slots, laufenden Instances und Slot-Pools

Bei komplexeren Slot-Layouts, bei denen die Hosts nicht identisch sind, müssen Sie die N+M-Verfügbarkeit für jeden Kapazitätspool berechnen. EC2 Sie können die folgende Formel verwenden, um zu berechnen, wie viele Hosts (die Steckplätze zu einem bestimmten EC2 Kapazitätspool beitragen) ausfallen können und die verbleibenden Hosts trotzdem die laufenden Instances übertragen können:

$$M = \left\lceil \frac{poolSlots_{available}}{serverSlots_{max}} \right\rceil$$

Wobei gilt:

- PoolSlots $_{available}$ ist die Anzahl der verfügbaren Steckplätze im angegebenen EC2 Kapazitätspool (Gesamtzahl der Steckplätze im Pool abzüglich der Anzahl der laufenden Instanzen)
- ServerSlots $_{max}$ ist die maximale Anzahl von Steckplätzen, die von einem Host zum angegebenen Kapazitätspool bereitgestellt werden EC2
- M ist die Anzahl der Hosts, die ausfallen können und die es den verbleibenden Hosts trotzdem ermöglichen, die laufenden Instances zu übertragen

Beispiel: Ein Outpost hat drei Hosts, die Slots zu einem `m5.2xlarge` Kapazitätspool beitragen. Der erste Host stellt 4 Steckplätze, der zweite 3 Steckplätze und der dritte Host 2 Steckplätze zur

Verfügung. Der `m5.2xlarge` Instance-Pool auf dem Outpost hat eine Gesamtkapazität von 9 Steckplätzen (4 + 3 +2). Der Outpost hat 4 laufende `m5.2xlarge` Instances. Wie viele Hosts fallen möglicherweise aus und ermöglichen es den verbleibenden Hosts trotzdem, die laufenden Instances zu übertragen?

$$poolSlots_{available} = total\ capacity - running\ instances = 9 - 4 = 5$$

$$serverSlots_{max} = \max([4, 3, 2]) = 4$$

$$M = \left[\frac{poolSlots_{available}}{serverSlots_{max}}\right] = \left[\frac{5}{4}\right] = [1.25] = 1$$

Antwort: Sie können einen der Hosts verlieren und trotzdem die laufenden Instances auf den verbleibenden Hosts weiterführen.

Empfohlene Methoden für die Planung der Rechenkapazität

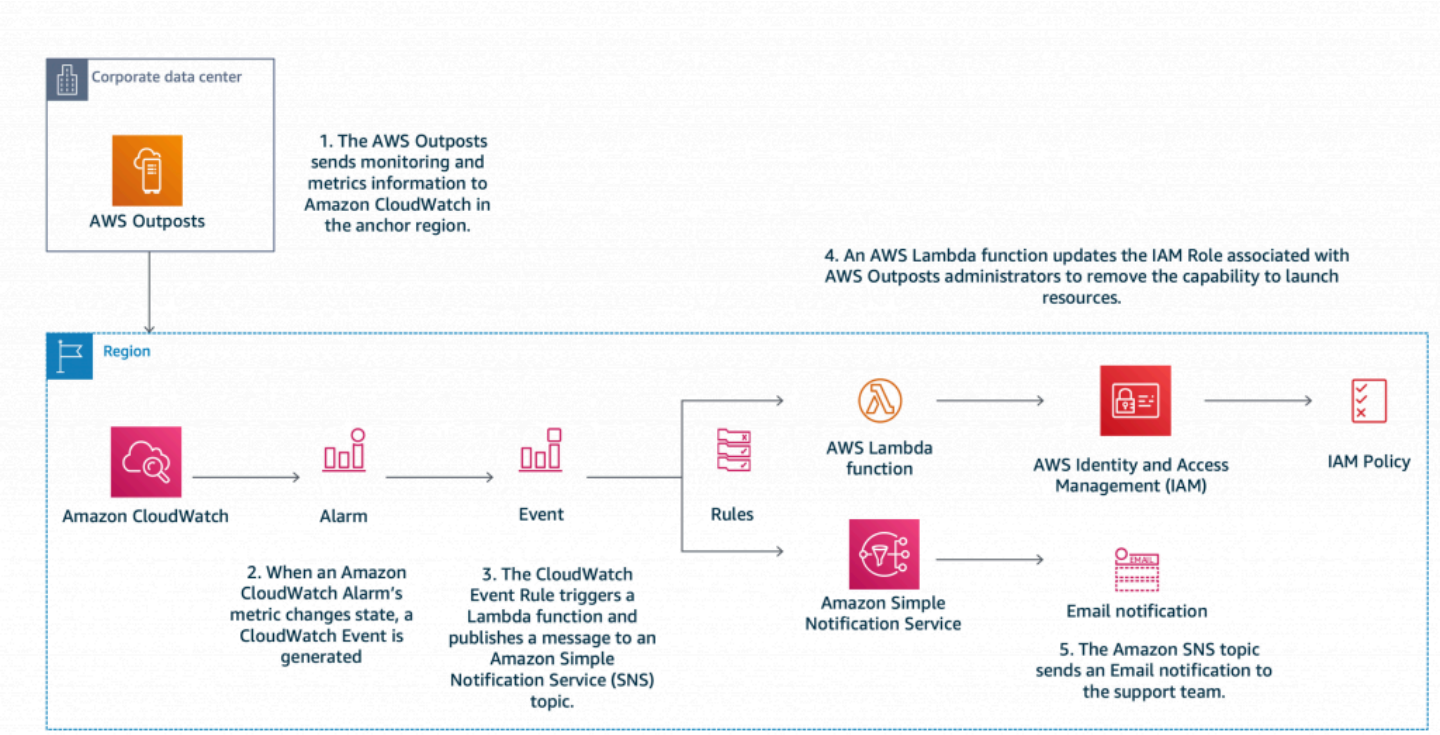
- Passen Sie Ihre Rechenkapazität so an, dass N+M-Redundanz für jeden EC2 Kapazitätspool auf einem Outpost bereitgestellt wird.
  - Stellen Sie N+M-Server für homogene oder identische Server mit heterogenen Steckplätzen bereit.
  - Berechnen Sie die N+M-Verfügbarkeit für jeden EC2 Kapazitätspool und stellen Sie sicher, dass jeder Pool Ihren Verfügbarkeitsanforderungen entspricht.

Kapazitätsverwaltung

Sie können die Nutzung des EC2 Outpost-Instance-Pools in den AWS Management Console und über CloudWatch Amazon-Metriken überwachen. Wenden Sie sich an den Enterprise Support, um die Slot-Layouts für Ihre Outposts abzurufen oder zu ändern.

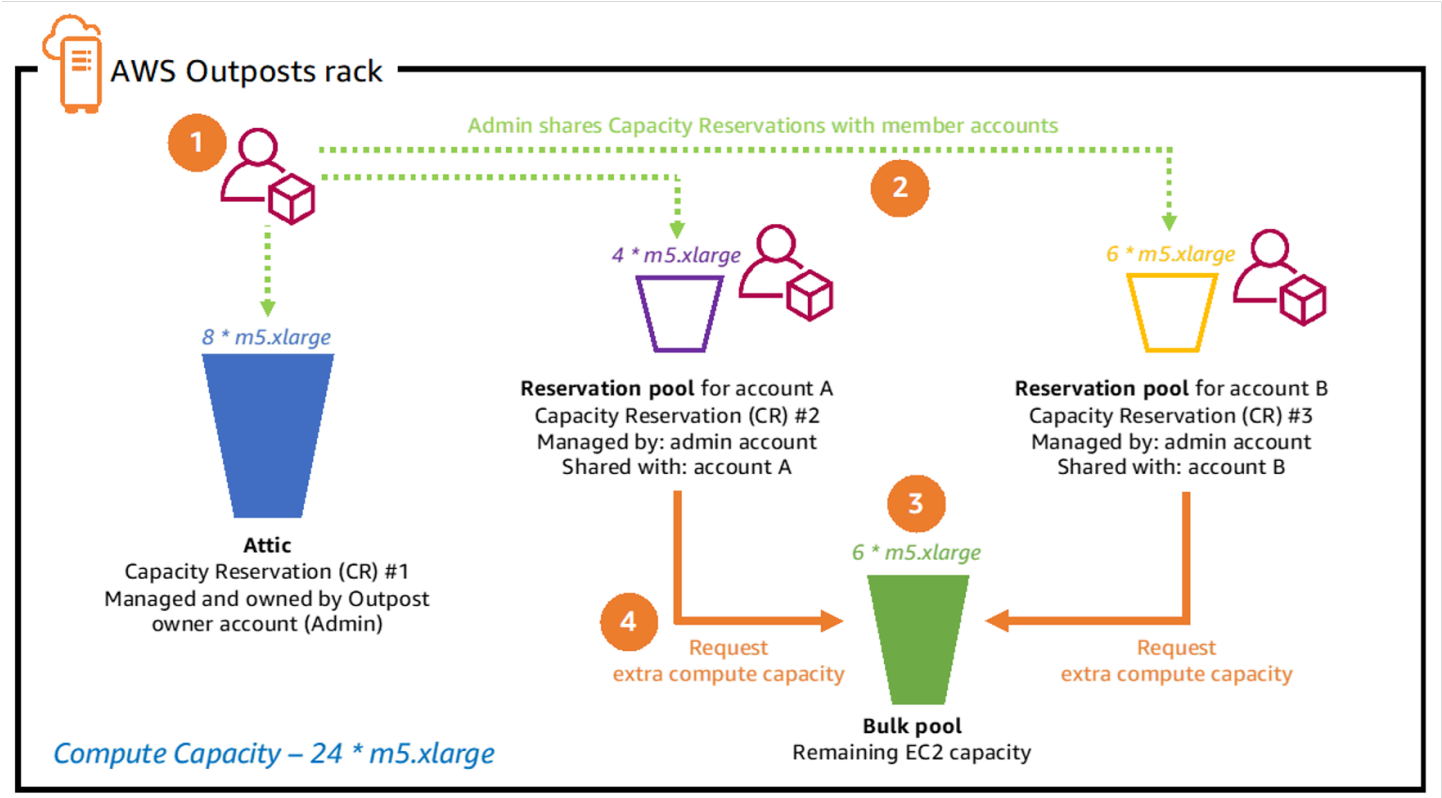
Sie verwenden dieselben Mechanismen für die auto Wiederherstellung und das EC2 Auto Scaling von Instanzen, um Instances wiederherzustellen oder zu ersetzen, die von Serverausfällen und Wartungsereignissen betroffen sind. Sie müssen Ihre Outpost-Kapazität überwachen und verwalten, um sicherzustellen, dass immer genügend Reservekapazitäten zur Verfügung stehen, um

Serverausfälle zu beheben. Der AWS Lambda Blogbeitrag Managing AWS Outposts your capacity using Amazon CloudWatch and blog bietet ein praktisches Tutorial, das Ihnen zeigt, wie Sie Ihre Outpost-Kapazität kombinieren AWS CloudWatch und AWS Lambda verwalten können, um die Instance-Verfügbarkeit aufrechtzuerhalten.

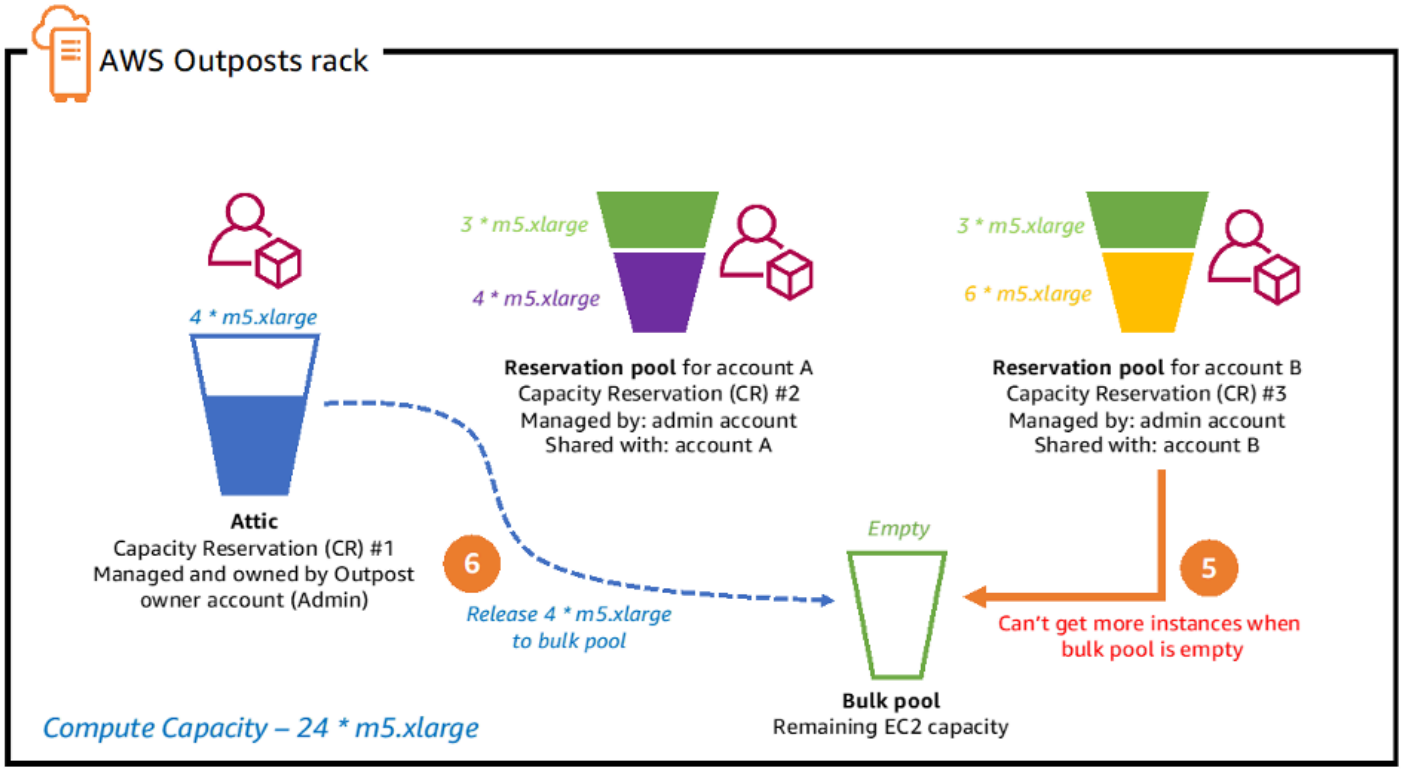


AWS Outposts Kapazitätsmanagement mit Amazon CloudWatch und AWS Lambda

Kapazitätsreservierungen können in einer Umgebung mit mehreren Konten verwendet werden, um zu kontrollieren, wie viel Ihrer Outpost-Rechenkapazität von einem einzelnen Konto oder einer AWS Organisationseinheit (OU) mit mehreren Konten genutzt wird. Sie können eine Kapazitätsreservierung für Amazon EC2 auf Outposts sowie auf unterstützten Outposts AWS-Services wie Amazon Elastic Kubernetes Service (EKS), Amazon Elastic Container Service (ECS) und Amazon Elastic Map Reduce (EMR) erstellen. Kapazitätsreservierungen werden über AWS Resource Access Manager (AWS RAM) im Outpost-Eigentümerkonto erstellt und für Konten freigegeben. Der Artikel Erstellen von Rechenkontingenten im AWS Outposts Rack mit gemeinsamer Nutzung von EC2 Kapazitätsreservierungen bietet ein praktisches Tutorial und zusätzliche Anleitungen zur Implementierung von Kapazitätsreservierungen mit Ihrem Outpost zum Zwecke der Kapazitätsverwaltung.



Capacity Reservation sharing process steps 1-4



Capacity Reservation sharing process steps 5-6

Empfohlene Vorgehensweisen für das Rechenkapazitätsmanagement

- Konfigurieren Sie Ihre EC2 Instances in Auto Scaling Scaling-Gruppen oder verwenden Sie Instance Auto Recovery, um ausgefallene Instances neu zu starten.
- Automatisieren Sie die Kapazitätsüberwachung für Ihre Outpost-Bereitstellungen und konfigurieren Sie Benachrichtigungen und (optional) automatische Antworten für Kapazitätsalarme.
- Verwenden Sie Kapazitätsreservierungen, um eine detaillierte Kontrolle darüber zu haben, wie viel Rechenkapazität von anderen Konten innerhalb Ihres Unternehmens gemeinsam genutzt wird. AWS

Platzierung von Instanzen

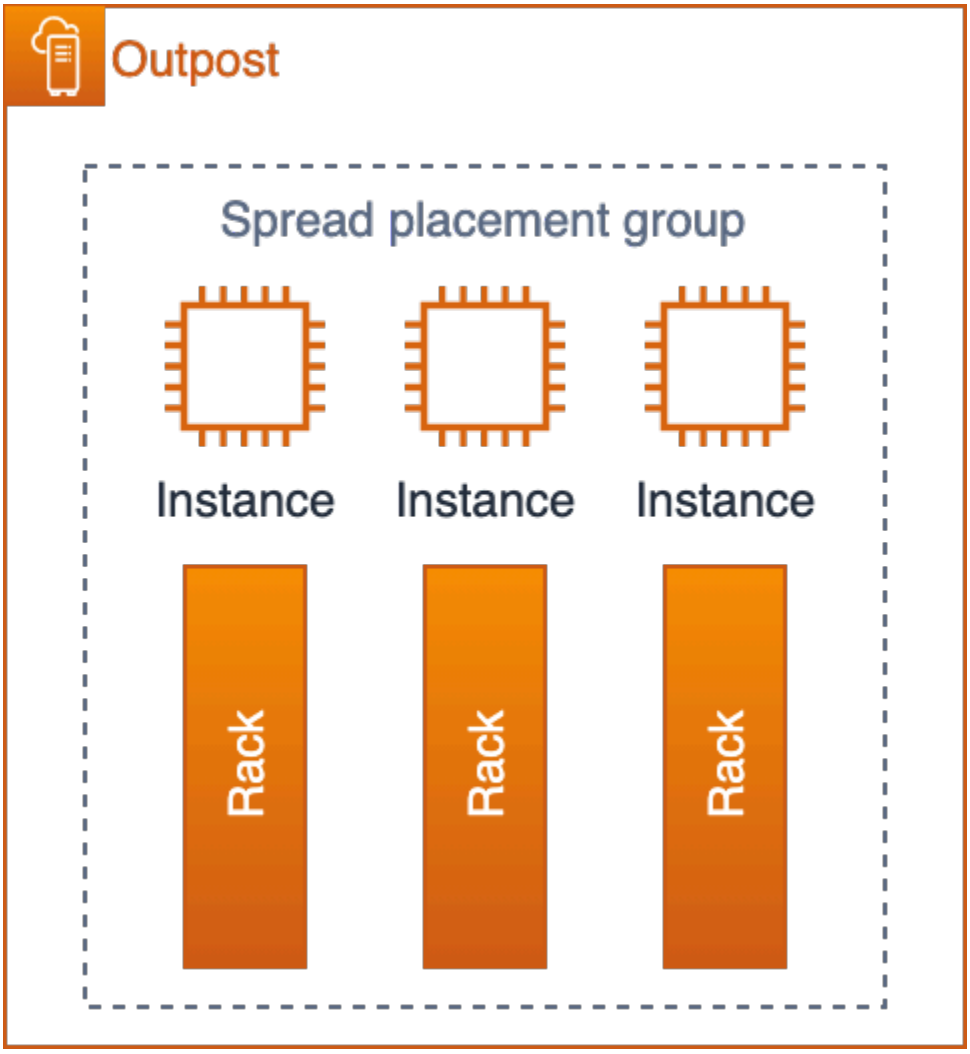
Outposts haben eine begrenzte Anzahl von Rechenhosts. Wenn Ihre Anwendung mehrere verwandte Instances auf Outposts bereitstellt, können die Instances ohne zusätzliche Konfiguration auf denselben Hosts oder auf Hosts im selben Rack bereitgestellt werden. Heute gibt es drei Mechanismen, mit denen Sie Instances verteilen können, um das Risiko zu minimieren, dass verwandte Instances auf derselben Infrastruktur ausgeführt werden:

Bereitstellung mehrerer Außenposten — Ähnlich wie bei einer Multi-AZ-Strategie in der Region können Sie Outposts in separaten Rechenzentren und Anwendungsressourcen in bestimmten Outposts bereitstellen. Auf diese Weise können Sie Instances auf dem gewünschten Outpost (einem logischen Satz von Racks) ausführen. Intra-VPC-Kommunikation über mehrere Outposts mit direktem VPC-Routing ist eine weitere Strategie, die verwendet werden kann, um Workloads auf mehrere Outposts innerhalb derselben VPC zu verteilen, indem die Outpost Local Gateways (LGW) verwendet werden, um Routen zwischen den Subnetzen auf den Outposts zu erstellen. Eine Strategie mit mehreren Outposts kann zum Schutz vor Rack- und Rechenzentrumsausfällen eingesetzt werden. Wenn die Außenposten in separaten AZs oder regionalen Ausfallmodi verankert sind, kann sie auch Schutz vor Ausfallmodi von AZ oder Region bieten. Weitere Informationen zu Architekturen mit mehreren Außenstellen finden Sie unter Larger Failure Modes.

EC2 Amazon-Platzierungsgruppen auf Outposts (Single-Outpost Multi-Rack-Instance-Platzierung) — Sie können Platzierungsgruppen auf Outposts erstellen, die Sie in Ihrem Konto erstellt haben. Auf diese Weise können Sie die Instances auf die zugrunde liegende Hardware auf einem Outpost an Ihrem Standort verteilen. Wenn Sie eine Platzierungsgruppe mit einer Spread-Strategie auf einem

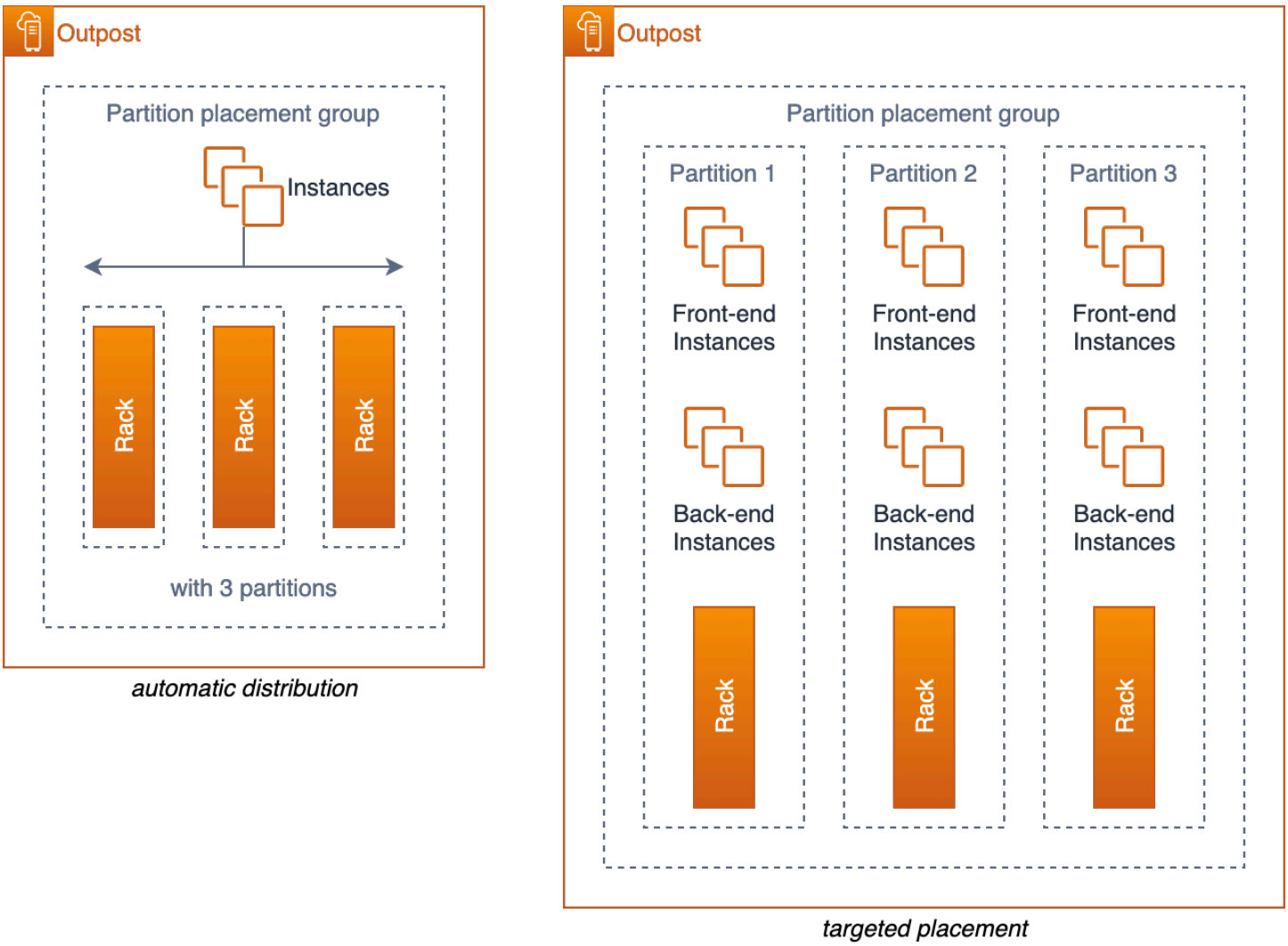
Outpost erstellen, können Sie wählen, ob die Platzierungsgruppe Instances über Hosts oder Racks verteilt.

Eine verteilte Platzierungsgruppe bietet eine einfache Möglichkeit, einzelne Instances auf Racks oder Hosts zu verteilen, um das Risiko korrelierter Ausfälle zu verringern. Sie dürfen in der Gruppe nur so viele Instances bereitstellen, wie Sie Hosts in Ihrem Outpost haben.



EC2 verteilte Platzierungsgruppe auf einem Außenposten mit drei Racks

Sie können Instances auch mit Platzierungsgruppen für Partitionen auf mehrere Racks verteilen. Verwenden Sie die automatische Verteilung, um Instanzen auf Partitionen in der Gruppe zu verteilen oder Instanzen auf ausgewählten Zielpartitionen bereitzustellen. Durch die Bereitstellung von Instances auf Zielpartitionen können Sie ausgewählte Ressourcen im selben Rack bereitstellen und gleichzeitig andere Ressourcen auf mehrere Racks verteilen. Wenn Sie beispielsweise einen logischen Outpost mit drei Racks haben, können Sie durch die Erstellung einer Partitionsplatzierungsgruppe mit drei Partitionen Ressourcen auf die Racks verteilen.



EC2 Platzierungsgruppen für Partitionen auf einem Outpost mit drei Racks

Creative Server-Slotting — Wenn Sie einen Outpost mit einem Rack haben oder wenn der Service, den Sie auf Outposts verwenden, keine Platzierungsgruppen unterstützt, können Sie Creative Slotting verwenden, um sicherzustellen, dass Ihre Instances nicht auf demselben physischen Server bereitgestellt werden. Wenn die zugehörigen Instances dieselbe EC2 Instance-Größe haben, können Sie Ihre Server möglicherweise in Steckplätze einteilen, um die Anzahl der auf jedem Server konfigurierten Steckplätze dieser Größe zu begrenzen und so die Steckplätze auf die Server zu verteilen. Durch Server-Slotting wird die Anzahl der Instanzen (dieser Größe) begrenzt, die auf einem einzelnen Server ausgeführt werden können.

Betrachten Sie als Beispiel das zuvor in Abbildung 13 gezeigte Steckplatz-Layout. Wenn Ihre Anwendung drei `m5.4xlarge` Instanzen auf dem mit diesem Steckplatz-Layout konfigurierten Outpost bereitstellen EC2 müsste, würde jede Instanz auf einem separaten Server platziert werden

und es bestünde keine Möglichkeit, dass diese Instanzen auf demselben Server ausgeführt werden könnten — solange die Steckplatzkonfiguration nicht geändert wird, um zusätzliche `m5.4xlarge` Steckplätze auf den Servern zu öffnen.

Empfohlene Methoden für die Platzierung von Recheninstanzen

- Verwenden Sie Amazon EC2 Placement-Gruppen auf Outposts, um die Platzierung von Instances in Racks innerhalb eines einzigen logischen Outposts zu kontrollieren.
- Anstatt einen Outpost mit einem einzigen mittleren oder großen Outpost-Rack zu bestellen, sollten Sie erwägen, die Kapazität in zwei kleine oder mittlere Racks aufzuteilen, damit Sie die Möglichkeit der EC2 Platzierungsgruppen nutzen können, Instances auf mehrere Racks zu verteilen.
- Die Amazon EC2 Placement-Gruppe auf Outposts kann verwendet werden, um die Platzierung von EKS-Knotengruppen, Control Plane-Knoten für EKS Local Cluster und ECS Task zu beeinflussen.
- Verwenden Sie Intra-VPC-Kommunikation, um Workloads auf mehrere Outposts innerhalb derselben VPC zu verteilen.

Speicher

Der AWS Outposts Rack-Service bietet drei Speichertypen:

- Instance-Speicher auf unterstützten EC2 Instance-Typen
- GP2-Volumes von Amazon Elastic Block Store (EBS) für persistenten Blockspeicher
- Amazon Simple Storage Service on Outposts (S3 on Outposts) für lokalen Objektspeicher

Instance-Speicher wird auf unterstützten Servern (`C5d`,, `M5d` `R5dG4dn`, und`I3en`) bereitgestellt. Genau wie in der Region bleiben die Daten in einem Instance-Speicher nur für die (laufende) Lebensdauer der Instance erhalten.

Outposts EBS-Volumes und S3 auf Outposts Object Storage werden als Teil der AWS Outposts Rack Managed Services bereitgestellt. Die Kunden sind für das Kapazitätsmanagement der Outpost-Speicherpools verantwortlich. Kunden geben bei der Bestellung eines Outpost ihre Speicheranforderungen für EBS- und S3-Speicher an. AWS konfiguriert den Outpost mit der Anzahl der Speicherserver, die zur Bereitstellung der angeforderten Speicherkapazität erforderlich sind. AWS ist verantwortlich für die Verfügbarkeit der Speicherdienste EBS und S3 auf Outposts. Es werden ausreichend Speicherserver bereitgestellt, um dem Outpost hochverfügbare Speicherdienste

bereitzustellen. Der Verlust eines einzelnen Speicherservers sollte weder die Dienste unterbrechen noch zu Datenverlusten führen.

Sie können die CloudWatch Metriken AWS Management Console und verwenden, um die Kapazitätsauslastung von Outpost EBS und S3 zu überwachen.

Datenschutz

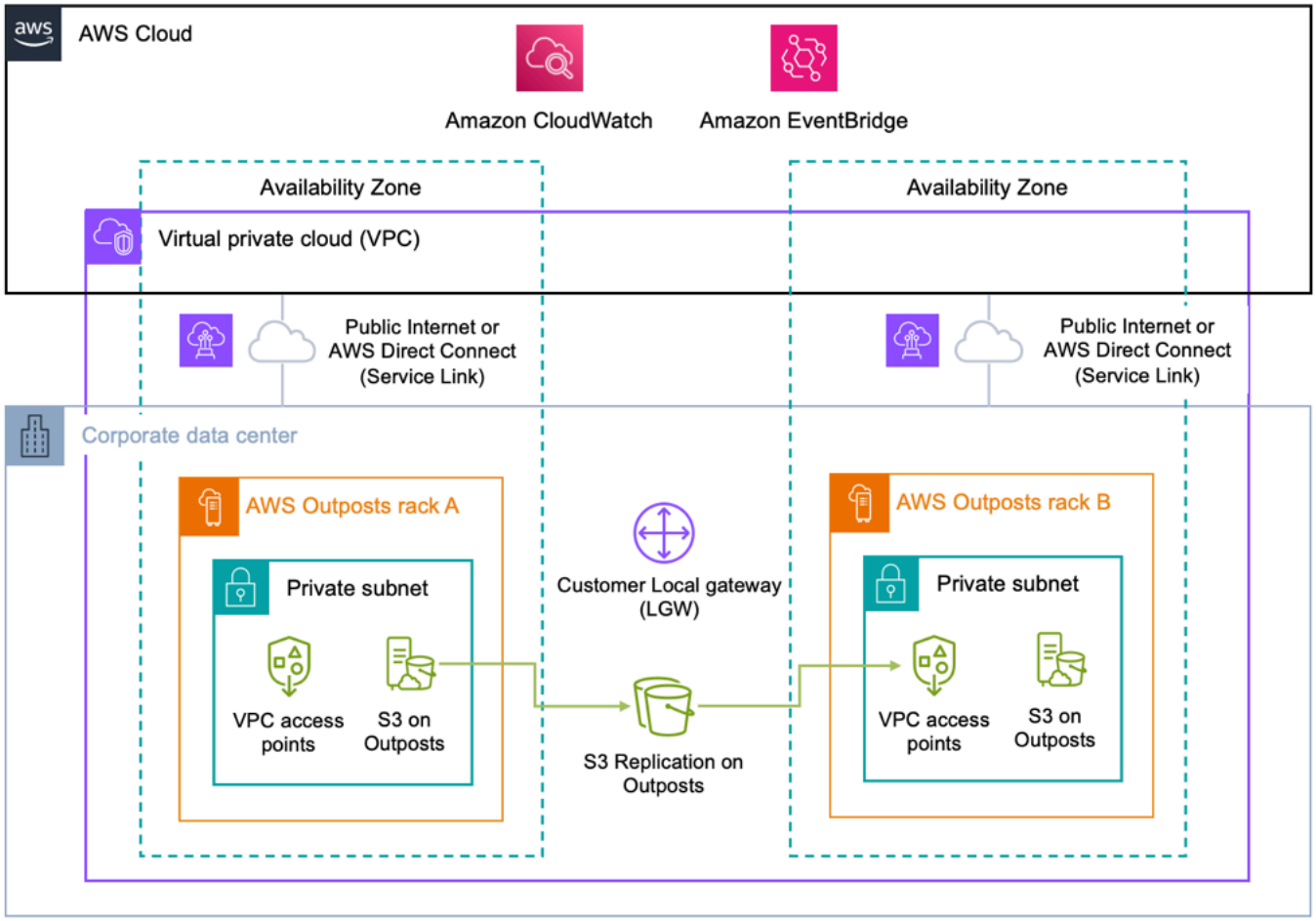
Für EBS-Volumes: AWS Outposts Rack unterstützt EBS-Volume-Snapshots und bietet so einen einfachen und sicheren Datenschutzmechanismus zum Schutz Ihrer Blockspeicherdaten. Snapshots sind point-in-time inkrementelle Backups Ihrer EBS-Volumes. Standardmäßig werden Snapshots von Amazon EBS-Volumes auf Ihrem Outpost auf Amazon S3 in der Region gespeichert. Wenn Ihre Outposts mit der Kapazität S3 on Outposts konfiguriert wurden, können Sie EBS Local Snapshots on Outposts verwenden, um Snapshots mithilfe von S3 on Outposts lokal in Ihrem Outpost zu speichern.

Für S3 in Outposts-Buckets (Anwendungsfälle für Datenresidenz):

- Sie können die S3-Versionierung für Outposts verwenden, um alle Änderungen und den Verlauf von Objekten zu speichern. Wenn diese Option aktiviert ist, speichert die S3-Versionsverwaltung mehrere unterschiedliche Kopien eines Objekts im selben Bucket. Sie können die S3-Versionsverwaltung verwenden, um sämtliche Versionen aller Objekte in Ihren Outposts-Buckets zu speichern, abzurufen oder wiederherzustellen. Mit der S3-Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.
- Sie können S3 Replication on Outposts verwenden, um Replikationsregeln zu erstellen und zu konfigurieren, um Ihre S3-Objekte automatisch in einen anderen Outpost oder in einen anderen Bucket auf demselben Outpost zu replizieren. Während der Replikation werden Objekte von S3 on Outposts über das lokale Gateway (LGW) des Kunden gesendet, und Objekte werden nicht zurück zum gesendet. AWS-Region S3 Replication on Outposts bietet eine einfache und flexible Möglichkeit, Daten innerhalb eines bestimmten Datenperimeters automatisch zu replizieren, um Datenredundanz und Compliance-Anforderungen zu erfüllen.

  S3 Replication on Outposts bietet außerdem detaillierte Metriken und Benachrichtigungen, um den Status Ihrer Objektreplikation zu überwachen. Sie können den Replikationsfortschritt überwachen, indem Sie ausstehende Bytes, ausstehende Operationen und die Replikationslatenz zwischen Ihren Quell- und Ziel-Outposts-Buckets mithilfe von Amazon verfolgen. CloudWatch Sie können auch EventBridge Amazon-Regeln einrichten, um Ereignisse mit Replikationsfehlern zu

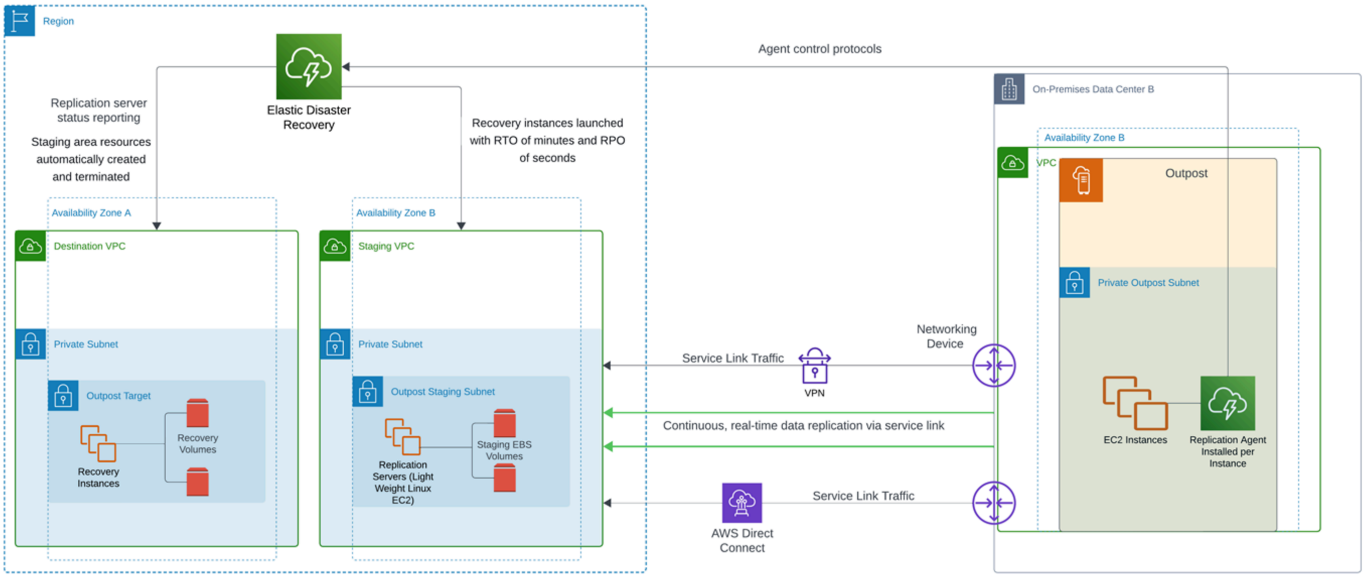
empfangen, um Konfigurationsprobleme schnell zu diagnostizieren und zu korrigieren. Weitere Informationen zur Konfiguration finden Sie im YouTube Video Amazon S3 Replication on Outposts.



Für S3 on Outposts-Buckets (Anwendungsfälle ohne Datenresidenz) zu AWS-Regionen: Sie können Amazon S3 on AWS DataSync Outposts-Datenübertragungen zwischen Ihrem Outpost und der Region automatisieren. DataSync ermöglicht es Ihnen, auszuwählen, was und wann übertragen werden soll und wie viel Bandbreite Sie verwenden möchten. Durch die Sicherung Ihrer lokalen S3 on Outposts-Buckets in S3-Buckets in den AWS-Region können Sie die 99,999999999% (11 9) Datenbeständigkeit und zusätzliche Speicherstufen (Standard, Infrequent Access und Glacier) zur Kostenoptimierung nutzen, die mit dem regionalen S3-Service verfügbar sind.

Instanzreplikation: Sie können AWS Elastic Disaster Recovery (AWS DRS) verwenden, um einzelne Instances und angehängten Blockspeicher von lokalen Systemen zu einem Outpost, von einem Outpost zur Region, von der Region zu einem Outpost oder von einem Outpost zu einem anderen Outpost zu replizieren. Der Blogbeitrag Architecting for Disaster Recovery on AWS Outposts Racks

with AWS Elastic Disaster Recovery beschreibt jedes dieser Szenarien und wie man eine Lösung mit DRS entwickelt. AWS



Disaster Recovery (DR) von einem Außenposten in die Region

Die Verwendung des AWS Outposts Racks als AWS DRS-Ziel (Replikationsziel) erfordert S3 Outposts Outposts-Speicher, der zum Speichern replizierter Amazon EBS-Snapshots verwendet wird. S3-Speicher auf Outposts ist auch auf den Quell-Outposts für das Failback erforderlich. Das Outposts-Rack muss Direct VPC Routing (DVR) verwenden, um DRS verwenden zu können. AWS AWS DRS kann nicht zum Schutz von Managed Service Instances auf Outposts verwendet werden. Es wird nur für die Notfallwiederherstellung von EC2 Instances und ihren angehängten EBS-Volumes unterstützt.

Empfohlene Verfahren für den Datenschutz:

- Verwenden Sie EBS-Snapshots, um point-in-time Backups von Blockspeicher-Volumes auf Amazon S3 in der Region oder S3 auf Outposts zu erstellen.
- Verwenden Sie S3 für die Objektversionierung in Outposts, um mehrere Versionen und den Verlauf Ihrer Objekte zu verwalten.
- Verwenden Sie S3 Replication on Outposts, um Ihre Objektdaten automatisch auf einen anderen Outpost zu replizieren.
- Verwenden Sie für Anwendungsfälle außerhalb der Datenresidenz, AWS DataSync um Objekte, die in S3 auf Outpost gespeichert sind, auf Amazon S3 in der Region zu sichern.

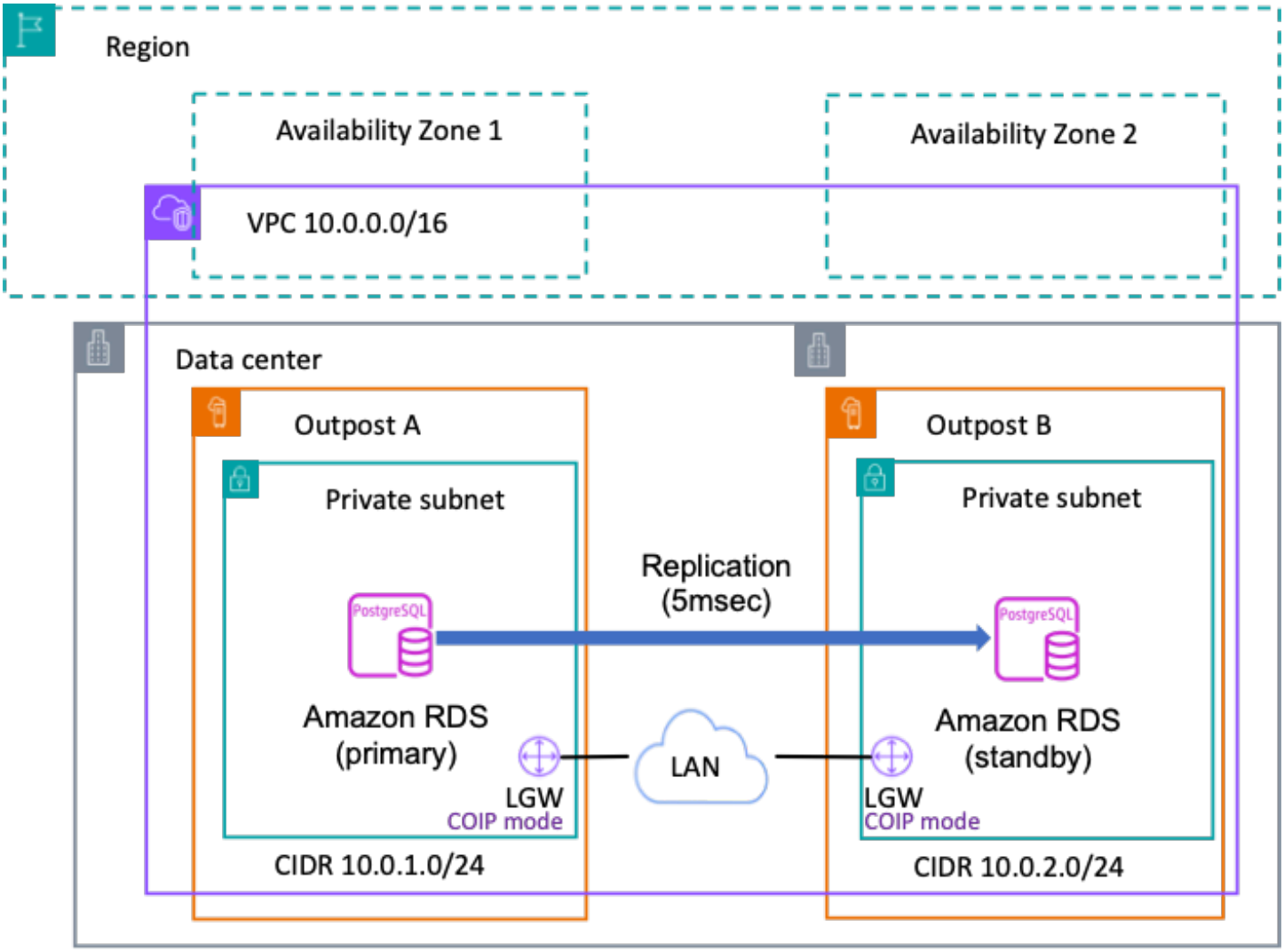
- Verwenden Sie AWS DRS, um Instanzen zwischen lokalen Systemen, logischen Outposts und der Region zu replizieren.

Datenbanken

Amazon Relational Database Service (RDS) on AWS Outposts erweitert RDS für SQL Server-, RDS für MySQL- und RDS für PostgreSQL-Datenbanken auf Bereitstellungen. AWS Outposts Für Bereitstellungen, bei denen eine hochverfügbare Architektur bereitgestellt werden muss, unterstützt Amazon RDS die Bereitstellung von Multi-AZ-Instances für PostgreSQL und MySQL auf. AWS Outposts

Amazon RDS auf Outposts mit Multi-AZ

In Multi-AZ-Bereitstellungen erstellt Amazon RDS eine primäre DB-Instance auf einer AWS Outposts und RDS repliziert die Daten synchron auf eine Standby-DB-Instance auf einem anderen Outposts. Um eine ausfallsichere Architektur bereitzustellen, AWS Outposts müssen beide in verschiedenen Availability Zones in einer bestimmten Region verankert sein und nach einem kundeneigenen IP-Modell (CoIP) betrieben werden. Um die Replikation zwischen der primären Instanz und der Standby-Instanz zu ermöglichen, muss eine Netzwerkverbindung zwischen den beiden Outposts mit einer Round-Time-Latenz (RTT) von einstelligen Millisekunden bestehen. Wir empfehlen 5 Millisekunden oder weniger. Erwägen Sie auch, die Replikationsverbindung zwischen Outposts mit ausreichender Bandbreite zu dimensionieren, um zu vermeiden, dass Replikationsaufträge in Warteschlangen stehen.



Amazon RDS auf Outpost mit Multi-AZ

Überlegungen zu Amazon RDS auf Outposts mit Multi-AZ

Sehen Sie sich die folgenden Überlegungen für Bereitstellungen von Amazon RDS on Outposts in Multi-AZ an:

- Verfügen Sie über mindestens zwei Outposts-Bereitstellungen, die in verschiedenen Availability Zones derselben verankert sind. AWS-Region
- Sowohl die Primär- als auch die Standby-Instanz benötigen eine einzelne VPC und ein Subnetz pro Outposts-Bereitstellung.
- Ordnen Sie die VPC Ihrer DB-Instance all Ihren lokalen Gateway-Routentabellen zu.
- Stellen Sie sicher, dass Ihre Outposts kundeneigenes IP-Routing verwenden.

- Ihr lokales Netzwerk muss ausgehenden und damit verbundenen eingehenden Verkehr zwischen Outposts for Internet Security Association und Key Management Protocol (ISAKAMP) zulassen, die UPD-Port 500 und IPsec Network Address Translation Traversal (NAT-T) über UDP-Port 4500 verwenden.
- Lokale RDS-Backups werden für Multi-AZ-Bereitstellungen nicht unterstützt.
- Wenn Ihr Workload den für Ihre Branche oder Region geltenden Vorschriften zur Datenresidenz entsprechen muss, wenden Sie sich an die Aufsichtsbehörden, um festzustellen, ob Multi-AZ RDS Ihren Anforderungen entspricht.

Weitere Informationen finden Sie unter Arbeiten mit Multi-AZ-Bereitstellungen für Amazon RDS auf AWS Outposts.

Amazon RDS auf AWS Outposts Read Replicas

Amazon RDS Read Replicas bieten verbesserte Leistung und Haltbarkeit für Amazon RDS-Datenbank-Instances (DB). Sie erleichtern die elastische Skalierung über die Kapazitätsbeschränkungen einer einzelnen DB-Instance hinaus für leseintensive Datenbank-Workloads. Amazon RDS on AWS Outposts verwendet die integrierten Replikationsfunktionen der MySQL- und PostgreSQL-DB-Engines, um eine Read Replica aus einer Quell-DB-Instance zu erstellen. Die Quell-DB-Instance wird zur primären DB-Instance. In der primären DB-Instance ausgeführte Updates werden asynchron in das Lesereplikat kopiert. Read Replica verwendet das kundeneigene IP-Modell (CoIP), und die Replikationen werden in Ihrem lokalen Netzwerk ausgeführt.

Überlegungen zu Amazon RDS on Outposts Read Replicas

Lesen Sie die folgenden Überlegungen zu Bereitstellungen von Amazon RDS on Outposts für Read Replicas:

- Sie können keine Lesereplikate für RDS für SQL Server auf DB-Instances von RDS on Outposts erstellen.
- Regionsübergreifende Lesereplikate werden in RDS on Outposts nicht unterstützt.
- Kaskadierende Lesereplikate werden in RDS on Outposts nicht unterstützt.
- Für die Quell-DB-Instance von RDS on Outposts kann es keine lokalen Backups geben. Das Backup-Ziel für die Quell-DB-Instance muss Ihre AWS-Region sein. Stellen Sie sicher, dass Sie über eine redundante Service Link-Verbindung mit mindestens 500 Mbit/s verfügen, um Ihre RDS-Backups an AWS-Region Datenbanken mit sich häufig ändernden Daten oder hohem Schreibverkehr zu senden.

- Sie benötigen kundeneigene IP-Pools (CoIP-Pools).
- Read Replicas auf RDS on Outposts können nur in derselben Virtual Private Cloud (VPC) wie die Quell-DB-Instance erstellt werden.
- Read Replicas auf RDS on Outposts können sich auf demselben Outpost oder einem anderen Outpost in derselben VPC wie die Quell-DB-Instance befinden.
- Sie können keine Read Replicas für DB-Instances erstellen, die mit AWS KMS External Key Store (XKS) verschlüsselt wurden.
- Das Erstellen Ihres Lesereplikats als Multi-AZ-DB-Instance ist unabhängig davon, ob die Quelldatenbank eine Multi-AZ-DB-Instance ist.

Automatische Skalierung von Amazon RDS-Speicher aktiviert AWS Outposts

Wenn Ihr Workload unvorhersehbar ist, können Sie die automatische Speicherskalierung für eine Amazon RDS-DB-Instance aktivieren. Amazon Relational Database Service (Amazon RDS) on AWS Outposts unterstützt die manuelle und automatische Speicherskalierung. Wenn Amazon RDS feststellt, dass Ihrer DB-Instance nicht mehr genügend freier Datenbankspeicher zur Verfügung steht, skaliert Amazon RDS Ihren Speicher automatisch auf der Grundlage der EBS-Kapazität, die für Ihre Outposts-Bereitstellung vorgesehen ist. Die Funktion bietet dieselben Funktionen wie in Regionen, in denen bestimmte Faktoren für die automatische Skalierung gelten. Weitere Informationen finden Sie im Amazon RDS-Autoscaling-Leitfaden. Es ist wichtig, den maximalen Speicherplatz, der RDS-Instances auf Outposts zugewiesen wird, sorgfältig zu verwalten, da EBS-Ressourcen auf die im Outpost bereitgestellte Kapazität beschränkt sind. Mit der automatischen Skalierung von Amazon RDS-Speicher können Sie ein maximales Speicherlimit festlegen und so sicherstellen, dass Ihre Bereitstellung innerhalb der verfügbaren EBS-Kapazität bleibt. Weitere Informationen zur Verwaltung Ihrer Outpost-Kapazität finden Sie im Abschnitt Kapazitätsmanagement dieses Whitepapers.

Amazon RDS bei AWS Outposts lokalem Backup

Lokale Amazon RDS-Backups AWS Outposts ermöglichen es Ihnen, eine RDS-DB-Instance direkt aus S3 wiederherzustellen, die lokal in Ihren Outposts gespeichert ist. Auf diese Weise können Sie die Anforderungen an die Datenresidenz erfüllen und die Latenz im Vergleich zur Wiederherstellung aus einem reduzieren. AWS-Region Wenn Amazon RDS aktiviert ist AWS Outposts, haben Sie die folgenden Wiederherstellungsoptionen:

- Aus einem manuellen DB-Snapshot, der in der übergeordneten Region oder lokal in Ihren Outposts gespeichert ist.
- ein automatisiertes Backup (point-in-time Wiederherstellung):
  - Wenn Sie Backups von der übergeordneten AWS-Region Seite wiederherstellen, können Sie Backups entweder in den AWS-Region oder auf Ihren Outposts speichern.
  - Bei der Wiederherstellung von Ihren Outposts müssen Backups lokal auf Outposts mit S3-Unterstützung gespeichert werden.

Überlegungen zum lokalen Amazon RDS-Backup auf AWS Outposts

Beachten Sie die folgenden Überlegungen, um die Vorteile der lokalen Amazon RDS-Backups zu nutzen AWS Outposts:

- Sie benötigen die Kapazität von S3 on Outposts, um die Backups lokal zu speichern.
- Lokale Backups werden auf MySQL- und PostgreSQL-DB-Instances unterstützt.
- Lokale Backups werden für Multi-AZ-Instance-Bereitstellungen oder Read Replicas nicht unterstützt.

Exportieren und Wiederherstellen von Snapshots für RDS auf AWS Outposts

Exportieren von Snapshots nach S3 und Wiederherstellen einer DB-Instance aus Amazon S3: RDS-Snapshots können zwar direkt aus Amazon S3 exportiert oder wiederhergestellt werden AWS-Region, dies wird jedoch in Umgebungen nicht unterstützt. AWS Outposts

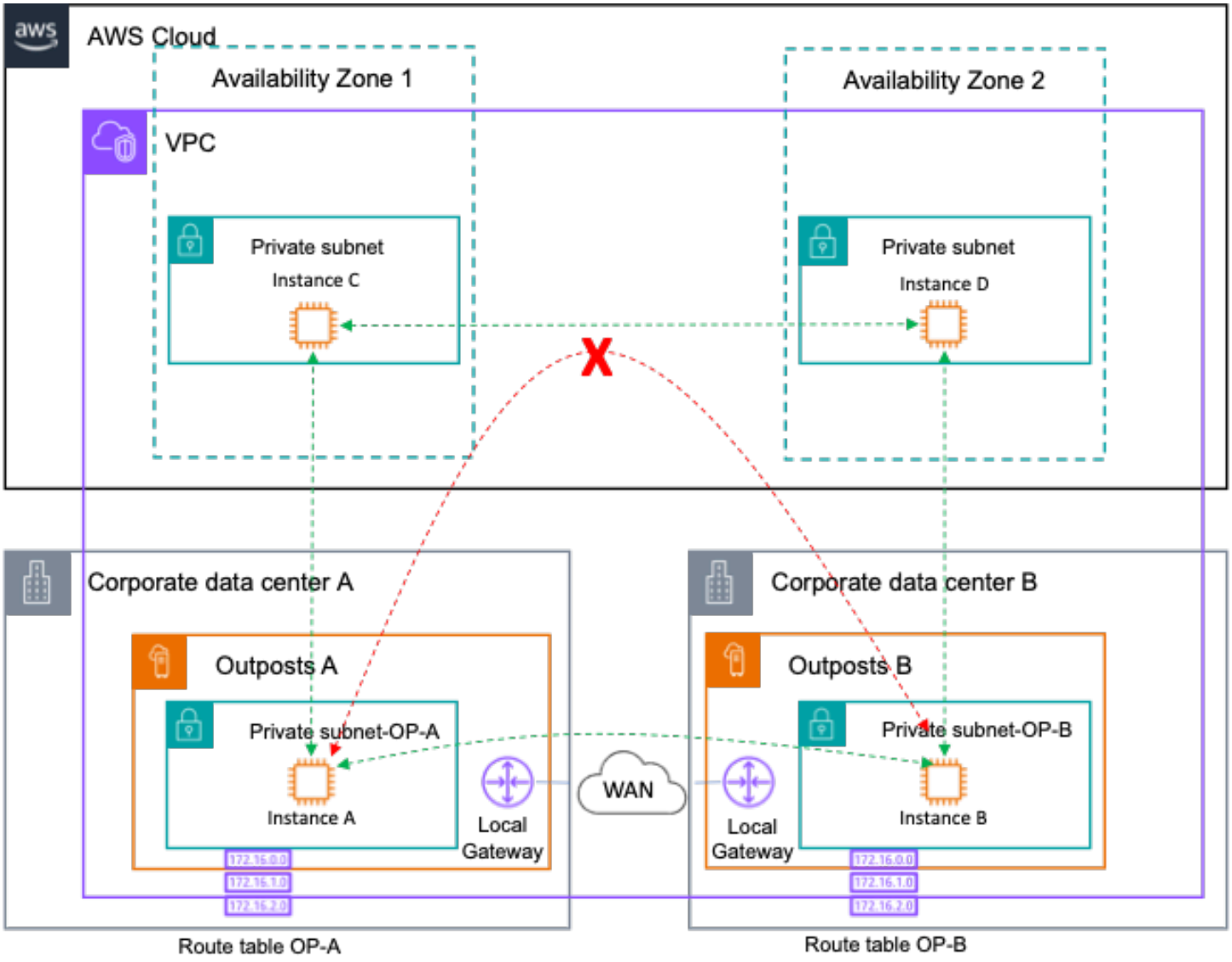
Größere Fehlermodi

Um HA-Architekturen so zu entwickeln, dass größere Ausfallmodi wie Rack-, Rechenzentrums-, Availability Zone- (AZ) oder Regionsausfälle vermieden werden, sollten Sie mehrere Outposts mit ausreichender Infrastrukturkapazität in separaten Rechenzentren mit unabhängiger Stromversorgung und WAN-Konnektivität bereitstellen. Sie verankern die Outposts in verschiedenen Availability Zones (AZs) innerhalb einer AWS-Region oder mehrerer Regionen. Sie sollten außerdem eine stabile und ausreichende site-to-site Konnektivität zwischen den Standorten bereitstellen, um die synchrone oder asynchrone Datenreplikation und die Umleitung des Workload-Datenverkehrs zu unterstützen. Abhängig von Ihrer Anwendungsarchitektur können Sie weltweit verfügbares Amazon Route 53 DNS und Amazon Route 53 on Outposts verwenden, um den Verkehr an den gewünschten Standort

zu leiten und die Umleitung des Datenverkehrs an überlebende Standorte bei großen Ausfällen zu automatisieren.

Outposts Rack Intra-VPC-Routing

AWS Outposts Das Rack unterstützt die Intra-VPC-Kommunikation über mehrere Outposts hinweg. Ressourcen auf zwei separaten logischen Outposts können miteinander kommunizieren, indem sie den Datenverkehr zwischen Subnetzen innerhalb derselben VPC, die sich über sie erstrecken, mithilfe der Outpost Local Gateways (LGW) weiterleiten. Bei der Intra-VPC-Kommunikation über mehrere Outposts hinweg können Sie die lokale Route in der mit dem Outposts-Subnetz verknüpften Routentabelle überschreiben, indem Sie dem anderen Outposts-Subnetz eine spezifischere Route hinzufügen und dabei das lokale LGW als nächsten Hop verwenden. Dies kann Vorteile bei der Architektur von Anwendungen bieten, die eine VPC zwischen zwei logischen Outposts als Amazon ECS über zwei Outposts-Racks oder Amazon EKS-Cluster erfordern. AWS Outposts



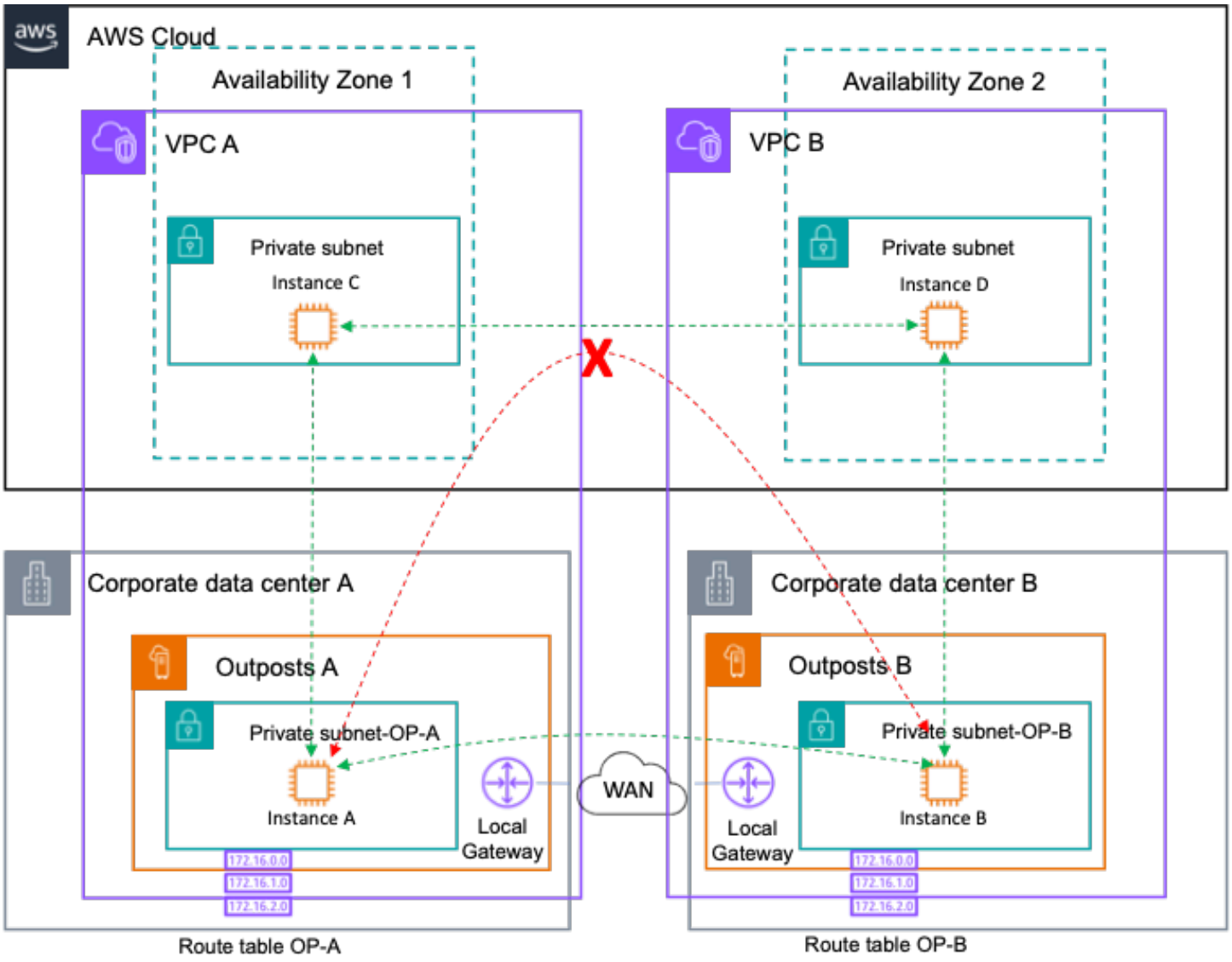
Netzwerkpfade für eine einzelne VPC mit mehreren logischen Outposts

Outposts-to-Outposts Die Weiterleitung des Datenverkehrs durch die Region ist blockiert, da es sich dabei um ein Anti-Pattern handelt. Bei einem solchen Verkehr würden Gebühren für ausgehenden Verkehr in beide Richtungen und eine deutlich höhere Latenz anfallen als bei der Weiterleitung des Datenverkehrs über das Kunden-WAN.

Outposts Rack-Inter-VPC-Routing

Ressourcen auf zwei separaten Outposts, die an unterschiedlichen Standorten eingesetzt werden, VPCs können über das Kundennetzwerk miteinander kommunizieren. Outposts-to-OutpostsDurch die Bereitstellung dieser Architektur können Sie den Datenverkehr über Ihre lokalen lokalen Netzwerke

und WAN-Netzwerke weiterleiten und Routen zu den entsprechenden Außenposten/VPC-Subnetzen hinzufügen.



Netzwerkpfade für mehrere VPC mit mehreren logischen Outposts

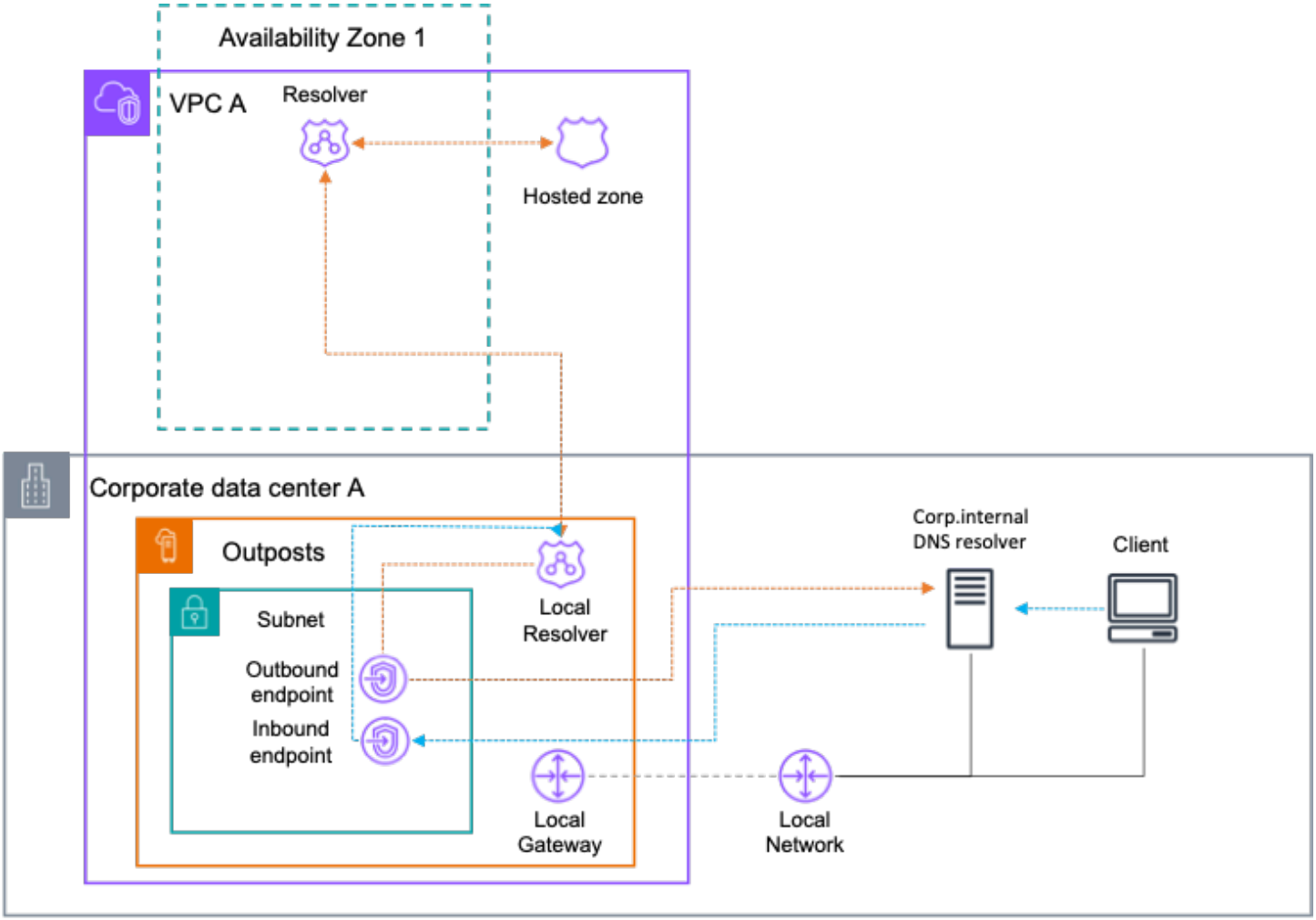
Empfohlene Vorgehensweisen zum Schutz vor größeren Ausfallarten:

- Setze mehrere Outposts ein, die in mehreren AZs Regionen verankert sind.
- Verwenden Sie bei einer Bereitstellung mit mehreren Außenposten VPCs für jeden Außenposten separat.

Lokaler Route-53-Resolver auf Outposts

Wenn die AWS Outposts Dienstverbindung durch eine vorübergehende Unterbrechung beeinträchtigt wird, schlägt die lokale DNS-Auflösung fehl, was es für Anwendungen und Dienste schwierig macht, andere Dienste zu erkennen, selbst wenn sie im selben Outposts-Rack ausgeführt werden. Wenn Route 53 Resolver aktiviert ist AWS Outposts, profitieren Anwendungen und Dienste jedoch weiterhin von der lokalen DNS-Auflösung, um andere Dienste zu erkennen — selbst wenn die Konnektivität zum übergeordneten AWS-Region Server unterbrochen wird. Gleichzeitig trägt der Route 53 Resolver on Outposts bei der DNS-Auflösung für lokale Hostnamen dazu bei, die Latenz zu reduzieren, da die Abfrageergebnisse zwischengespeichert und lokal bereitgestellt werden und gleichzeitig vollständig in die Route 53 Resolver-Endpunkte integriert sind.

Route 53 53-Resolver Eingehende Endpunkte leiten DNS-Anfragen, die sie von außerhalb der VPC erhalten, an den Resolver weiter, der in Outposts ausgeführt wird. Im Gegensatz dazu ermöglichen Route 53 Resolver Outbound Route 53 53-Resolvern, DNS-Abfragen an DNS-Resolver weiterzuleiten, die Sie in Ihrem lokalen Netzwerk verwalten, wie in der folgenden Abbildung dargestellt.



Route 53-Resolver auf Outposts

Überlegungen zu Route 53 Resolver on Outposts

Berücksichtigen Sie dabei Folgendes:

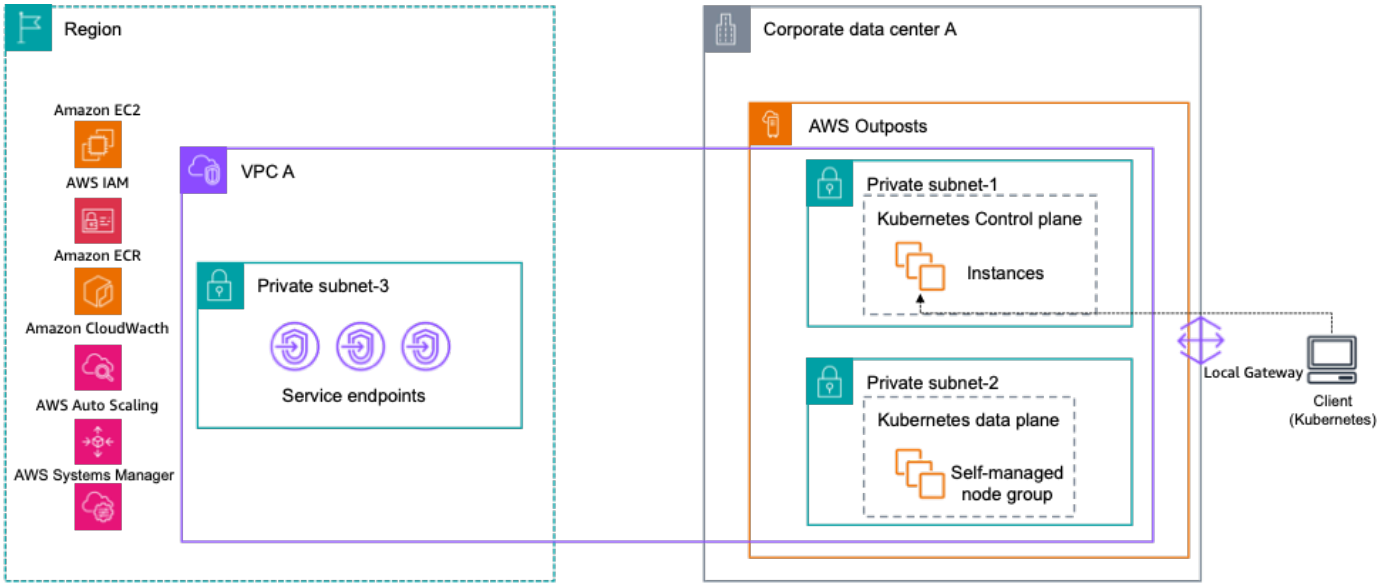
- Sie müssen den Route 53 Resolver auf Outposts aktivieren, und er gilt für die gesamte Outposts-Bereitstellung, auch wenn diese mehrere Compute-Racks unter einer einzigen Outposts-ID umfasst.
- Um diese Funktion zu aktivieren, müssen Ihre Outposts über genügend Rechenkapazität verfügen, um den lokalen Resolver in Form von mindestens 4 EC2 Instanzen von c5.xlarge, m5.large oder m5.xlarge bereitzustellen.
- Wenn Sie privates DNS verwenden, müssen Sie die Private Hosted Zone mit den erforderlichen Outposts VPCs 'teilen, um die Datensätze lokal im Route 53 Resolver on Outposts zwischenzuspeichern.

- Um die Integration mit lokalem DNS mit eingehenden und ausgehenden Endpunkten zu ermöglichen, müssen Ihre Outposts über genügend Rechenkapazität verfügen, um zwei EC2 Instanzen pro Route53-Endpunkt bereitzustellen.

Lokaler EKS-Cluster auf Outposts

Wenn es zu Verbindungsabbrüchen zwischen Outposts und der übergeordneten Region kommt, kann es zu Problemen mit Diensten wie EKS Extended Cluster kommen, bei denen sich die Kontrollebene in der Region befindet. Zu den Herausforderungen gehört der Verlust der Kommunikation zwischen der EKS-Steuerebene und den Worker-Knoten und. PODs Obwohl beide Worker-Nodes weiterhin Anwendungen betreiben und warten PODs können, die sich lokal auf Outposts befinden, kann es sein, dass die Kubernetes-Kontrollebene sie als fehlerhaft einstuft und ihren Austausch einplant, wenn die Verbindung zur Kontrollebene wiederhergestellt ist. Dies kann zu Anwendungsausfällen führen, wenn die Konnektivität wiederhergestellt ist.

Um dies zu vereinfachen, besteht die Möglichkeit, Ihren gesamten EKS-Cluster auf Outposts zu hosten. In dieser Konfiguration werden sowohl die Kubernetes-Steuerebene als auch Ihre Worker-Knoten lokal vor Ort auf der Rechenkapazität Ihrer Outposts ausgeführt. Auf diese Weise funktioniert Ihr Cluster auch bei einem vorübergehenden Ausfall Ihrer Service Link-Verbindung und nach deren Wiederherstellung weiter.



Lokaler Amazon EKS-Cluster auf Outposts

Überlegungen zum lokalen EKS-Cluster auf Outposts

Es gibt einige Überlegungen, wenn ein lokaler EKS-Cluster in Outposts bereitgestellt wird:

- Während einer Verbindungsunterbrechung gibt es keine Optionen, um Änderungen am Cluster selbst vorzunehmen, die das Hinzufügen neuer Worker-Knoten oder die automatische Skalierung einer Knotengruppe erfordern, solange dies von der übergeordneten Region abhängt EC2 und die AWS ASG-API-Aufrufe an sie richten.
- • In der eksctl-Unterstützung sind eine Reihe von Funktionen auf lokalen Clustern aufgeführt, die nicht unterstützt werden. AWS Outposts .

Schlussfolgerung

Mit AWS Outposts Rack können Sie hochverfügbare lokale Anwendungen mit vertrauten AWS Tools und Services wie Amazon, Amazon EBS EC2, Amazon S3 on Outposts, Amazon ECS, Amazon EKS und Amazon RDS erstellen, verwalten und skalieren. Workloads können lokal ausgeführt werden, Clients bedienen, auf Anwendungen und Systeme in Ihren lokalen Netzwerken zugreifen und auf das gesamte Serviceangebot in der zugreifen. AWS-Region Das Outposts-Rack ist ideal für Workloads, die einen Zugriff auf lokale Systeme mit geringer Latenz, lokale Datenverarbeitung, Datenresidenz und Migration von Anwendungen mit lokalen Systemabhängigkeiten erfordern.

Wenn Sie eine Outpost-Bereitstellung mit ausreichend Strom, Platz und Kühlung sowie zuverlässigen Verbindungen zu den AWS-Region Geräten bereitstellen, können Sie hochverfügbare Dienste für ein einzelnes Rechenzentrum einrichten. Und um ein höheres Maß an Verfügbarkeit und Ausfallsicherheit zu erreichen, können Sie mehrere Outposts bereitstellen und Ihre Anwendungen über logische und geografische Grenzen hinweg verteilen.

Das Outposts Rack macht den undifferenzierten Aufbau von lokalen Rechen-, Speicher- und Anwendungsnetzwerkpools überflüssig und ermöglicht es Ihnen, die Reichweite der AWS globalen Infrastruktur auf Ihre Rechenzentren und Colocation-Einrichtungen auszudehnen. Jetzt können Sie Ihre Zeit und Energie darauf konzentrieren, Ihre Anwendungen zu modernisieren, Ihre Anwendungsbereitstellungen zu optimieren und die geschäftliche Wirkung Ihrer IT-Services zu erhöhen.

Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Jesus Federico, leitender Lösungsarchitekt, Telco, Amazon Web Services
- Mallory Gershenfeld, S3 auf Outposts, Amazon Web Services
- Rob Goodwin, leitender Lösungsarchitekt, Hybrid Cloud, Amazon Web Services
- Chris Lunsford, leitender spezialisierter Lösungsarchitekt AWS Outposts, Amazon Web Services
- Rohan Mathews, leitender Architekt AWS Outposts, Amazon Web Services
- Brianna Rosentrater, Architektin für spezialisierte Hybrid-Edge-Lösungen, Amazon Web Services
- Leonardo Solano, leitender Architekt für spezialisierte Hybrid-Edge-Lösungen, Amazon Web Services
-

Dokumentverlauf

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Änderung	Beschreibung	Datum
Größere Aktualisierung	Updates zu Netzwerken, DRS-Unterstützung, Amazon EKS Local Cluster, Placement Groups und Amazon RDS hinzugefügt auf AWS Outposts	24. November 2024
Kleines Update	Bei der Kapazitätsplanung wurden zusätzliche Hinweise zur Zeitplanung hinzugefügt.	9. Februar 2024
Kleines Update	Aktualisiert, um den seit der ersten Veröffentlichung eingeführten Funktionen Rechnung zu tragen.	19. Juli 2023
Kleines Update	Die empfohlenen Vorgehens weisen für Netzwerkv erbindungen mit hoher Verfügbarkeit wurden aktualisi ert.	29. Juni 2023
Erste Veröffentlichung	Das Whitepaper wurde erstmals veröffentlicht.	12. August 2021

> **Note**
>
> Um RSS-Updates zu abonnieren, muss für den von Ihnen verwendeten Browser ein RSS-Plug-In aktiviert sein.

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

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